IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 November 2025, accepted 24 November 2025, date of publication 28 November 2025,
date of current version 5 December 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3638604

TOPICAL REVIEW

A Critical Review of Advanced Protection Devices in AC Microgrid

KAYODE EBENEZER OJO[1], AKSHAY KUMAR SAHA[1], (Senior Member, IEEE), AND VIRANJAY M. SRIVASTAVA[1,2], (Senior Member, IEEE)

[1]Discipline of Electrical, Electronic and Computer Engineering, University of KwaZulu-Natal, Durban 4041, South Africa
[2]Department of Electronics Engineering, Birmingham City University, B4 7XG Birmingham, U.K.

Corresponding author: Akshay Kumar Saha (saha@ukzn.ac.za)

ABSTRACT Protection is a crucial component of any power system that aims to deliver reliable, safe, and secure electricity of high quality and consistency. Creating a dependable protection system for an AC microgrid is challenging due to numerous practical considerations. In this work, several protection devices (PDs) in AC microgrids are systematically analyzed, with a focus on systems that employ electronically connected Distributed Energy Resources (DERs). This work employed several mathematical modeling equations to illustrate the challenges in microgrid protection associated with various operating modes. This study emphasizes the move toward intelligent and adaptive PDs, which offer enhanced fault isolation, real-time load balancing, fault detection, and system resilience. This research also underlines the usefulness of artificial intelligence (AI) in reducing the negative consequences of cyberattacks and cybersecurity challenges, especially those that jeopardize data integrity and confidentiality in microgrid PDs. Through an examination of pertinent standards and regulations, this paper explores how sophisticated communication and measurement methods might facilitate adaptive microgrid PDs that can update and modify relay settings automatically. The paper ends with several recommendations, highlighting the necessity of stronger cybersecurity measures and more reliable PDs to guarantee that the microgrid keeps playing a vital part in the shift to low-carbon energy.

INDEX TERMS AC microgrids, artificial intelligence, communication, cyberattacks, distributed energy resources, protection devices.

I. INTRODUCTION

Microgrids (MGs) are cutting-edge solutions to contemporary power system challenges, offering enhanced energy security, improved grid stability, and support for climate change mitigation. Within a particular electrical boundary, a group of distributed energy resources (DERs), local loads, and a control and protection system can be referred to as a microgrid [1]. From the standpoint of a utility, a microgrid is an independent component of the power system that can be deployed with local loads without the need for a transmission system. From the user's standpoint, however, it is a carefully built system that, with the help of a protective system, local controller, and power optimizer, provides stable, dependable, and efficient power [2]. MGs usually function in two modes: islanded mode and grid-connected mode. When in grid-connected mode, a microgrid is powered by both its DERs and the utility grid, but DERs are the main power source. In grid-connected mode, the utility grid supplements the microgrid by meeting additional load demands and maintaining voltage and frequency stability, and overall system reliability. When the load is in islanded mode, the only energy source that can meet its needs is micro energy resources. Energy management is crucial in islanded mode to meet load demand during peak and off-peak load periods. Only necessary loads are supplied with electricity during times of peak demand, while extra energy is stored locally during off-peak hours to maintain the power balance [3], [4]. Despite the fact that MGs offer numerous benefits to the economy and environment, such as reduced expenses, less infrastructure, and less power

The associate editor coordinating the review of this manuscript and approving it for publication was Ayman El-Baz.

loss, they also encounter several operational and technical challenges, including issues with protection, system stability, managing voltage and frequency, and power quality. The variety of DERs and the dynamic nature of microgrid topologies present significant difficulties for system operators and protection engineers. As microgrid usage continues to increase globally, strong protection plans are needed due to technical developments and legislative incentives [5].

Protective measures are crucial for identifying and reducing operating risks, disruptions, and malfunctions to guarantee a steady supply of energy to vital loads. Protection systems avoid blackouts, cascading failures, and power supply interruptions by separating the defective area from the healthy areas [6]. Microgrid protection development is a dynamic, multifaceted field influenced by changing regulatory frameworks, operational demands, and technology improvements. Protection devices (PDs) have evolved since the early days of microgrid development, when traditional centralized grid protection systems were employed. Basic protection against anomalies and failures was provided by these traditional systems, which included circuit breakers (CBs), voltage protectors, and overcurrent relays. Conventional power systems' traditional PDs require a specific amount of fault current to operate effectively. Nevertheless, they might not function properly when fault currents fluctuate as a result of disruptions or the sporadic nature of contemporary power plants [7]. Conventional protection methods are limited by the dynamic nature of microgrid operations, the growing number of DERs, and smart grid features. To enhance the adaptability and reliability of future energy systems, it is essential to comprehend historical changes, technological improvements, and practical challenges in MGs protection [8].

In recent years, scientists and engineers have put a lot of effort into creating more reliable and improved protection systems that are suited to the particular needs of microgrid situations. Additionally, a variety of innovative techniques are offered to enhance the resilience and efficacy of MGs' protection, including adaptive relay coordination algorithms, computational intelligence (CI)-based methodologies, optimal network topology, and distributed energy management systems (EMSs). Modern technologies that enable rapid fault detection, isolation, and restoration, like communication-enabled relays [9], synchro phasors [10], and intelligent electronic devices (IEDs) [11], have revolutionized MGs' safety. These devices increase the reliability and flexibility of microgrid operations by providing real-time data collection, critical analysis, and communication capabilities to enhance situational awareness through coordinated control actions [12]. Despite these advancements, there are still important research gaps in the protection of microgrids. Research and development are still ongoing in the areas of scalability, interoperability of various manufacturers' protection systems, and validation of communication protocol standardizing PDs under diverse operational scenarios. Furthermore, the growing danger of electromagnetic disruptions and cyber-physical attacks emphasizes the necessity of strong cybersecurity defenses as well as ongoing research and development in MGs protection [13].

Numerous review articles have covered a range of related subjects relating to MGs' protection devices, including the necessary circumstances, fault protection in grid-connected and islanded modes, microgrid protection structure, AC/DC protection problems, and suggested solutions. An extensive examination of hybrid AC/DC networks: perspectives on energy management, control, protection, and system planning is provided in [14]. The authors examine important facets of hybrid AC/DC microgrids, such as energy management, control tactics, optimization approaches, and protective measures. The integration of different energy sources, system stability and dependability, power distribution optimization, energy storage management, and online fault detection are all made possible by neural network-based optimization. The study highlights the benefits of hybrid AC/DC microgrids over traditional microgrids, especially the application of sophisticated control and optimization strategies and the use of interlinking converters for effective AC–DC power transfer. The authors of [15] discuss issues related to hybrid microgrids, the integration of AC and DC microgrids, their security and reliability, how to optimize power generation and load management in different scenarios, how to effectively handle uncertainty for renewable energy resources (RESs), and how to create hybrid microgrids that are affordable. Following a review of the design challenges of microgrid protection systems, the authors of [16] share some real-world experiences based on their own engineering, design, and field experience in addressing these challenges through a variety of approaches. Understanding all operational modes, configurations, and transitions is essential for designing microgrid protection systems. It's also critical to make sure that relays and controllers communicate quickly and reliably, especially in the event of a failure.

An overview of MG protection using converter-based resources (CBRs) is provided in [17]. This study proposes and uses a single test system to demonstrate all of the protection issues and the creative solutions that have been created to address the conventional protection systems' failure in MGs with CBRs. Additionally, the paper discusses the protection challenges of MGs with CBRs using the proposed test system. These challenges include the different modes of operation of MGs, changes in microgrid configurations, bidirectional current flow, different fault current levels observed by relays, and issues related to converter fault current characteristics. The authors of [18] covered the architecture of AC, DC, and hybrid MGs as well as associated protection concerns and potential solutions for both grid-connected and islanded microgrid operating modes. By classifying protection strategies into conventional, communication-based, and adaptive devices, the paper highlights the main challenges of microgrids, such as bidirectional power flow, intermittent

generation, variable fault current levels, and mode transitions. It also highlights the necessity of flexible, fast-acting, and scalable protection frameworks to keep up with the dynamic behavior of microgrids. Similarly, the authors of [19] offer a critical analysis of the problems and defenses for the DG-integrated AC microgrids. Considering the various connections and configurations, this study highlights the benefits and drawbacks of each protection plan as well as the obvious opportunities for any innovation in protection strategies to improve the security, dependability, and selectivity of AC microgrids. The study also focuses on incorporating smart devices and ways that make the existing protection mechanisms more intelligent and effective. In [20], an adaptive microgrid protection mechanism based on the communication system is thoroughly reviewed. The primary associated communication technologies and optimization strategies are thoroughly examined in this article. Additionally, a viewpoint on the future of communication deployments in MGs is provided, demonstrating the feasibility of multi-connectivity and 5G wireless systems to facilitate adaptive protection. Furthermore, the authors of [21] carried out a comprehensive analysis of adaptive protection of MGs, going over a range of relevant types, their benefits, and drawbacks. The latest research that uses computational intelligence to achieve adaptive defense is also reviewed. These technologies have the potential to revolutionize protection solutions globally with a more flexible and reliable approach. To help researchers and protection engineers discover microgrid protection difficulties and associated mitigation strategies, the authors of [22] provide a thorough examination and comparison of PDs and the difficulties in implementing them for various microgrid designs with a range of operational needs. To further illustrate the protection issues with MGs about various modes of operation, several simulation experiments were carried out. A comprehensive literature analysis on the state of the art and developments in the field of AC-microgrid protection is provided in [23]. The study includes the current state of affairs, significant obstacles, and ongoing research aimed at delivering a reliable relaying system in various MG operating situations. Additionally, the work focuses on evaluating the clever methods and tools that contribute to making the current security systems smarter. The survey's main goal is also to expand the researcher's database by adding pertinent references that may be very helpful for their future research.

Survey papers show that research on MG protection has changed significantly, moving away from static, inflexible methods and toward dynamic, adaptable, and flexible ones that better consider the changing characteristics of contemporary power networks. The increasing requirement to guarantee supply reliability, system stability, and the safety of PDs and the grid is making power system operation, protection, and management more difficult. The requirement is for a suitable self-adaptive protection system that adjusts its parameters in response to ongoing changes in the grid's configuration and system conditions. This study aims to critically examine the most recent PDs in AC microgrids, highlight issues related to microgrid PDs and appropriate solutions, examine various cyber-physical attacks and new trends to lessen their effects, and assess how well industry standardization for MGs protection is working. A brief overview of the evolution of microgrid PDs is also provided, covering their historical developments, technological advancements, and emerging contemporary trends in protective measures. This paper also adds to the current conversation on MG protection by integrating empirical data, a mathematical modeling equation, and real-world experiences to offer a useful understanding of the dynamics and complexity of AC microgrids' security. Here is a summary of the study's contributions:

- Outlines the chronological evolution and integration of various technologies over time to establish context and identify current research gaps in microgrid protection.
- Critically investigates the advancements in AC microgrids PDs, emphasizing mathematical modeling, associated challenges, and proposed solutions through in-depth analysis.
- Perform a case study, using the CERTS AC microgrid system that demonstrated the difficulties, problems, and fixes of every protection technique.
- Analyzes the technological challenges (cyber-attack and cybersecurity issues) currently faced by microgrid PDs and proposes solutions, with a particular focus on incorporating AI-driven mechanisms to enhance protection performance.
- Critically analyzes recent updates in standardization and regulation specifically related to microgrid PDs, to ensure reliable operation.
- Lastly, this study outlines the pertinent research directions to improve and make the PDs intelligent and self-adaptive.

II. EVOLUTION OF PROTECTIVE DEVICES

Protective devices are essential components of systems that demand a high degree of safety and reliability. Their development has coincided with the advancement of safety laws and technology. These devices are designed to detect, isolate, or reduce harmful events to prevent injury or system damage. Identifying kinds, establishing values, and situating protective relays and other devices necessary for a dependable and secure power system are all part of the coordination of microgrid PDs. Consequently, several difficulties have arisen as a result of DG integration into microgrids. The detection of distribution network flaws has become increasingly challenging due to high fault current levels, which traditional relays are not well-equipped to handle [24]. Furthermore, the network topology frequently changes when DGs are placed close to loads, and MGs can function in a variety of modes, including grid-connected and islanded, which can reduce the efficacy and jeopardize the dependability of relay-based protection. The new PDs, however, are more intricate. The development of PDs reflects the power system's evolution, the evolution of MGs' integration with the main grid, and the evolution of the

TABLE 1. Historical progression of protective devices.

Refs.	Evolutions	Periods	Devices	Applications	Purposes
[28]	Early grids and minimal protection	Late 19th century	Fuses, Mechanical circuit breakers, and Switches.	Generation, Transmission, Distribution, Substation, and Microgrids.	• Fuses protect equipment by stopping the circuit when high current flows. • When a fault happens, mechanical CBs allow the circuit to open and close. • The microgrids use manual switching devices to regulate the electrical flow, mainly to prevent interruptions.
[29]	Advancements in relay technology	Mid–20th century	Electromechanical relays	Microgrid systems, Power systems, and Industrial automation.	• In microgrid configurations, electromechanical relays significantly enhance the coordination and reliability of protection systems. • These relays use basic electrical elements like current, voltage, and frequency to effectively identify faults. • Electromechanical relays provide more versatile control capabilities, improved monitoring, and better integration with control systems.
[30]	Introduction of digital protection relays	Late 20th century	Digital protection relays.	Smart grids, Transmission, and Distribution networks.	• Digital relays transformed the electrical protection sector for both macro and micro power grids. • Using digital signal processing techniques, digital relays improved sensitivity and accuracy in fault detection and discrimination. • Digital relays facilitate smooth connection with other grid assets, including remote monitoring stations, SCADA systems, and control systems.
[31]	Integration of communication and control systems	Early–21st– century	Control and communication systems, including Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA).	Microgrid systems, Transmission network, Industrial automation.	• SCADA systems provide real-time monitoring, control, and data collection, serving as the central nervous system of microgrid networks. • The integration of control and communication systems enabled microgrid networks to operate effectively and reliably while managing communication protocols. • In microgrid networks, PLCs served as control units, carrying out protective tasks, device coordination, and control logic.
[32]	Development of smart grid technology and DERs	Mid–21st century	IoT devices such as intelligent relays/switches, Smart meters, and Reclosers.	Smart grids, DERs, Networking, and securing systems.	• To ensure the stability, dependability, and resilience of the grid, new PDs are needed as smart devices in the electrical system evolve. • Intelligent relays with complex algorithms and communication capabilities are examples of advanced microgrid PDs that guarantee the microgrid's voltage and frequency management.
[33]	Deployment of synchro phasor technology	Late 21st century	Phasor data concentrators (PDCs), Phasor measurement units (PMUs), GPS, and IEDs.	Wide area protection systems (WAPS), DERs, Smart grid, and Fault detection systems.	• Synchro phasor provides benefits such as improved stability in dynamic environments, increased safety awareness, and faster fault detection during microgrid operation. • The main advantage of synchro phasors is their ability to quickly and accurately detect faults in the microgrid network through voltage and current phasor analysis. • It also maintained high grid reliability and decreased outage time.
[34]	Combining sophisticated analytics with cyber-physical systems (CPS)	Present trend and potential future	Smart sensors, Cyber physical systems (CPS), Digital twins, Remote terminal units.	Smart grid, Energy systems, Autonomous vehicles, Cybersecurity.	• The system is made more resilient by utilizing CPS, AI, and sophisticated analytics in MGs, which allow for quick identification and reaction to equipment malfunctions, cyberattacks, and grid problems. • Microgrid protection systems create vast amounts of data, which require analysis using advanced analytics and AI approaches. • To safeguard vital infrastructure against cyberattacks and unwanted access, cybersecurity solutions such as encryption, authentication, intrusion detection, and secure communication protocols are also implemented.

grid architecture. Table 1 shows the development of PDs over time to the advanced device configurations of today [25].

Historically, protection systems were made to be as simple and economical as possible, with distribution systems usually consisting of fuses, circuit breakers, reclosers, and overcurrent relays. These systems flowed power in a single direction and had a radial architecture. If the current is over a predetermined threshold, overcurrent relays would trip the circuit breaker; if the current exceeded a predetermined value, fuses would melt and stop the power flow. Reclosers, which have two reaction levels—fast and slow—would automatically re-energize a distribution circuit once a temporary problem was resolved, restoring electricity. However, for self-sufficient distribution systems, such as MGs, these protections are no longer adequate. In distribution systems, the effect of high DG penetration on the widely utilized overcurrent (OC) relay is one of the primary problems with relay detection procedures. It becomes challenging to decide whether studies are necessary because new DGs are frequently activated without prior notification [26], [27]. Therefore, the current protection mechanisms need to be improved to guarantee adaptation to the changing structure and operational conditions of distribution systems.

III. AC MICROGRID PROTECTION DEVICES

AC microgrids are a complicated problem because of the network's dynamic nature, which includes (a) the ability to switch between grid-connected and islanded modes of operation, (b) the ability to flow power in both directions, and (c) the integration of intermittent RESs with real-time changes in resource availability. As a result, the fault current contributions may differ significantly based on the network's event conditions. All distributed energy resources (DERs) and AC loads are connected via AC buses in an AC microgrid. With converters, which are used to convert electricity from DC to AC, DERs that produce DC power can be connected to AC buses. The load is connected to the AC bus via a transformer, which also supplies the required voltage level. Transformers and CBs connect the AC bus and the AC utility grid at the point of common coupling (PCC). As shown in Fig. 1, the purpose of the PDs is to safeguard transformers, power converters, load side devices, DERs, and ESSs [17]. Problems with protection in an AC microgrid can be roughly classified into two groups: problems with protection when the microgrid is running in its islanded state and problems with protection when it is connected to the grid. Erroneous tripping at isolation devices, CB reaction time at the microgrid and utility grid PCC, re-synchronization, and the speed at which the microgrid and utility grid are reconnected after the issue has been resolved are some of the protection challenges in the grid-connected operating mode. In islanded mode, the complexity of the microgrid dictates the speed at which PDs react to events. When the overcurrent protection relays' response time is longer than necessary, the main goal of the islanded operating mode is to lower the short-circuit current. Even though AC microgrids offer several benefits, controlling system stability during mode transitions and preventing false tripping are two of their main concerns. Appropriate PDs should be chosen for their speed, enhanced selectivity, flexibility, ease of use, novel configuration possibilities, and affordability to ensure the power system grid operates safely and reliably [35], [36].

Furthermore, the protection issues of MGs need to be addressed more thoroughly, and this section focuses more on the development of various PDs for AC microgrids. Additionally, it describes the setup, difficulties, current research trends with current solutions, and potential future applications for various PDs. The overcurrent protection device, voltage protection device, ground fault protection device, differential protection device, distance protection device, arc flash protection device, communication protection device, harmonic protection device, synchronization protection device, and adaptive protection device are various AC microgrids protection devices.

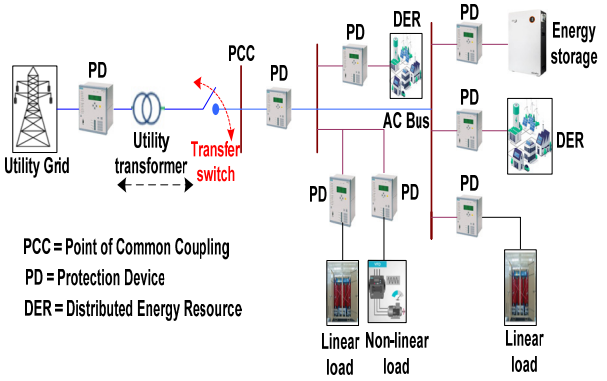

FIGURE 1. Typical AC microgrids PDs [17].

A. OVERCURRENT PROTECTION DEVICE

Designing PDs in a constant-voltage power system mostly relies on current dynamics, and integrating DER is more difficult. One of the most widely used protection system characteristics in distribution networks is overcurrent protection. Overcurrent protection is essential to AC microgrids because it can affect equipment and throw the grid out of balance, which could be dangerous. Isolating the error sections prevents cascade failures and broad outages, hence achieving stability [37]. The overcurrent protection relay operates on a fairly basic principle: it compares the current passing through the current transformer's (CT) secondary winding with a preset threshold (pickup current) to create and deliver the trip signal to the CBs. Nevertheless, there are particular difficulties in implementing it in AC microgrids that are not present in traditional power distribution networks. Traditional overcurrent PDs are not built to handle the complexity introduced by the decentralized and dynamic character of MGs, which frequently include RESs with inverter-based technology [38]. To coordinate Directional Overcurrent Relays (DOCRs) in microgrids, the

authors of [39] propose a Mixed-Integer Linear Programming (MILP) paradigm. Relay settings, such as Time Multiplier Settings (TMS) and characteristic curves, are optimized by the model to reduce tripping times while preserving selectivity. The model is formulated as an optimization assignment problem. The collection of offline settings for every relay is one of the choice variables. To minimize operating time across the specified scenarios while taking an adaptive function into account, a centralized controller determines the operating mode and transmits the settings to the relays. The decision variables are the TMS_{ic} for the relay's times of the available curve. The auxiliary variable x_{ic} allows the model to select a single curve for each relay, which allows the upper and lower boundary conditions to be set. When compared to employing a single standard, the integration of the IEEE and IEC standard curves improves coordination performance, which is a significant contribution. In order to establish common relay settings that are applicable to both microgrid operating modes, the authors of [40] suggest a novel optimal protection coordination system. The strategy allows for the best possible selection of conventional IEC-60255 relay characteristics by introducing a dual-setting directional overcurrent relay (DOCR) with an additional relay characteristic identifier (RCI). Optimizing relay settings and relay characteristics (RCI) results in the best possible coordination between the dual setting DOCRs. Relay operating time is minimized without violating any constraints by choosing the best values for each decision variable. Each relay is therefore linked to twice as many variables as in traditional DOCR. The relay is linked to forward settings for fault current flowing forward (TMS_{fow}, PS_{fow}, and RCI), and reverse settings (TMS_{rev}, PS_{rev}, and RCI) for fault current flowing backward. In this paper genetic algorithms (GA) and grey wolf optimization (GWO) are used to obtain the values of all decision variables, which are represented as a mixed-integer nonlinear programming (MINLP) model. The scheme's higher performance is confirmed on the distribution sections of the IEEE-14 and IEEE-30 bus benchmark systems. The authors of [41] propose an improved microgrid overcurrent protection method using the beetle antenna search (BAS) algorithm and fault acceleration factor, enhancing coordination between primary and backup relays. The study uses a compound fault acceleration factor to increase protection speed under fault conditions and provides a novel Time Dial Setting (TDS) for inverse-time protection. The inverse-time over-current relay (ITOCR), whose operation duration is inversely proportional to the fault current, can represent the severity of faults. The ideal configuration of the I-ITOCR's parameters is obtained by solving the nonlinear optimization issue of the problem using the BAS method. Because the BAS approach only requires one person, it significantly lowers computing complexity as compared to the particle swarm optimization technique. BAS evaluates the local areas' fitness and helps people get to the global ideal solution by using the local regions' optimal solution. The efficacy of the approach is confirmed by case studies in DIgSILENT/PowerFactory.

Bidirectional current flow, as opposed to classic radial systems' unidirectional flow from a central source, is one of the difficulties in protecting against overcurrent in AC microgrids. Fault identification in MGs is complicated by the several distributed generation (DG) sources that introduce different current injection sites. Due to the inability of traditional overcurrent relays to precisely detect the direction of the fault current, this bidirectional flow may result in protection device miscoordination. Fig. 2 illustrates this restriction by displaying the conventional relay coordination method. Protection design is made more difficult by the network topology heterogeneity brought on by frequent switching between grid-connected and islanded modes. Protection strategies must be adaptable and agile to account for this dynamic behavior. The microgrid's narrow and overlapping protective zones make it difficult to coordinate PDs [42]. Numerous methods are put forth and put into practice in sophisticated microgrid systems to overcome these issues. At the forefront are adaptive protection methods, which allow protection settings to be dynamically adjusted in response to changes in operating mode or network configuration [8]. The implementation of IEDs and directional relays improves fault detection accuracy by determining the direction of current flow, which enables more accurate fault isolation [43]. Furthermore, smart inverters with fault detection algorithms and current limitation capabilities can help protect the system by controlling fault currents and informing other system components of fault events [44]. In both grid-connected and islanded modes, the effectiveness of overcurrent protective devices in an AC microgrid is contingent upon appropriate coordination, adaptive settings, and the capacity to react to fluctuating fault levels.

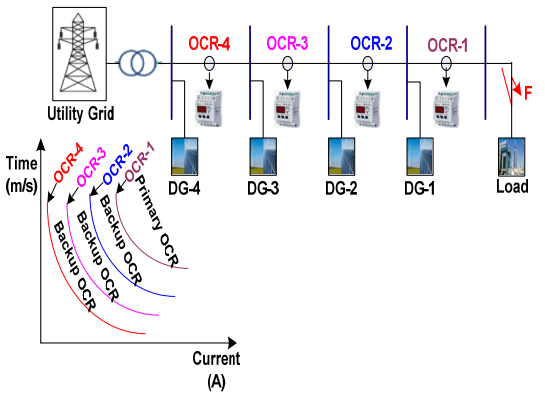

FIGURE 2. Conventional protective relay coordination [42].

B. VOLTAGE PROTECTION DEVICE

Voltage protection is a crucial component of AC microgrids that ensures the electrical system's dependability and

integrity. To protect power system equipment and preserve quality, it is made to function in response to variations in voltage. Additionally, it is essential to grid stability since it keeps voltage levels within reasonable bounds, which is required for the best possible system performance without compromising stability. The integrity and effectiveness of the AC microgrids are guaranteed by voltage protection, which also enhances power quality by lowering voltage oscillations and fluctuations. However, maintaining steady voltage levels becomes difficult since MGs are dynamic and decentralized [45]. To prevent harm on the load side, the authors of [46] identify the development of an undervoltage and overvoltage protection. Unexpected increases in load brought on by system defects are typically the cause of voltages below the rated value. When a circuit with a subpar or broken voltage regulator experiences a fast drop in load, the voltage rises above the rated levels. The proposed method, which is demonstrated in the study, uses a step-down transformer to lower the 230 V AC supply to 12 V. A bridge rectifier corrects this voltage, and a capacitor filters it to create a steady DC output. A comparator circuit (IC LM324) that tracks voltage levels is then given a steady DC supply by a voltage regulator. The regulated DC output is compared to predetermined upper and lower threshold values by the comparator. To prevent harm to delicate appliances, the comparator activates a relay that disconnects the load in the event of an overvoltage or undervoltage condition. To protect linked devices, the system thus makes sure that it automatically disconnects during abnormal voltage situations. A novel voltage-based relay for microgrid protection is suggested in [47]. Within a designated protection zone, the relay uses active power differential and sensitivity calculations based on voltage measurements. The PMU measuring technology, the communication link, and the IED executing the protection algorithm are all integrated into the protection system based on the suggested algorithm. Inherent latencies result from the algorithm's processing time, the physical layer medium's propagation delay, and measurement reporting delays. This causes a delay in fault identification since the IED receives the local PMU data before the data from the remote PMUs. The synchronized voltage readings from the nearby and local nodes are fed into the IED that is executing this algorithm via PMUs. For an accurate assessment of the relay travel time once a problem occurs, the latency must be described. To evaluate the relay's performance under various fault scenarios, it is modeled in Dig SILENT Power Factory and deployed at the nodes of a microgrid test system. In [48], the authors examine voltage-based protection and suggest ways to improve an existing method to make settings simpler and increase selectivity and dependability. The study establishes and modifies the plug setting multiplier (m) and time dial setting (TDS) for primary and backup direct power flow relays in both grid-connected and islanded microgrid scenarios, guaranteeing appropriate coordination with a 200 ms coordination time interval (CTI); in the islanded mode, the backup relay parameters (m) are decreased, and reverse relay settings are established for three-phase faults at the PCC considering all operating DERs. The comparative study demonstrated the superiority of the enhanced approach over the other two analyzed methods because the Jamali Voltage-based Protection (JVP) method failed to achieve protection security for multiple operating scenarios, and the conventional overcurrent is limited to fault current amplitudes. Failure resistance was used to differentiate the success rates of the JVP approach, which was tested for the same six scenarios. The sympathetic trip is avoided by the Enhanced Method (EM). This enhancement was made possible by the fact that the relay starter of the EM is dependent on the fault current, which the relay current does not surpass. The findings show that the updated strategy performs better than both the original technique and conventional overcurrent protection in a variety of AC microgrid topologies. Fig. 3 illustrates a voltage-based protection device using a communication link. The protection device operates in two steps: First, the a-b-c frame of the supply voltage is converted to the d-q frame. The second stage involves calculating the disturbance signal (VDIST), which represents the supply voltage divergence from a reference, using the disturbed d-q values. A larger disturbance is indicated by a higher VDIST. The device uses upper and lower limiters, hysteresis comparators, and low-pass filters (LPFs) to increase the sensitivity of fault detection [49]. Microgrid voltage protection is difficult since DGs like solar PV and wind have variable outputs that might lead to dangerous voltage swings.

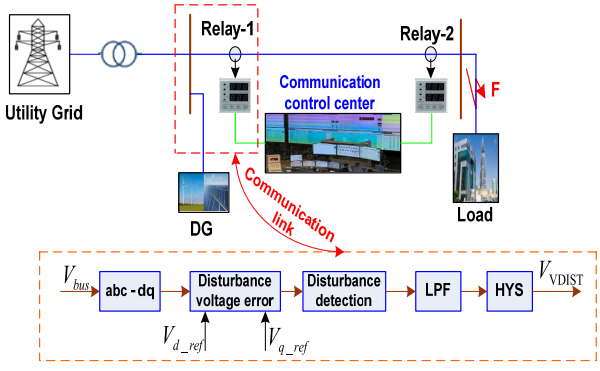

FIGURE 3. Voltage-based protection device using communication [49].

Grid-connected and islanded mode transitions can also cause voltage transients. Effective methods rely on controllers and protection units communicating in real time, and PDs must detect these events accurately without false tripping. Furthermore, real-time communication between controllers and protection units is essential to voltage PDs. Communication breakdowns or delays may make the protection system less reliable [45]. Numerous approaches have been put forth to overcome these issues. Using peer-to-peer communication-based protection mechanisms and

local intelligence reduces the voltage protection latency and increases dependability [50]. PDs are becoming more and more equipped with adaptive settings that react to instantaneous changes in load, DGs, and network architecture. Additionally, this keeps protection effective even under a variety of operating situations [51]. Grid resilience can be increased, and needless tripping can be avoided with voltage riding capabilities. Furthermore, by integrating an Energy Management System (EMS), voltage PDs can use real-time monitoring and predictive analytics to adjust to variations in load [52].

C. GROUND FAULT PROTECTION DEVICE

Protection against ground faults is essential to the secure and dependable functioning of AC microgrid systems. Early problem detection and line isolation are its main responsibilities to protect infrastructure, power system workers, and equipment. This improves system dependability by reducing the likelihood of prolonged outages brought on by early ground faults. Ground fault PDs are essential for operational safety and dependability because they prevent electrocution. In compensated distribution networks, cable insulation failure is usually decisive, making the self-extinction strategy for arcing ground faults in cable lines less effective than in overhead lines. The arc self-extinguishes during the current zero-crossings, but when the instantaneous phase-to-ground voltage increases above the damaged dielectric withstand threshold, the damaged insulation fails again. Consequently, a re-striking fault occurs. Faults that self-clear and become recurring due to permanent insulation failure are known as re-striking faults. Many utilities trip when a ground fault is detected by the protection device without cutting off cable distribution lines. The Petersen coil control system can also be modified to incorporate residual current compensation. The re-striking mechanism is lessened by this technology, which zeros out the ground fault current [53], [54].

In different grounding systems, a single line to ground fault, including HIFs, causes a low magnitude fault current. Zero-sequence quantities are commonly used as the basis for ground fault detection techniques. An extremely low magnitude is the zero-sequence impedance of a grounded system. This low value allowed for the evaluation of single line-to-ground faults to concentrate on the positive- and negative-sequence impedances without suffering a major loss of accuracy. Fig. 4 (a and b) depicts the forward and reverse ground faults in about zero-sequence [54]. In a forward ground fault, the relay measures V_0 across XC_{0L}. The primary current I_0 flows in at the CT polarity mark. At the relay location, $\theta_{L0} = 90^0$ and forward fault of $Z_0 = +XC_{0L}$. Where, V_0 = Zero-sequence voltage; I_0 = Zero-sequence current; Z_0 = Zero-sequence network; XC_{0L} = Zero-sequence capacitive reactance; and θ_{L0} = Line zero-sequence impedance angle.

$$V_0 = -I_0 \times (-jXC_{0L}) \tag{1}$$
$$V_0 = jXC_{0L}I_0 \tag{2}$$

During reverse ground fault, the relay measures V_0 across the series combination $Z_{0L} - jXC_{0L}$, and the current I_0 through the same series combination. For this reverse fault, the primary current I_0 flows out of the CT polarity mark. At the relay location, $XC_{0L} \gg Z_{0L}$. Typically, $Z_0 = -XC_{0L}$. Where, Z_{0L} = Zero-sequence line impedance and XC_{0L} = Zero-sequence capacitance of the protected line.

$$V_0 = I_0 \times (Z_{0L} - jXC_{0L}) \tag{3}$$
$$V_0 = -jXC_{0L}I_0 \tag{4}$$

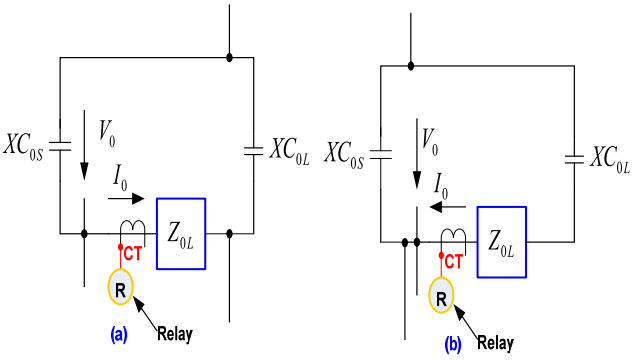

FIGURE 4. Zero-sequence network: (a) forward ground fault, (b) reverse ground fault [54].

Due to their low current generation, ground faults with high impedance in AC microgrids—such as arcing faults, faults via soil, or faults through wet insulation—may escape unnoticed by conventional PDs. Traditional PDs might not work correctly during islanded operation because the utility grid isn't there to serve as a fault reference. It is necessary for ground fault detection to adjust to both islanded and grid-connected modes. When there are both phase and ground faults, the microgrid's healthy sections are unnecessarily disconnected due to a lack of selective tripping. Also, managing grounding across interconnected nodes is a technically challenging task when dealing with several dispersed generators. Numerous methods are suggested since adaptive protection in real-time data can change settings dynamically according to DER status, failure history, and operating mode [55]. Insulation monitoring devices in impedance-grounded systems can continuously check insulation resistance and identify ground defects or deterioration before hazardous levels are reached [56]. In a dynamic MG system, devices that connect to central controllers via IEC 61850 are necessary for precise ground fault detection [57].

D. DIFFERENTIAL PROTECTION DEVICE

Modern power system protection tactics are based on differential protection, which monitors the difference in electrical quantities across a protected zone to identify and isolate failures. An imbalance in the currents or a difference that is beyond a predetermined threshold indicates a malfunction in the protected zone. One of the most dependable PDs for MGs

in power systems for safeguarding transformers and transmission lines is differential protection. This is due to differential PDs, which only identify a defect if the currents entering and exiting the component being protected do not match. It allows the faulty area to be tripped quickly and selectively while maintaining system functionality. This plan is straightforward, economical, and simple to execute. In power systems, it is commonly utilized. The test process shows that the fault current swings regardless of whether there are MGs or changes in the DG state. It is also very selective and provides great fault resistance. To preserve the safety and security of the power system and power engineers, differential protection enables defects to be identified considerably more quickly and stops cascading failures [58], [59]. In Fig. 5, the schematic for differential-based PDs with a communication link is displayed. To convey data promptly, differential protection requires reliable communication between the ends of the equipment that has to be protected. The primary CT may be instantly informed of any internal faults thanks to this reliable connection, which guarantees maximal selectivity and timely preventative measures [60].

In order to account for sequence-component extractor delays and fault current harmonics, the authors of [61] propose a current differential protection (CDP) strategy for distribution networks using inverter-interfaced distributed generators (IIDGs). In the study, the dynamic behavior of the IIDGs considering the sequence-component extractor based on the Pade's approximation is described, where the T/4 delay extractor of the IIDGs generates a two-stage behavior in the fault transient process. Because of its great sensitivity and selectivity, the CDP principle is frequently applied in contemporary DNs. The start-up criterion is the current version. According to the Prony approach, protective relays at two terminals obtain the necessary transient electric quantity after being picked up. The frequency-characteristic ratio (FCR) is designed to modify the constraint coefficient adaptively. In DNs with IIDGs, the problem of relays tripping falsely or failing is finally addressed by implementing a protective criterion based on FCR. In summary, the T/4 delay sequence component extractor will play a role in the two-stage behavior of the IIDGs fault transient process. High accuracy (<0.1 %) and robustness across a range of fault circumstances are demonstrated using PSCAD/EMTDC simulations on a 10kV network, which makes the scheme appropriate for both IIDG-integrated and traditional networks. Furthermore, the authors of [62] suggest an adaptive wide-area current differential protection system based on multiple agents, in which an expert system is used to dynamically establish the primary and backup zones. The study portrayed every relay in the network as an independent agent that could coordinate and communicate with nearby agents over a common communication infrastructure. The multi-agent system (MAS) was equipped with an expert system that allows it to dynamically generate primary and backup protection zones based on real-time system variables, including topology changes, loading, and fault locations. Zone borders and relay responsibilities were regularly updated by the expert system using a set of adaptive rules and decision logic. In these zones, predictive self-healing techniques guard against malfunctions, and relay agents collaborate to provide differential protection. Simulation results show that the suggested adaptive wide-area protection system is reliable and effective when compared with conventional differential protection methods. Differential PDs still faced some difficulties, like non-uniform and current profile fluctuation because of numerous DER modifications, as with any protective system. This leads to false trips and makes calculating the differential current more difficult. The differential protection technique necessitates synchronized current measurements from both ends of the protected zone, as traditional differential relays struggled in situations including bi-directional power flow and communication latency [63]. According to contemporary suggested solutions, newly developed differential PDs are outfitted with adaptive logic and digital signal processors (DSPs) to dynamically modify protection settings in response to load profiles, network configuration, and DER status [64]. Protocols like IEC 61850 with the Global Positioning System (GPS) guarantee precise and dependable transmission of current measurements between relay endpoints when time-based synchronized communication is used [65]. Combining inverter control logic with smart-based protection enables real-time coordination and supports the decision-making of differential relays. Furthermore, differential protection can be improved by using real-time operational data from the EMS to estimate the likelihood of faults and dynamically modify thresholds [61].

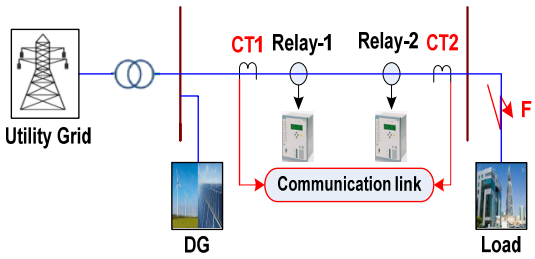

FIGURE 5. Schematic for differential-based protection device [60].

E. DISTANCE PROTECTION DEVICE

Distance protections rely on apparent impedance; they can be Mho, quadrilateral, polygonal, or other forms, and their properties are typically displayed in the R-X plane. These PDs use voltage and current measurements at relay points. The current and voltage phasors at a relay point are represented mathematically in numerical relays, which are used to offer distance protection. The relay trips and sends a signal to the CBs if the current value is different from the predicted level. To identify the location of the fault and the faulted portion within the protected zone, distance protection's targeted tripping is crucial [66]. Distance protection guarantees quick operation, reduces outages, and lessens the system's overall impact.

Furthermore, distance safeguards can be modified to meet the requirements of an AC microgrid based on the microgrid system's specific relay settings and characteristics. Relays that operate based on the distance of a line fault are known as distance relays or impedance relays. More precisely, the relay's ability to function depends on the impedance between the relay and the failure location. Impedance-based protection distinguishes between faults and loads in distribution networks, guaranteeing network stability. For distance protection, however, relay-to-relay communication is typically not necessary [67].

The three distance protection relay zones—Zones 1, 2, and 3—are shown in Fig. 6. Zones 2 and 3 are time-delayed and overrun onto neighboring lines, whereas Zone 1 operates without delay and covers 80 % of the protected line. As backup protection, Zone 3 provides extra security against ambiguous or unreported flaws and extends coverage to adjacent sectors [68].

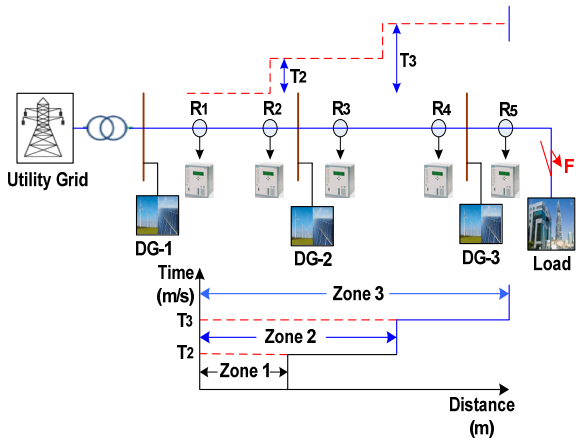

FIGURE 6. Three zones of distance protective relays [68].

In [69], the authors investigate distance relays and use the wavelet transform (WT) approach to identify errors. Wavelet analysis is frequently utilized for signal processing that can be successfully applied to overcome the challenges of traveling wave protection methods. The low and regulated current contribution from inverters can result in imprecise fault distance estimation, as distance protection depends on precise line impedance measurement. When network topology changes, system impedance changes as well, influencing zone settings and making static distance protection settings useless. Due to variations in power flow, distance relays intended for unidirectional systems in AC microgrids may misread directionality, resulting in improper tripping decisions or failure to detect failures. In fault conditions that change quickly, coordination problems might arise from overlapping zones and changing relay settings. Furthermore, the suggested technique allows for more precise problem detection by utilizing real-time data to dynamically modify settings via an intelligent relay [70]. Compared to standard distance relays, pilot protection and traveling wave techniques provide quicker and more precise fault detection in crucial microgrid portions. In addition, hybrid techniques that include multi-function relays enable redundancy and improved coverage of all fault types in a variety of operating modes [71].

F. ADAPTIVE PROTECTION DEVICE

Adaptive protection is described as "an online activity that uses externally generated signals or control action to modify the preferred protective response to a change in system conditions or requirements promptly." The implementation of an adaptive protection plan for microgrids requires digital relays and communication infrastructure. In addition to having many setting values, digital relays should be able to sense the current direction. The adaptive protection device enables real-time protection setting modifications in reaction to external changes in the power supply. This guarantees the dependable operation of the entire grid by enabling power system operators to react to changing conditions swiftly and efficiently [72]. Similarly, adaptive protection automatically modifies relay settings and protection functions in response to variations in power conditions. This is done to promptly protect the power system from any potential faults or overloads, ensuring its safety and dependability. The system is continuously monitored and updated in adaptive protection systems since changes are made automatically. However, the majority of adaptive protection systems need to interact with outside parties to detect changes in power system circumstances. The additional advantage of an adaptive protection mechanism is its ability to promptly identify any malfunction or disturbance in the MGs and take appropriate action to avert any major failures [73]. Communication-based adaptive protection and local information-based adaptive protection are the two main categories of adaptive protection. In [74], the authors suggested an adaptive protection method for islanded microgrids that relies on non-communication and voltage-restrained overcurrent protection. The study's approach did away with the necessity for communication links between relays by dynamically adjusting relay settings based on locally detected voltage and current signals. The adaptive algorithm adjusted the time dial and pickup current settings in response to changes in voltage during fault events. Under various load and fault impedance situations, the scheme increased the sensitivity of fault detection by integrating voltage dependency into the relay function. The approach, however, was only tested on small-scale islanded systems, a microgrid model in the time domain. Several fault scenarios, including single-line-to-ground, line-to-line, and three-phase faults, were simulated to assess the relay response and the coordination between primary and backup protection devices, ignoring the complexity of bigger or grid-connected microgrids with different fault levels and bidirectional power flows. To provide selectivity, sensitivity, and dependability across a variety of operating situations and during transitions between islanded and grid-connected modes, this highlights a research gap in the development of scalable adaptive protection systems. In [75], the

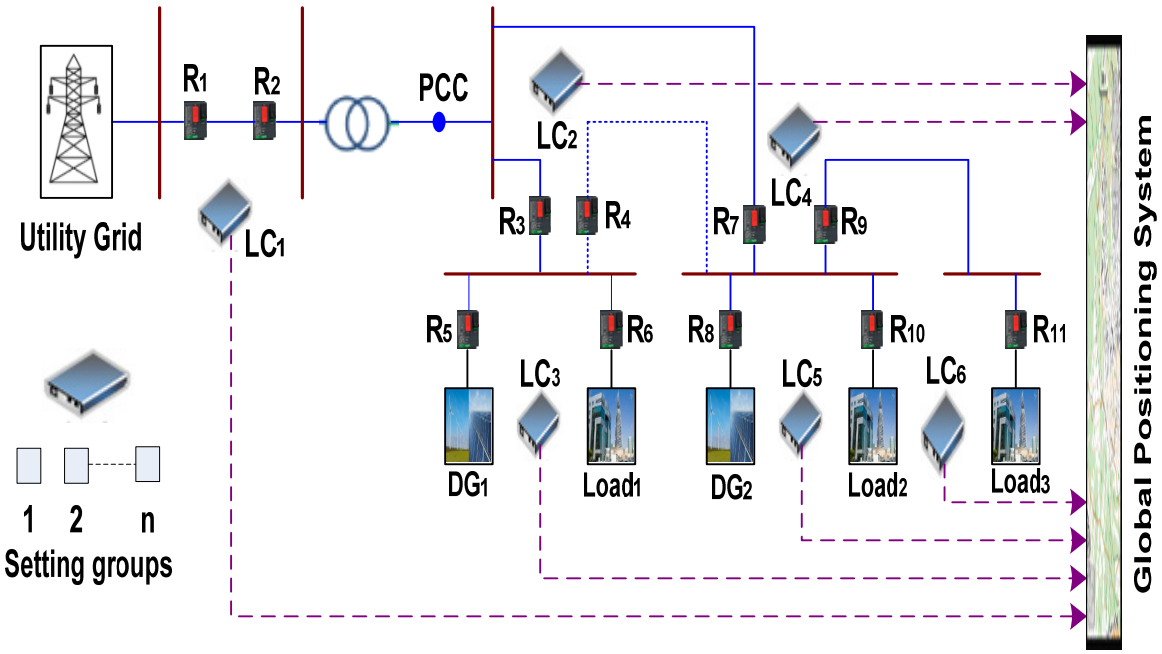

FIGURE 7. Decentralized adaptive protection device for microgrids [76].

authors propose a coordinated adaptive protection approach for AC microgrids that adapts the settings of PDs according to operation modes and system situations. In the initial phase of the suggested adaptive algorithm, an offline environment will be used for the isolation, coordination, and selective and sensitive fault detection of the suggested protective modules. When the suggested algorithm in the online stage detects a change in the system, a new set of settings for the suggested modules will be made to adjust the settings appropriately. Selective, sensitive, and adaptive criteria are met by adapting a new set of settings in this way to provide a quick and dependable functioning. For both the grid-connected and islanded modes of operation, the coordinated time delays and the pickup current (Ip) and time multiple settings (TMS) of directional over-current relays are computed offline for the suggested protection strategy. An online adaptive protection strategy is then suggested to identify various fault kinds in various places. According to simulation studies, faults can be detected and isolated under a variety of fault circumstances quickly, selectively, and cooperatively. The two components of communication-based adaptive protection are decentralized and centralized. Data is gathered and processed from the network by a base station or central server, which is part of the centralized component. To the central controller, each local controller transmits its current state. Every local controller is in charge of alerting the central controller to events that take place in their area. Data generation and transmission are the responsibilities of each node in the decentralized segment. To identify the problematic areas and determine the direction of the fault current, each local controller may speak with its neighboring local controllers (LCs). Each local controller may communicate with its adjacent local controllers to find the direction of fault current and to isolate the faulty sections. Each local controller is equipped with the necessary intelligence and information to react upon any contingency in the system. Every LC is armed with the knowledge and insight needed to respond to any system interruption. As a result, these two components cooperate to guarantee the network's dependability and security. Fig. 7 illustrates a decentralized adaptive protection approach for microgrids [76].

Although adaptive protection devices with numerous setting groups operate quickly and reliably, there are still gaps in the optimization of relay characteristics and high-set relays (HSRs) while lowering limitations. To find the best solutions for directional overcurrent relays (DOCRs) and HSRs, the authors [77] proposed an optimized adaptive protection coordination of microgrids by dual-setting DOCRs considering different topologies based on limited independent relays' setting groups. According to the study, the dual-setting curve model can help meet the coordination restrictions in different MG states. Selecting the proper levels or components of this relay type does not require communication links between protective relays. According to a breakpoint, the relay working curve is split into two sections (levels), and current and time settings can be chosen independently for each section. Utilizing an adaptive protection method, the optimization factors are employed in accordance with the technical demands of the DS features. There is a limit to how many setting groups can be used with DS-DOCRs in the suggested approach. When the suggested method was applied to the IEEE 30-

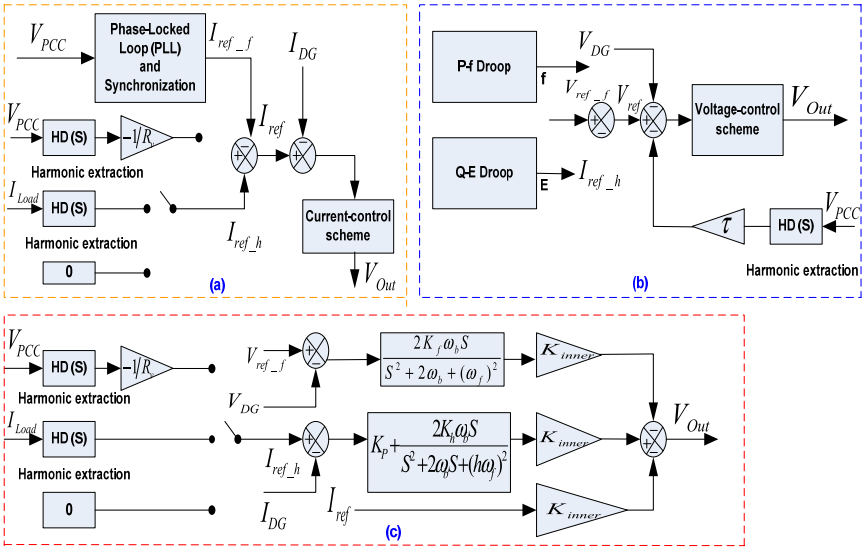

FIGURE 8. Harmonic compensation strategies in microgrid topologies: (a) CCM, (b) VCM, and (c) HCM [81], [82].

bus test system's distribution network, the findings showed that, in comparison to DS-DOCRs, the adaptive protection scheme's speed could be increased by approximately 46.26 % via relay curve type and BP optimization. In [78], the authors employed adaptive methods that have two relay configurations: one for the grid-connected mode and another for the islanded mode. Through constant monitoring of the microgrid's topology and operational state, a main controller in the study managed the adaptive process. The controller communicated in real-time with local relays via a specialized communication protocol and infrastructure. To guarantee smooth adaptation of protection parameters, the controller activated the relevant relay setting group upon identifying a mode transfer or network reconfiguration. The microgrid's current configuration was determined by the relays using topology-sensing techniques, and all protective settings were synchronized and verified by the main controller. Similarly, an intelligent adaptive protection strategy for AC-MGs is proposed in [79], which highlights the potential of adaptive neuro-fuzzy inference systems (ANFIS) and artificial neural networks (ANNs) along with a discrete wavelet transform-based signal processing technique. According to the operating conditions of the system, the adaptive protection system (APS) is thought to be able to adjust the fault reaction. Its incorporation with clever strategies is known to enhance the approach's accuracy and response time. These methods show how the suggested methodology can be used to improve system security and efficiency through the creation, testing, and assessment of protection mechanisms. Given that the DWT-based ANN approach for fault classification has been found to have superior classification accuracy under a variety of abnormalities and noise conditions, it can be integrated with an intelligent trip sequence generation approach that can manage measured characteristics and the rate at which those characteristics change. This is accomplished by combining the fault identification and classification approach with ANFIS. The system's defect is kept consistent throughout the simulation period to effectively examine its effects. The findings support the effectiveness of the suggested methodology, promoting the use of AI-based defense tactics for AC-MGs and laying the groundwork for a more resilient and sophisticated defense system. For communication between the relays and the main controller, this adaptive device chooses the relay communication protocol and communication infrastructure. By sensing the microgrid's topology and communicating with the main controller, the relays update the parameters.

G. HARMONIC PROTECTION DEVICE

Nonlinear loads in the network cause distortions in voltage and current known as harmonics. When integrating DERs, harmonics are one of the most important problems. Following IEEE standard 519-2014, a low-voltage system must be examined harmonically if the PCC has a total harmonic distortion (THD) of greater than 8 %. Modern relays can be used to control the system's harmonics by measuring THD at the inverter terminals. The system's efficiency can be considerably increased by managing the harmonics. At the PCC and the location of their production, harmonic reduction is possible [80]. In microgrid topologies, harmonic compensation is accomplished primarily through three methods: the hybrid control method (HCM), the voltage control method (VCM), and the current control method (CCM). A harmonic correction technique based on CCM is shown in Fig. 8(a). The fixed reference used in the technique is proportional and resonance-regulated. The CCM controls the output current in

line harmonic compensation with minimal harmonic distortion. The current reference (I_{ref}) is calculated as follows:

$$I_{ref} = I_{ref\_f} + I_{ref\_h} \tag{5}$$

$$I_{ref} = I_{ref\_f} - H_D(s)\frac{V_{PCC}}{R_v} \tag{6}$$

Where, I_{ref_f} is the base current reference, I_{ref_h} is the harmonic current reference, R_v is the equal network resistance in harmony frequency, and $H_D(s)$ represents a harmonic determinant for the extraction of harmonic voltage. Similarly, the VCM-based harmonic compensation approach is shown in Fig. 8(b). By creating a high harmonic impedance at the system output in a more challenging manner, this technique offers harmonic compensation. Here, a feed-forward term (τ) is used to change the voltage reference.

$$V_{ref} = V_{ref\_f} + V_{ref\_h} \tag{7}$$

$$V_{ref} = V_{ref\_f} - \tau H_D(s) \times V_{PCC} \tag{8}$$

In this equation, $H_D(s)$ is the voltage detector, τ is the gain of the forward feed term, assuming the gain is -1 for CCM with VCM compensation strategies. With HCM, voltage and current harmonics can be controlled simultaneously. By varying the filter capacitor voltage, this technique regulates the system's output power. The compensatory technique for HCM is shown in Fig. 8(c). It can therefore be defined mathematically as follows: First, the first term is a closed-loop term that represents the fundamental capacitor voltage; second, it represents the DG line harmonic current; and third, it represents an active damping term [81], [82].

$$V_{out} = G_{power}(s)\left(V_{ref\_f} - V_C\right) + G_{harmonic}(s)\left(I_{ref\_h} - I_{DG}\right) + G_{damping}(s)I_{load} \tag{9}$$

The key distinction between the three harmonic compensation techniques is that, whereas VCM is highly sensitive to variations in network impedance, CCM and HCM are less susceptible to feeder impedance changes. The growing prevalence of converter-based DG has raised the levels of harmonics in MG topologies. In the presence of weak grid conditions, the harmonic and resonant properties of a multi-inverter grid-connected system can adversely impact power quality. In [83], the authors examine the resonant and harmonic properties of grid-connected systems with multiple inverters under weak grid scenarios. First, the study models the inverter's harmonic currents, verifies the accuracy of the high- and low-frequency harmonics in a closed loop, and examines the features of the harmonic currents as the parameters change. Second, a multi-inverter grid-connected equivalent model based on the triple-decomposition conductance is constructed and evaluated in conjunction with the resonant modal analysis approach using the resonant characteristics of the inverter with feed-forward connection. Next, an impedance reshaping method for harmonic resonance is suggested. This method uses improved weighted average current control (WACC) to suppress background harmonics, the point of common coupling (PCC) paralleling the virtual conductance method to suppress system resonance, and an impedance reshaping resonance suppression method to improve the system's stability margin. Lastly, simulations and data comparisons with various suppression techniques confirm the superiority and efficacy of the suggested approach. Additionally, the authors [84] suggest a method for estimating harmonic impedance that uses OPTICS clustering and similarity metrics to increase estimation accuracy. The harmonic comprehensive contribution and total harmonic contribution indices are introduced in the study using a subjective analytic hierarchy technique to facilitate evaluation. Harmonic sources from both the utility and customer sides typically produce the harmonics at the PCC. The Thevenin equivalent circuit is shown with the concerned customer as the customer side and the other components as the utility side. To lessen the impact of outliers, the harmonic impedance of the filtered and clustered data is estimated using the complex domain robust regression approach. The findings of the contribution evaluation are not comparable since the harmonic voltage evaluation index and the harmonic current evaluation index assess harmonic contribution from two distinct angles. According to simulations, the technique lessens the impact of utility impedance variations and background harmonic voltage fluctuations, resulting in more precise impedance estimates and efficient harmonic contribution evaluation.

H. COMMUNICATION PROTECTION DEVICE

A communication network system can be used as a protective tool for MGs to modify the tripping characteristics and dynamically update the settings in real-time. Also, the device is used to monitor and adjust the relay setting based on the dynamic features of the MG's system configuration. In MGs, communication-based PDs offer various benefits, including immunity to external loading conditions, efficient handling of high-impedance faults, support for bi-directional power flow, adaptability to different operating modes, and suitability for looped network configurations. Communication systems can reconfigure the system during abnormal operating conditions. These protection techniques utilize information such as voltage, current, phase angles, and direction to exchange permissive and blocking signals between relays. This information is used by relays to identify and fix errors. Peer-to-peer or network-based protocols require dependable, fast communication channels, such as fiber-optic or Ethernet networks, to function effectively [85]. In MGs, communication-based protection methods like Directional Comparison Blocking (DCB), Permissive Overreaching Transfer Tripping (POTT), Direct Transfer Trip (DTT), and Directional interlocking are frequently employed as primary protection. A slower backup mechanism, usually time-graded overcurrent protection with voltage or directional monitoring, is used to keep the system safe in the event of a communication loss [86].

To protect a variety of electrical equipment in both grid-connected and islanded modes, the authors [87] suggest a Centralized Intelligent Station-Level Protection (CISP) method for networked microgrids. The method dynamically determines protective zones and algorithms based on system topology and operational conditions by utilizing network theory-based zone selection and adaptive relaying, utilizing IEC 61869-9 Sampled Values (SVs) measurements and IEC 61850 GOOSE messages, intelligently determines the protection zones, and automatically selects the protection algorithms to use in each of the protection zones based on the prevailing system topology and operating conditions. The efficacy of CISP in a range of configurations, operating scenarios, and fault circumstances is illustrated by real-time RTDS simulations. A data mining technique was used by the authors of [88] to identify the best relay settings and configurations for microgrid security systems. Several zones within the microgrid cluster and the external electrical grid are covered by the suggested system, which handles a variety of irregular conditions such as conventional faults, high-impedance faults, islanding scenarios, and unfavorable events. The discrete Wavelet transform and the Taguchi methodology are used to create the suggested methodology. With this combination, Scalo-grams produced from the fault signals can be used to optimize the training of convolutional neural networks. Using communication-assisted digital relays, this technique chooses the most pertinent electrical characteristics to improve fault isolation and detection. By dynamically modifying relay settings in response to real-time data, the system enhances response times and protection coordination in microgrid scenarios. To provide the speed and dependability needed for different microgrid protection functions, such as bus, line, and anti-islanding protection, the authors of [89] emphasize the importance of communication-based protection systems. The study highlights the advantages of combining voltage, current, and temporal characteristics as a viable approach to addressing microgrid security issues. Strengthening microgrid security requires the development of autonomous systems like numerous agents, the advancement of communication technologies, and the incorporation of intelligent components like grids and inverters. Inverse-based protection coordination based on voltage, current, and time has the potential to improve coordination reliability and increase the sensitivity of fault detection. Thus, MGs can operate safely and effectively in a variety of operational situations because of these systems' quick fault detection and isolation capabilities. Through the utilization of cutting-edge communication technology, these protective strategies improve the general stability and resilience of microgrid networks.

I. ARC FLASH PROTECTION DEVICE

One of the most important features of AC microgrids is arc flash prevention, which shields workers and equipment from dangers. Arc flashes are a type of explosion that releases heat and thermal radiation, which can cause massive burns, severe injuries, or even death to workers in their path. Arc blast typically comes after arc flash. Electrical equipment may blow up as a result, and a plasma fireball may form. The temperature can rise above 35,000 °F as a result of this process. Arc burst might result from the intense pressure created by this high temperature, which could also quickly heat the surrounding air [90]. Arc flash results in flying shrapnel, pressure waves, fire, and blinding illumination. To identify anomalous currents or circumstances connected to arc flash occurrences, arc flash comprises current sensors, optical detectors, and arc flash relay units. PDs, such as arc flash relays or CBs, are tripped to open the circuit's defective segment and isolate it from the rest of the system when a fault situation is recognized. To reduce the impact of an arc flash incident, mitigation techniques such as arc-resistant equipment designs and arc flash barriers collect and divert energy. The safety functionality and adherence to regulations like IEEE 1584.1, OSHA 1910, and NFPA 70E [91] make arc flash protection crucial for AC microgrids. Using arc flash prevention devices lowers the likelihood of accidents in AC microgrids, in addition to ensuring a safe working environment for employees. The utilization of AC microgrids and the development of DER have recently increased interest in arc flash PDs. The device's design requires a thorough analysis and discussion of the difficulties.

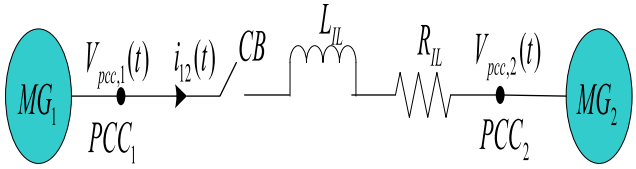

FIGURE 9. Schematic of synchronous MGs with a focus on PCCs [99].

To assist facility owners in creating efficient hazard management plans, the author of [92] provides techniques for assessing arc-flash energy levels. The approach comprised measuring and experimenting with arc-flash energy in a variety of industrial sites with varying equipment configurations and operating conditions. Electrical installations, including distribution boards, control panels, and switchgear assemblies, provided the data, with a focus on systems with significant short-circuit currents. Standardized arc-flash analysis techniques based on IEEE 1584 and associated industry standards were used in the study to calculate incident energy and identify the arc-flash boundaries for various fault scenarios. To determine how equipment design, installation procedures, and operational conditions affected the amount of arc-flash energy, the experimental findings were examined. To demonstrate the variation in outcomes among industrial settings, statistical comparisons of the measured data were conducted. By reducing the risks related to high-current electric arcs in industrial power systems, the findings improve worker safety and system dependability. In [93], the authors

show that using hybrid connectors as arc eliminators can mitigate the impacts of short circuits and arc faults by significantly reducing arc energy and arc length. Through the suppression of high-intensity sound waves, the limitation of temperature and pressure rise, and the prevention of material erosion, equipment damage, and the ejection of molten debris inside closed switchgear. In circuits impacted by an arc disturbance, experimental research has demonstrated that sections of antiparallel-linked thyristors acting as an electric arc eliminator can put out an electric arc with an intensity of 30 (kA) in less than 1 ms. The quantity of energy generated in the arc was greatly decreased by shortening the arc disturbance duration, which also greatly decreased the electric arc's dangerous effects. The authors of [94] offer suggestions for reducing maintenance risks as well as a technique for estimating arc flash incidence energy in mixed AC/DC systems, including PV power plants. The study demonstrates how we might lower the possibility of these negative outcomes for the employees of these power plants. A 300 kW PV power plant example scenario is modeled with all of its parts and current protection configurations. Utilizing a sophisticated smart protection software to coordinate protective devices, the power of the electric arc flash is assessed using the recommended analytical-simulation-based approach in accordance with IEEE 1584 standard. The appropriate PD settings will then be chosen for the staff's safety and the lowest arc power. Additionally, the authors of [95] look into how to calculate the incident energy of an arc flash for distribution overhead feeders that use DERs. To reduce the risk of arc flash, the efficiency of neutral grounding resistors and low-set instantaneous protection is investigated. Nine Dominion Energy distribution feeders that link solar inverters are used to assess how DERs affect arc flash incident energy. DER step-up transformer winding configuration, DER unintended islanding run-on time, and DER mega volt-ampere (MVA) capacity are among the elements considered. Variations in protection complexity and Short-Circuit Current Level (SCCL) present difficulties for arc flash PDs in AC microgrids. Early diagnosis is crucial because arc faults can cause damage and fire threats due to the high-power discharges they produce between conductors. In order to detect arc defects, the authors [96] proposed instrument transformers to measure voltage and current signals, decompose the voltage signal using a discrete wavelet transform, and apply a variety of machine learning classifiers. Discrete Wavelet Transforms (DWTs) were used in the study to break down the recorded voltage signals into various frequency components. To differentiate the transient behavior of arc faults from other disturbances or normal operating circumstances, this decomposition made it possible to extract important time-frequency properties. Following that, the collected characteristics were fed into a variety of machine learning classifiers, including k-nearest neighbors (k-NN), support vector machines (SVM), and decision trees. The best model for precise and quick arc defect detection was found by training and testing these classifiers on simulated data. The approach uses MATLAB/Simulink simulations to assess these classifiers' performance for microgrid arc failure detection. Metrics including accuracy, sensitivity, specificity, and reaction time were used to evaluate each classifier's performance, proving the viability of the suggested hybrid signal processing and machine learning method for microgrid arc fault detection.

J. SYNCHRONIZATION PROTECTION DEVICE

Synchronization is the process of reducing the voltage, phase angle, and frequency variations between an active grid and a voltage or current source. Sources of voltage and current can include power plants, DERs, and microgrids. To arrange DERs and the utility grid for safe and dependable operations, synchronization protection is essential for AC microgrids. Grid-feeding DERs and grid-forming DERs are the two categories into which synchronization processes in MGs can be divided. Grid-feeding DERs, as current sources, usually use phase-locked loops (PLLs) to synchronize with the grid, whereas grid-forming DERs and the islanded MGs, as voltage sources, require a more complete synchronization control unit to minimize voltage, phase angle, and frequency differences before connecting to the power grid [97]. Moreover, synchronization protection reduces the risk of over-voltage and under-frequency fluctuations, which lessens the possibility of cascading failures and a broad power supply interruption. It is the foundation for grid stability, equipment safety, and system reliability. The longevity of DERs and grid infrastructure is increased by this approach, which enables the identification of synchronization parameter failures before communication establishment. The primary component that contributes to ensuring the security and dependability of microgrid systems is synchronization protection, which makes it easier to connect DERs to the grid safely while reducing the likelihood of operational errors and the shutdown of vital loads. However, the rising usage of DER and dynamic load patterns in the current AC microgrids makes classic synchronization devices incompatible [98]. Fig. 9 presents a schematic of two synchronous MGs with a focus on the PCCs of MG_1 and the PCCs of MG_2 and the interlinking line between them. Considering the single-phase equivalent circuit of the interconnection, apply Kirchhoff's voltage law.

$$R_{IL} i_{12}(t) + L_{IL} \frac{di_{12}(t)}{dt} = V_{PCC,1}(t) - V_{PCC,2}(t) \quad (10)$$

where R_{IL} and L_{IL} are the resistance and inductance of the interlinking line, and $i_{12}(t)$ is the single-phase current from MG_1 to MG_2. Considering that the PCC's voltages are sinusoidal. Hence, $V_{PCC,1}(t) = V_{p1}\sin(\omega_1 t + \emptyset_{PCC,1})$ and $V_{PCC,2}(t) = V_{p2}\sin(\omega_2 t + \emptyset_{PCC,2})$. The equivalent current is expressed as: $i_{12,pr1}(t) = I_{pr1}\sin(\omega_1 t + \theta_1)$ and $i_{12,pr2}(t) = I_{pr2}\sin(\omega_2 t + \theta_2)$. The single-phase current from MG_1 to MG_2 is expressed as:

$$i_{12}(t) = \left(I_{pr2} sin(\theta_2) - I_{pr1} sin(\theta_1)\right)^{e^{-(R/L)t}} + i_{12,pr1}(t) - i_{12,pr2}(t) \quad (11)$$

TABLE 2. Issues and solutions of PDs in AC microgrids.

Devices	Issues	Solutions
Overcurrent protection device [42]-[44]	• Bidirectional current flow in the AC microgrids makes fault detection and isolation more difficult. • Variations in SCCLs impact the dependability of the device. • Limited fault contribution from inverters. • Relay desensitization in island mode makes it difficult for PDs to detect and isolate faults effectively.	• Integrated adaptive approach that is both adaptable and robust for real-time configuration and operating situations. • Using IEDs, a sequence component-based technique, is intended to mitigate faults and restore systems. • Combine overcurrent relays with additional requirements, such as differential protection or ROCOV. • Use communication-based control to lower relay pickup thresholds.
Voltage protection device [50]-[52]	• Changes in setup, load, and DER plugin-out provide difficulties for voltage PDs. • Voltage protection is made more difficult by distortion, noise, and harmonics. • Quick reaction to changes in load without requiring needless disconnections. • Voltage reference and measurement are made more difficult by numerous DERs and grid interface locations.	• Using cutting-edge voltage regulation methods to react swiftly to RES variations. • Reduced distortion and harmonics caused by power electronics. • To adjust to sudden variations in load, load-sensing and management systems should be included. • For coordinated protection, use centralized control and synchronized measurement equipment (such as PMUs).
Ground fault protection device [55]-[57]	• Lack of zero-sequence current contribution. • Phase faults and ground faults can overlap, making coordination difficult. • Protection consistency is impacted by the fact that ground fault characteristics vary between modes. • Requires monitoring and collaboration in real time to prevent false positives.	• Use different indicators, such as voltage imbalance or zero-sequence voltage. • Ascertain appropriate time-current grading and keep ground and phase protection logic separate. • Make use of adaptive protection plans that change parameters according to the operating system. • Improved coordination strategies should be developed to adapt to shifting microgrid conditions.
Differential protection device [61], [64], [65]	• Avoid false trips caused by DG sources' inconsistent outputs. • Coordination between protective devices is necessary due to many sources and changing loads. • HIFs can be difficult to detect because of their low current generation. • During islanding, changes in operational conditions can affect the sensitivity and stability of protection systems.	• Use intelligent protection techniques according to the microgrids' mode of operation. • Make use of cutting-edge communication tools to transmit data in real time. • Create protection that is restricted by harmonics to lessen the effects of electrical noise. • Integrate signal processing techniques to improve dependability.
Distance protection device [70], [71]	• IIDGs' modest fault current levels make HIF detection challenging. • Variable fault responses and intermittent DER output can significantly impact system performance and reliability. • Loss of communication and coordination due to the decentralized architecture of microgrids. • High fault resistance distorts impedance measurements, causing distance relays to fail to detect faults accurately.	• Make use of sophisticated ML techniques for DER impact control and HIF identification. • Strong microgrid control to preserve system sustainability and stability in the event of a problem. • Using novel techniques, such as fault ride-through (FRT) requirements. • Impedance compensation methods or adaptive algorithms can be used to rectify distance estimations.
Adaptive protection device [72]-[74]	• Fault levels are changed by frequent transitions between grid-connected and islanded modes. • Timely data exchange is essential to adaptive systems and can be interrupted. • High-speed data processing is required for adaptive algorithms. • The requirement for an appropriate communication channel configuration and power flow.	• Use dynamic setting groups and real-time mode detection. • Make use of fallback local decision-making and redundant communication channels. • Utilize edge computing and algorithms that are optimized. • IED with a fast-acting relay and an improved ML module.
Harmonic protection device [80], [83], [84]	• Lack of standards for harmonic protection. • Voltage and current waveform distortion. • HIFs cannot be detected. • Filtering and computation take a long time.	• Adhere to IEC 61000 and IEEE 519 standards. • DSP techniques to improve measurement accuracy. • Zero sequence and positive sequence-based mechanism. • Adaptive devices based on real-time harmonic profiles.
Communication protection device [85]-[87]	• Disconnecting a communication route can result in significant data loss and lower the safety and dependability. • Cyberattacks can target communication networks. • Data loss when the network is congested. • Data sharing may be hampered by a lack of bandwidth, particularly in dense microgrids with several DERs.	• Give priority to time-sensitive data and use real-time communication protocols (like IEC 61850 GOOSE). • Use intrusion detection systems, firewalls, robust encryption, and authentication. • Execute QoS (quality of service) management. • Use edge computing and effective protocols to maximize data transmission.

TABLE 2. (*Continued.*) **Issues and solutions of PDs in AC microgrids.**

Arc flash protection device [91], [95], [96]	• Arc flash incident energy estimations are made more difficult by the SCCL variance in microgrid operation modes. • The approach to arc flash protection is impacted by the RESs' intermittent nature. • Bi-directional fault current flow caused by DERs can make protection strategies more difficult to implement. • Preventing miscoordination by making sure that additional safety devices are properly coordinated.	• Making use of sophisticated incident energy estimates that consider different SCCLs • Creating dynamic configuration management solutions for systems that allow protection strategy adjustments. • Using adaptive protection techniques to respond to faults effectively. • Modernizing control and communication systems to enable real-time coordination and data transfer.
Synchronization protection device [97], [98]	• Synchronization parameters change depending on the circumstances in both islanded and grid-connected modes. • Minimizing communication channel latency to improve device synchronization. • Addressing the voltage and frequency variations caused by sporadic RESs. • Adjusting system configurations while preserving stability and synchronization.	• Using sophisticated control techniques to ensure steady synchronization in both islanded and grid-connected modes. • Modernizing communication systems to increase signal accuracy and decrease latency. • Using ESS to support frequency and reduce voltage imbalance in transient situations. • Intelligent protection mechanisms that can distinguish between changes in power flow and faults.

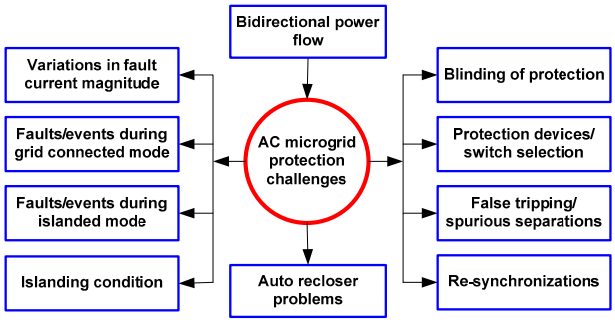

FIGURE 10. Framework of AC microgrid protection difficulties [105].

Thus, in closing of CB, the inrush current is expressed as:

$$I_{inrush} = i_{12,pr1}(t) - i_{12,pr2}(t) | t \geq 4L_{IL}/R_{IL} \tag{12}$$

I_{pr1}, I_{pr2}, θ_1, and θ_2 are obtained using the superposition principle:

$$I_{pr1} = \frac{V_{p1}}{\sqrt{R_{IL}^2 - (\omega_1 L_{IL})^2}}; I_{pr1} = \frac{V_{p2}}{\sqrt{R_{IL}^2 - (\omega_2 L_{IL})^2}};$$

$$\theta_1 = \emptyset_1 - tan^{-1}\left(\frac{\omega_1 L_{IL}}{R_{IL}}\right); \theta_2 = \emptyset_2 - tan^{-1}\left(\frac{\omega_2 L_{IL}}{R_{IL}}\right).$$

In system-level dynamic studies, the interconnected transmission line is typically regarded as a constant complex impedance, whereas grid-following inverter-based resources (IBRs) have been characterized as current sources synced to the main grid via phase-locked loops (PLL). The authors of [100] use three different voltage source converter (VSC) control strategies—grid-feeding, grid-forming, and grid-supporting—to examine microgrid performance during islanding and synchronization. Each control method was modeled within a microgrid simulation framework, simulating the inverter-interfaced distributed generation (DG) units. Based on reference signals, the grid-feeding control technique was created to introduce preset amounts of active and reactive electricity into the grid. The grid-forming control maintains voltage and frequency stability by managing the converter's internal voltage source parameters, while the grid-supporting control provides supplementary assistance by changing power output to preserve system stability throughout transitions. Their comparison of the advantages and disadvantages of each approach demonstrates that, although grid-feeding control guarantees straightforward power injection, grid-forming gives superior voltage and frequency stability, and grid-supporting offers more resilience during transitions. The simulations were conducted using time-domain analytic methods to evaluate parameters. The performance of these control modes was examined under numerous operational situations, including islanding events, synchronization with the main grid, and load changes. In addition, the authors of [101] provide a technique for synchronizing MGs with limited-capacity power systems that minimizes the impact on producing equipment shafts by employing a passive synchronization algorithm. Microgrids and external networks have trouble synchronizing because of frequent load fluctuations that throw off synchronization conditions. Phase angle mismatches brought on by abrupt power changes may result in excessive equalizing currents, equipment stress, or generator disconnection. To decrease shock moments during parallel operation, a unique auto-synchronizer algorithm for reclosers is developed. Real-time simulation improves power system efficiency, reliability, and resource consumption by lowering the shock moment. The integration of data-based systems that rely on online data and dispersed control structures increases the risk of cyberattacks. In [102], the authors offer a sophisticated microgrid protection and control system that permits smooth islanding and grid synchronization. The study demonstrates its effectiveness, integrating data-driven monitoring and distributed control structures, emphasizing resilience against cyberattacks and coordination failures, while addressing gaps in the literature on relay protection settings, communication delays, DER transformer layouts, and grounding. The approach comprised

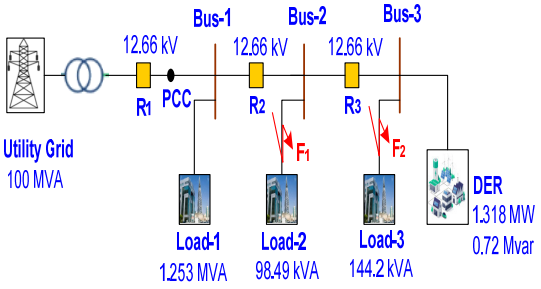

FIGURE 11. Test network for investigating the dynamics of fault current level [22].

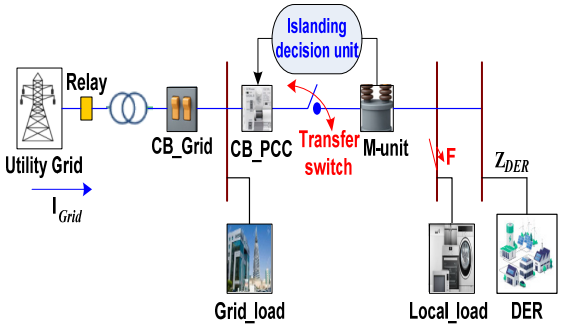

FIGURE 12. Modeling to investigate islanding condition detection [109].

simulating grounding techniques, DER transformer configurations, and relay protection settings in a single simulation environment. Data flow between controllers and communication delays were included to assess the system's real-time responsiveness in both failure and normal scenarios. To verify the efficacy of the suggested method, simulation experiments were conducted with an emphasis on operational continuity, coordination dependability, and fault detection accuracy in islanding and reconnection scenarios. The findings showed that the system improves cyber resilience and protection adaptability, thereby resolving significant issues noted in previous microgrid protection studies. To synchronize several decentralized generators in both grid-connected and islanded microgrids, the authors of [103] presented the Automatic Adaptive Synchronization (A2S) technique, which combines control and optimization techniques. The technique uses an AI-based control circuit with a lower switching frequency to manage synchronization, and a voltage-sensing-based control strategy in conjunction with the Rain Optimization Algorithm (ROA) for grid and load voltage detection. The system maintained steady operation even during voltage faults by achieving fast synchronization with a response time of 25.8 ms and a frequency variation of 0.15 Hz. The suggested approach outperformed RES-based voltage sources and other sophisticated controllers, attaining low total harmonic distortion (THD) levels of 2.28 % and 2.52 % in normal and fault scenarios, respectively.

While most PDs are helpful in both grid-connected and islanded modes, they do have certain drawbacks. They need a centralized controller and real-time monitoring of the communication channel. Some protection solutions use intelligent classifiers, optimization algorithms, and a microprocessor to address the various microgrid protection issues. According to the literature, none of these devices can effectively address all MG protection issues because of their limitations, which include network topology, MG sizes and types, communication links, centralized controllers, bidirectional current flow, modified fault current levels resulting from changes in operational modes, relay settings, computational cost and time, and relay location. Therefore, if the adaptive protection strategy lessens reliance on the microgrid topology, centralized controller, communication link, and computation cost, it is more beneficial. A selection of recent research solutions is included in Table 2, along with the challenges that microgrid PDs face [104].

IV. AC MICROGRID PROTECTION: CHALLENGES AND SOLUTION

Since DERs are sporadic, a microgrid is a collection of DERs. The total power generated by all of the DERs in the microgrid is not consistent because of their intermittent nature. These power generation variations disrupted the microgrid PDs because the fault current fluctuates, causing relays to malfunction. When the fault site is close to the DERs, the fault current is large; when it is far from the DERs, the fault current is low. Fault current is determined by the total impedance between the DERs and the points of fault. The overall impedance is also influenced by the distance between the fault point and the DER's generation. Consequently, it is crucial to investigate the microgrid protection concerns related to the level of DER integration in both grid-connected and islanded modes. Fig. 10 illustrates the framework difficulties of protecting the AC microgrid.

A. VARIATIONS IN FAULT CURRENT MAGNITUDE

Fault current level expansion is influenced by the type of microgrid network operating mode, DER integration into the microgrid, grid connection type, installed DG locations, DG type, different power electronics converters used with DGs, and grid impedance. In the two primary operating modes—islanded and grid-connected—the LV network usually raises the fault level to a significant degree when DERs connect. Because both DERs and the utility grid contribute to the microgrid that feeds the fault, the fault current in grid-connected operation mode is noticeably high. In contrast, the fault current is very low when operating in islanded mode because DERs with low power are the only source in a microgrid. Different DER types have different fault current feeds. Synchronous DERs have fault currents that are five times greater than their rated current [105]. The authors of [106] state that, as the penetration level of DERs grew, the fault current level increased dramatically. Thus, the integration level of the DER should be taken into consideration when

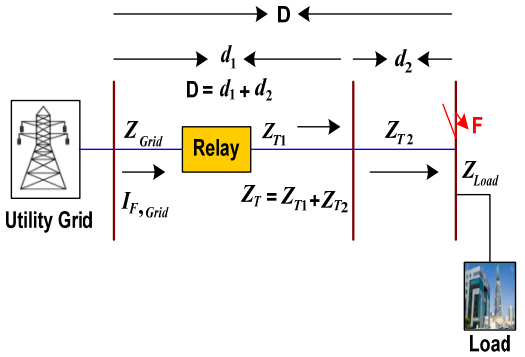

FIGURE 13. Modeling of the utility grid without DER to investigate blinding protection [111].

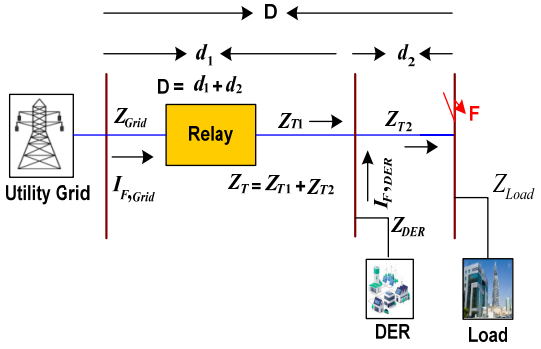

FIGURE 14. Modeling of the utility grid with DER to investigate blinding protection [111].

setting the relay pickup parameters. Operational mode, DER count, and DER type all affect the fault current's magnitude. Therefore, it is challenging to make accurate fault current predictions. Additionally, the challenges of lowering the fault current magnitude during islanding mode can be overcome by attaching a flywheel or supercapacitor with a power electronics converter-based DER to the LV side of the busbar, which raises the fault current value. In some ways, this can address the problem of fault current magnitude. This method necessitates a substantial financial outlay for the installation, use, and upkeep of the enormous storage device.

B. FAULTS/EVENTS DURING GRID-CONNECTED MODE

In normal operation, protection systems trip when a utility-side malfunction occurs. The feeder line protection system must act fast to disconnect the problematic component from the network in the event of a microgrid side fault that occurs while the grid is connected. The PDs' response times are influenced by the microgrid's features, protection strategy, and complexity. Additionally, when in grid-connected mode, DERs must continue to function while PCC protection devices are being detected and tripped, and their PDs should not trip before PCC PDs in the event of a utility grid-side breakdown. All DERs must be able to ride through faults to detect such a situation. Despite their difficulty in detecting, several non-fault events at the LV point of common coupling, including open-phase conditions and voltage imbalance, can negatively affect sensitive loads and micro sources. Therefore, particular protection measures are needed to address these issues [107]. In [22], the test network used to investigate the fault current level dynamics in the grid-connected mode is simulated by the authors, as illustrated in Fig. 11. In particular, two fault spots were taken into consideration to illustrate how the position of the generating unit affected the fault current levels. The load characteristics and equivalent impedance between the fault location and the generating source were considered when calculating the fault current at each point. The simulation results show that because the fault current depends on the load and impedance value at that fault site, it is higher at fault point 1 in grid-connected mode than it is at fault point 2. A fault that occurs distant from the generating unit will have a low fault current level, while one that happens near it will have a high fault current level because total impedance increases with distance.

C. FAULTS/EVENTS DURING ISLANDED MODE

Microgrids in islanded mode have distinct problems compared to those in grid-connected mode. In an islanded microgrid, the fault current is roughly five times the normal current. Compared to the microgrid's grid-connected operating mode, the fault current is significantly lower in the islanded mode. Conventional overcurrent protection relays and devices trip due to a high magnitude fault current provided by the utility grid. Furthermore, conventional relays and overcurrent PDs are usually configured to function at 2 to 10 times the nominal current. Their present-time coordination is disrupted, nonetheless, by the notable decrease in fault current levels. Thus, the most affected relays are those with strongly inverse properties, like fuses, and those with instantaneous overcurrent [108]. Similarly, as illustrated in Fig. 11, the authors of [22] also simulate the test system that is utilized to study the dynamics of fault current level during the islanded mode. The PCC serves as a barrier between the microgrid and the main grid. The test system was modeled to assess the effects of load characteristics and impedance variations on fault current magnitudes. This system was also utilized in the grid-connected fault analysis. According to simulation results, the fault current at fault point 2, which is influenced by load and impedance, is higher than at fault point 1 in islanded mode, as was previously mentioned in the grid-connected fault analysis.

D. ISLANDING CONDITION

Islanding happens when a microgrid that is connected to the main grid separates from it for unusual reasons or a breakdown, but it nevertheless supplies the local load. Fig. 12 shows the modeling utilized to investigate the identification of islanding situations. The microgrid is connected to the utility grid via the PCC. The islanding detecting relay is located at the PCC. This islanding technique is in charge of

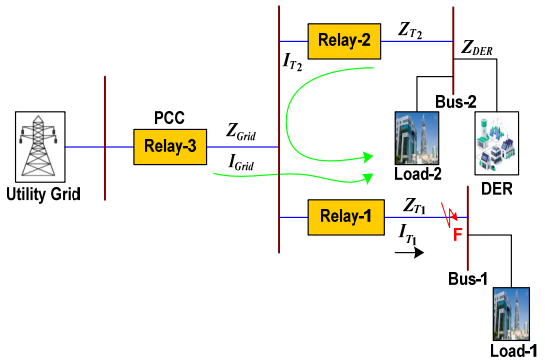

FIGURE 15. Modeling of the utility grid with DER to investigate false tripping [116].

identifying the islanding state when a mains outage or a utility grid region malfunction occurs. After identifying the islanding condition, the relay at the PCC disconnects the microgrid from the utility grid. The protective relays malfunction as a result of the substantial impact on PCC's system characteristics during this islanding state. To solve the challenges, a robust protection mechanism that can accurately detect when a microgrid is transitioning between grid-connected and islanded modes is required. To enhance the power system's overall performance, it must also ensure appropriate protection for the microgrid and connected loads [109].

E. BLINDING OF PROTECTION

When DERs are incorporated into a traditional power system, the additional impedance from DERs can lower fault current levels, which makes it more difficult for PDs to identify and isolate faults. This phenomenon is known as blinding of protection. Additionally, the integration of RESs between the utility grid and the load usually results in a loss of protection. To prevent fault detection, the RES's extra impedance lowers the fault current below the overcurrent relay's pickup threshold. Relay inactivity causes failed fault isolation and compromised system protection [110].

The expression for fault current computation for conventional power systems without DER integration will be established initially to investigate the blinding protection issue of a microgrid. The microgrid's expression upon DER integration will next be ascertained to investigate the blinded condition of the microgrid's protection. When a fault occurs at the far end of the feeder, as shown in Fig. 13, the overcurrent relay effectively eliminates the problem due to the high fault current flow in a conventional power system without DER integration. Likewise, in Fig. 14, when a DER is incorporated into a traditional power system to create a microgrid, the rated current is changed because the system's impedance rises as a result of the DER's impedance. The fault current falls below the overcurrent relay's pickup setting as a result of this increase in impedance. Consequently, when a failure occurs at the far end of the feeder, the utility grid and DER both contribute to the fault current; however, the decreased current may make it difficult for the overcurrent relay to identify the problem [111]. To determine, without DER inclusion, the conventional power system's overall fault current. The fault's location is D, and each phase's peak fault current is determined using equation (13).

$$I_F = I_F, Grid \tag{13}$$

$$I_F, Grid = \frac{V_{Th}}{\sqrt{3Z_{Th}}} \tag{14}$$

where I_F is the total fault current, V_{Th} is the pre-fault voltage, and Z_{Th} is the Thevenin's impedance. Let Z_{Grid}, Z_{T1}, Z_{T2}, and Z_{Load} is a representation of the load, transmission line sections, and utility grid impedance. The impedance of Thevenin can therefore be computed as follows:

$$Z_{Th} = Z_{Grid} + Z_{T1} + Z_{T2} \tag{15}$$

The total fault current of the conventional power system without DER integration is obtained in equation (16) by substituting equation (15) back into (14).

$$I_F = I_F, Grid = \frac{V_{Th}}{\sqrt{3\left(Z_{Grid} + Z_{T1} + Z_{T2}\right)}} \tag{16}$$

Likewise, to ascertain the total fault current when a DER is integrated into a conventional power system to establish a microgrid. Equation (17) is used to calculate the peak fault current for each phase, and the fault is located at a distance D.

$$I_F = \frac{V_{Th}}{\sqrt{3Z_{Th}}} \tag{17}$$

where I_F is the total fault current, V_{Th} is the pre-fault voltage, and Z_{Th} is the Thevenin's impedance. Let Z_{Grid}, Z_{T1}, Z_{T2}, Z_{DER}, and Z_{Load} represents the transmission line segments, DER, microgrid load, impedance of utility grid, respectively. Thus, the Thevenin's impedance can be calculated as follows:

$$Z_{Th} = \frac{\left(Z_{Grid} + Z_{T1}\right)\left(Z_{DER}\right)}{Z_{Grid} + Z_{T1} + Z_{DER}} + Z_{T2} \tag{18}$$

Consequently, the fault current contribution from the DER in the microgrid can be computed using equation (19). With a larger impedance translating into a lower fault current, this equation shows how DER impedance may contribute to the fault current level.

$$I_F, DER = \frac{Z_{Grid} + Z_{T1}}{Z_{Grid} + Z_{T1} + Z_{DER}} \times I_F \tag{19}$$

The utility grid's contribution to fault current can be computed using equation (20). This formula illustrates the relationship between utility grid impedance and fault current level, showing that a lower impedance results in a higher fault current.

$$I_F, Grid = \frac{Z_{DER}}{Z_{Grid} + Z_{T1} + Z_{DER}} \times I_F \tag{20}$$

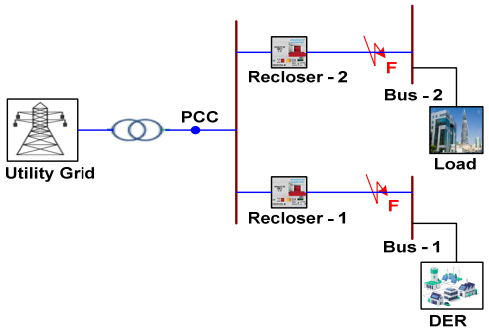

FIGURE 16. Modeling to investigate auto recloser problems under normal protection system operation [122].

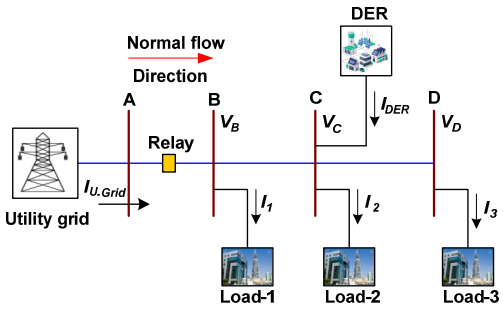

FIGURE 17. Modeling of bidirectional power flow [123].

F. PROTECTION DEVICES BASED SWITCH SELECTION

The operational speed, available fault current, and system voltage level requirements all influence the choice of PDs. These factors allow PDs to vary from high-speed solid-state switches to traditional CBs, each of which has unique benefits concerning response time and compatibility with particular microgrid layouts. The current and voltage parameters of the system affect the PDs' switching speed; therefore, higher fault current levels typically result in faster PD response times. As such, sizing should be considered in addition to voltage standards and system current when choosing PDs. Considering the cooperation between several PDs is also crucial. The AS/NZS 3000:2018 standard [112] states that to reduce false tripping in all power systems, the right PD selection is essential. Maintaining system stability and avoiding needless disruptions to unaffected loads are two benefits of making sure PDs are properly graded and coordinated. To ensure proper selectivity and avoid unnecessary disconnecting unaffected system components, upstream PDs should remain dormant, and downstream PDs should operate for a specific fault current [113].

G. FALSE TRIPPING/SPURIOUS SEPARATIONS

False tripping, also known as spurious separations in MGs, happens when PDs misinterpret external or typical occurrences as internal failures, causing needless utility grid disconnections. One major contributing factor is the incapacity of PCC switching devices to reliably determine whether a problem is on the main grid or in the microgrid. This misidentification can complicate system restoration, interfere with the power supply, and lower reliability [114]. The most efficient way to prevent false tripping at the moment is a transfer trip, which allows the PCC breaker to trip quickly by receiving a signal from the utility substation breaker. False tripping at the PCC is therefore expensive since it shortens the life of PDs and raises the cost of maintenance required to get the system back up and running after erroneous separations. In addition to lowering microgrid power quality, false tripping can result in needless non-priority load outages and financial losses during over-frequency operation periods meant for microgrid exports [115].

To study false tripping, Fig. 15 displays the utility grid system modeling using DER. When a large number of DERs are added to a microgrid, the power network's lines and feeders experience bidirectional fault current flow under fault conditions. The fault current that occurs at bus-1 load is supplied by a DER located at bus-2; in some cases, a DER contributes a significant portion of the fault current. Relay-1 operates in the forwarding direction during a malfunction, but Relay-2 may trip in the other direction. The problem should be resolved if Relay 1 trips. However, a large current of I_{DER} may cause the DER unit of Relay-2 to trip due to the considerable fault current that disconnects bus-1 from the utility grid, depending on the relay settings and DER size. Thus, this problem occurs because omnidirectional overcurrent relays might not be able to discriminate between the fault current flow direction. For this reason, this type of tripping is called "false tripping." Similar to this, sympathetic tripping, sometimes known as false tripping, happens in large distributed power systems when a Relay-2 trips before the Relay-1 on the real failed feeder because it is experiencing a larger fault current than its pickup value. This leads to the unintended isolation of major network sections, such as bus 2. This causes significant network segments, like bus 2, to inadvertently become isolated. The microgrid's power system will become seriously unreliable as a result of sympathetic tripping [116], [117]. Therefore, the following is the mathematical expression for the fault current contribution of a DER and the utility grid:

$$I_F = \frac{V_{Th}}{\sqrt{3}Z_{Th}} \tag{21}$$

$$Z_{Th} = Z_{Grid} + \left(\frac{Z_{T1} * (Z_{T2} + Z_{DER})}{Z_{T1} + (Z_{T2} + Z_{DER})}\right) \tag{22}$$

However, the following is the mathematical expression for the utility grid's fault current contribution without DER:

$$Z_{Th} = Z_{Grid} + Z_{T1} \tag{23}$$

Here, the impedance of feeder-1 is assumed as Z_{T1}, the impedance of feeder-2 is assumed as Z_{T2}, the impedance of the utility grid is Z_{Grid}, the impedance of the DER is Z_{DER}, the

fault voltage is V_{Th}, and Z_{Th} the network impedance during a fault with the presence of DER at feeder-2.

H. RE-SYNCHRONIZATION

Resynchronization is the process of reconnecting an islanded microgrid to the main utility grid; resynchronization of a microgrid at the PCC involves making sure that synchronization equipment is available and that the utility grid can support all previously islanded loads before reconnection. Although this procedure is required to restore grid-connected operations, it is technically challenging. Before reconnecting to the utility grid, a microgrid operating in an islanded mode must resynchronize. It is risky to reconnect without synchronization because an unsynchronized operation may result in current flowing near short circuits, endangering microgrid generators and causing blackouts. Moreover, the identical phase order, corresponding phase voltages and frequency, protective device coordination, and phase angle between the two systems are requirements for a successful connection of an islanded microgrid to the utility grid [118].

Passive, active, and open transfer transition synchronization are the three popular synchronization techniques. Compared to the open transfer transition method, both passive and active synchronization techniques maintain a high degree of reliability. The active synchronization technique, on the other hand, is more complicated and costlier [119]. In [120], they are discussed in detail. The foundation of passive synchronization is the PCC's monitoring of the utility and microgrid voltage. The passive approach has the benefit of being simple to use and requiring no additional communication. One major drawback is that upon reconnection, voltage spikes and inrush currents may result from mismatched voltage magnitudes between the utility grid and the microgrid. To provide a faster and more seamless grid connection, active synchronization employs extra control. This method is the safest way to reconnect MGs to the utility grid during an open transfer transition, although it lowers system reliability.

I. AUTO RECLOSER PROBLEMS

In power systems, auto-reclosers are conventional PDs that are frequently employed as CBs to automatically restore service following brief breakdowns. Unless actively altered or altered by the control system, switching in CB does not return to its initial condition. In contrast, the auto-recloser control system action automatically returns to the initial condition after a certain amount of time has passed after switching has taken place. Auto-reclosers work well at power system sites that are susceptible to arcing and transient faults, including those brought on by lightning strikes, which usually go away in a few cycles and are unlikely to become permanent. Through automatic service restoration, auto-reclosers improve system stability and minimize the requirement for manual intervention by eliminating the need for staff to reset circuit breakers at the fault location [121].

In Fig. 16, the utility grid system modeling using DER to examine the auto-recloser issues is displayed. When a system malfunction occurs, the auto-recloser's CB opens, then closes again after a certain amount of time to determine whether the malfunction was fixed. If the defect is fixed, it keeps supplying; if not, it trips more frequently than before. After each journey, check to see if the issue is automatically fixed, but it keeps going back to its closed condition. The auto-recloser changes to a permanently open status after a few trips if the issue persists. According to the ANSI C37.2 standard, the auto recloser device number is 79, which refers to the ''Reclosing relay'' [122].

J. BIDIRECTIONAL POWER FLOW

Electrical power moves in a single direction in radial-configured power systems, from the source to the points of consumption. In contrast, the two-way power flow makes shielding MGs extremely difficult. Bidirectional power flow is produced during regular operation by the integration of DER near the load in an active network. In these situations, traditional protective systems might not be adequate because they are primarily built for unidirectional power flow. Fig. 17 illustrates the microgrid's bidirectional power flow. In the absence of DER, power moves radially from the generating plant to the grid and then to the load. But when DER is integrated, the current that the relay at Bus A senses decreases, suggesting bidirectional power flow [123]. In recent research, the authors of [124] examine how EVs' energy storage and grid-supporting capabilities can be used to improve power system stability. Using a medium-level load (residential and industrial), the study theoretically integrates a significant number of EVs into the grid system and examines the effects on peak load, load factor, and voltage sag over the whole grid model. In this paper, a type 2 AC charging station with a medium load demand and grid integration was analyzed. This system was connected to EVs with various charging circumstances. Power quality measurements are greatly impacted by this method, which makes use of EVs' bidirectional power flow capacity to deliver auxiliary services like voltage management and spinning reserves. The simulation results show how EVs affect both the electric load and the overall suggested grid model. While bidirectional power flow necessitates sophisticated control and real-time monitoring to guarantee system reliability, conventional protective devices are made for unidirectional flow and may malfunction under reverse currents.

V. AC MICROGRID PROTECTION: CRITICAL ANALYSIS OF PROTECTION STRATEGIES

This section provides a critical examination of the various protection strategies presented in the existing literature. The authors of [125] proposed an adaptive protection technique for smart distribution networks based on the variation features of fault current and load current. According to the suggested approach, the status of CBs—which represent the connection statuses of DGs—is continuously tracked in real time. Should

TABLE 3. Summary of the review on the preferred solution for AC microgrids protection strategies.

Protection strategies	Refs.	Presence of DG	Objectives	Results	Simulation/ experimental	Validations
Adaptive protection technique	[125]	Intelligent distribution system with DGs	Based on fault-current and load-current fluctuation characteristics.	Findings support the suggested method's accuracy and efficacy.	MATLAB/ Simulink	Nil
Adaptive overcurrent protection	[126]	Grid-connected and islanded modes	To calculate relay pickup and guarantee a distribution system with reduced communication overhead.	Performance is assessed for all operational states, fault kinds, and fault impedances.	MATLAB/ Simulink	IEEE-15 bus system
Passive islanding detection technique	[127]	Inverter based-DGs	Effectively differentiates between real islanding and variations in grid frequency.	Fast, reliable, accurate, and simple to use.	MATLAB/ Simulink	Nil
Adaptive decentralized protection technique	[128]	Without DG	Addressing the issues of blindness and sympathetic tripping	Keeping overcurrent relays in a microgrid network coordinated even in unpredictable circumstances	MATLAB/ Simulink	IEEE-14 bus system
Directional overcurrent protection	[129]	Without DG	Emphasizing problems like false trips and blindness in safety systems caused by variations in short circuit currents	Demonstrates the efficacy of digital twins in validating protection methods by proving that protection coordination fails during malfunctions.	MATLAB/ Simulink	Nil
Communication protection technique	[130]	Smart grid	Removing the necessity for optical fibers or conventional wiring in a cognitive radio system.	Performance was assessed in a variety of communication contexts.	MATLAB/ Simulink	Nil
Data mining and wavelet multiresolution techniques	[131]	Without DG	To preprocess signals for THD, voltage, and current.	The random forest model was tested and trained.	MATLAB/ Simulink	Nil
Multi-agent system-based hierarchical protection strategy	[132]	Distribution network with DG	To quickly and independently continue primary-level protection cooperation.	In terms of economy and speed of protection, hierarchical is more efficient.	MATLAB/ Simulink	Isfahan-76 bus system
Time-domain-based direction protection strategy	[133]	Grid-connected microgrid	Within a half-cycle, locate the fault in both grid-interconnected microgrids.	It increases the overlaid directional element's reliability in situations where IBRs are the primary fault current source.	EMTP-RV/ MATLAB	IEEE-33 bus system
Reinforcement learning (DDPG/SAC) protection strategy	[134]	Grid-connected microgrid	To resolve the microgrid's EMS's high-dimensional, stochastic challenge.	The scheduling of microgrid elements to engage in the power market is effectively handled by both algorithms.	MATLAB/ Simulink	Nil
Coordination protection strategy	[135]	Without DG	To determine the fault types, zone, and ROCOV.	The technique successfully preserves coordination in the face of various kinds.	MATLAB/ Simulink	IEEE-14 bus system
Adaptive-based islanding detection technique	[136]	Islanded microgrid	For ROCOF, a general and dependable solution for different kinds of microgrids.	Accurately identifies islanding situations, even when there is no power mismatch.	MATLAB/ Simulink	Nil
Differential protection strategy	[137]	Islanded microgrid	To improve the effectiveness and dependability of fault protection in islanded microgrids.	Nil	MATLAB/ Simulink	IEEE-13 bus system
Multi-agent-based protection strategy	[138]	Radial distribution network with DG	Regarding IED-assisted relays in looped microgrids.	The approach is effective in a range of fault sites and DG penetration levels.	ETAP/ MATLAB	Nil

there be any changes, the calculation and setting agents are activated to automatically start the relay setting calculation. The suggested approach can change with every MW variance in DGs. It is based on the protection functions and IEDs that are currently in use, albeit being adaptive. The IEDs monitor the condition of DGs and CBs. whereby the relay

and calculation agents are activated to update the IEDs in the event of a status change. The adaptive protection model is created using the Dig SILENT Programming Language (DPL). The simulation findings verify that the suggested strategy works correctly and is effective. Similarly, a relaying strategy for adaptive overcurrent protection is suggested for distribution systems operating in both islanded and grid-connected modes. An AOCR technique that is dynamic and can be locally implemented in relays was used in the study. The relay adaptively adapts its pickup settings to operating conditions based on real-time DER status and a moving average line load estimate. The adaptive protection problem is rewritten to guarantee low computational complexity for real-world implementation. Significantly less communication overhead is ensured by the PD's estimation of relay pickup independent of external controllers. Accordingly, transient system models in Simulink are used to examine the dependability of a 15-bus distribution system for all possible combinations of state and fault types/impedances [126]. The authors of [127] offer a passive islanding detection technique for IBDGs based on synchro phasor readings. The voltage-to-current ratio and the rate of change of voltage (ROCOV), which are tracked by micro-PMUs at the PCC, are the foundations of the VoI index, which is used in a decentralized islanding detection technique. This method successfully distinguishes grid frequency changes from actual islanding and is shown through simulations to be accurate, dependable, fast, and easy to implement for IBDGs. The authors of [128] discuss sympathetic tripping and blindness issues and propose an adaptive decentralized protection method to guarantee dependable overcurrent relay coordination in microgrids, even in unpredictable circumstances. The technique first estimates relay settings without taking distributed generation (DG) into account. From the relay's point of view, fault currents that include DG contributions are computed using Thevenin equivalent circuits. The suggested solution works better than traditional relay coordination techniques in DG-integrated microgrids, according to simulation findings conducted on modified IEEE 9-bus and 14-bus systems in MATLAB and DIgSILENT PowerFactory Version 2023.

In [129], a validation method for directional overcurrent protection strategies in distributed energy resource (DER) ring-topology distribution systems is presented. The work addresses issues including fluctuating short-circuit levels, false trips, and protection blindness by evaluating protection coordination under DER-supplied loads using both offline and real-time simulations using a digital twin. The situations under study, where the ring network functioned in conjunction with the main grid, proved the efficacy of the recommended protective strategy. The speed and selectivity of the protection mechanism remained consistent with the reference case, but the incorporation of DERs led to an increase in short circuit current. The findings indicate the efficacy of the suggested approach in dynamic fault circumstances and improve validation accuracy using digital twin-based electromagnetic transient (EMT) research. A backup protection method based on cognitive radio for smart grid applications is provided in [130]. Instead of using optical fibers or conventional wiring, the suggested protection plan makes use of a cognitive radio-based wireless sensor network. The work implements a backup protection mechanism for the smart grid using CR-based Wireless Sensor Networks (CRWSN). CRWSNs are made up of many SUs (sensors) spread throughout a certain region that continuously detect gaps in the spectrum and exploit such gaps to send their transducer data. Using spectrum sensing and frequency allocation methods common to cognitive radio systems, it functions on unlicensed spectrum channels. Additionally, the suggested technique was simulated in MATLAB/Simulink to assess its cost-effectiveness, and its performance was assessed in a range of communication scenarios. The authors of [131] suggested a wavelet multiresolution analysis and data mining method to improve the security and safety of microgrids. After preprocessing voltage and current data and calculating total harmonic distortion using wavelet transform decomposition, statistical indices, including mean, median, and standard deviation, are extracted, along with negative sequence components of power. A random forest classifier is then trained using these features to detect, identify, and classify faults. With analysis in Python, MATLAB/Simulink simulations for both grid-connected and islanded microgrids demonstrated that the suggested approach performed better than decision tree and support vector machine classifiers documented in the literature.

A hierarchical protection approach based on a multi-agent system was introduced by the authors of [132] for distribution networks that have a large penetration of electronically-coupled DGs. The fundamental benefit of the suggested supplemental method is its capacity to quickly and independently sustain protective coordination at the primary level while the main relay goes through laborious setup adjustments in response to changes in network conditions. In the proposed supplemental system, the distribution network is divided into multiple zones that connect via point-to-point communication, with converter-based DGs serving as the sole MAS agents. Through several simulation case studies on the Isfahan-76 bus system's distribution network, the efficacy of the suggested approach is confirmed. The authors of [133] suggested a time-domain protection plan for radial and looped microgrids using inverter-based resources that can function in both islanded and grid-connected modes. For quick fault discrimination, the technique uses an ultra-high-speed sub-cycle directional element backed by low-bandwidth relay-to-relay communication. The scheme determines the fault direction by computing the superimposed positive-sequence direct component of transient energy using Park's transformation and time-domain superimposed characteristics. In inverter-based settings, delta and DDSRF filters are used to improve reliability. A modified IEEE 34-bus system was used to validate the suggested method, which demonstrated excellent reliability and quick problem detection. In [134], the authors describe an energy management

system based on reinforcement learning as a resilient microgrid power system integrity protection strategy. The study evaluates the efficacy of two methods—the Soft-Actor Critic (SAC) technique and the deep deterministic policy gradient (DDPG) method—for resolving the high-dimensional, continuous, and stochastic problem of the grid-connected microgrid's energy management system. DDPG is devoted to instability because of the deterministic nature of the actor interacting with the Q-function. By using a stochastic actor, the actor-critic RL algorithm SAC was developed to address the shortcomings of DDPG, including its hyperparameter and instability. SAC uses the replay buffer of DDGP as a deterministic technique to acquire efficient samples by reviewing prior operation instances, in addition to implementing a stochastic policy to get stability characteristics of on-policy approaches, such as trust region policy optimization. To demonstrate the effectiveness of the suggested methods, real data from GASA-based islanded MGs in Korea are used for validation. The results showed that both methods work well for scheduling microgrid components to participate in the power market exchange. For each number of episodes, DDPG demonstrated better time convergence than SAC.

Similarly, the authors of [135] introduce a robust coordination system for MG protection based on ROCOV. The suggested protection plan determines the ROCOV using local measurements at a low sample frequency, enabling precise fault and defective zone identification and dependable primary and backup relay coordination. The suggested plan was evaluated on a modified IEEE 14-bus meshed network using MATLAB/Simulink. According to the results, it is effective at keeping primary and backup relays coordinated across a range of fault kinds, locations, and network topologies. In [136], the authors suggested an Islanding Detection Technique (IDT) based on the adaptive rate of change of frequency (ROCOF), which provides a general and dependable solution for different kinds of microgrids. Two configurations—(i) generator-based MGs and (ii) hybrid MGs that combine generators, PV, and storage—are used in its development and implementation in MATLAB/Simulink. Findings show that even in situations when there is no power imbalance, the suggested IDT can identify islanding conditions with accuracy. In [137], the authors suggested a graph-theoretical method for islanded microgrid partitioning based on a differential protection system. The suggested approach uses graph theory to design protection zones based on topology and power flow, improving fault protection efficiency and reliability in islanded microgrids. The microgrid is divided into several protective zones using the algorithm. The degree of microgrid system reliability varies with the number of protection zones. The network must be divided into separate protection zones to implement a differential zone protection method. The IEEE-13 node microgrid is used for validation. The authors of [138] suggest utilizing IED-assisted relays as part of a multi-agent-based protection strategy for looped microgrids. Tokens are used to keep unaffected zones from malfunctioning during failures. To ensure that only the relays inside the impacted zone are operational, the token is transmitted among IEDs in order to identify and isolate the defective portion when a fault occurs. By removing the single points of failure seen in centralized systems, this decentralized strategy not only increases cybersecurity resilience but also fault selectivity and dependability. The method's efficiency is confirmed by simulations in MATLAB and ETAP across a range of fault sites and DG penetration levels.

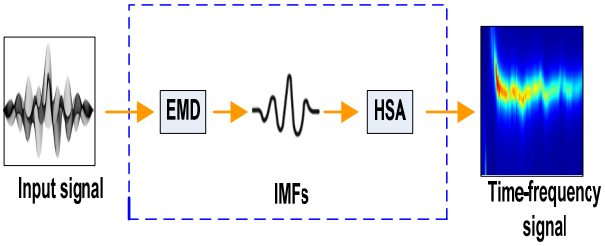

FIGURE 18. Operation mode of HHT.

The aforementioned evaluation studies show that while each system is made to meet a particular problem, no single protection approach can handle all microgrid protection concerns. More studies on microgrid PDs are therefore necessary to address all of the issues associated with MG protection. The review of the AC microgrids' protection strategies is summarized in Table 3, which can serve as a valuable resource for creating more sophisticated protection plans for all the problems.

VI. PROTECTION STRATEGIES: SIGNAL PROCESSING AND ARTIFICIAL INTELLIGENCE

Since traditional protection schemes are unable to handle the nonlinear dynamics, bidirectional power flows, and variable fault characteristics introduced by distributed generation (DG) units and inverter-based resources, signal processing-based protection techniques have become essential to the protection and control of AC microgrids. These methods may precisely identify, categorize, and isolate errors by examining voltage and current waveforms in real time. A fault condition causes the system's parameters to deviate from normal, which modifies the output of the system. System flaws are correlated with the output signal pattern or feature. The characteristics of interest for fault identification are retrieved for pattern analysis by examining the time-domain, frequency-domain, and time-frequency-domain. Several signal-processing techniques, including Wavelet Transform (WT), Traveling Wave (TW), Hilbert–Huang Transform (HHT), and Stockwell Transform (ST), are used in MGs to extract some distinguishing features from system signals for processing [45], [139]. WT is a signal processing tool that analyzes non-stationary signals in the time-frequency domain with a data window that may be adjusted for higher resolution. WT makes it possible for protective devices to examine both transient and steady-state signal components under unusual circumstances.

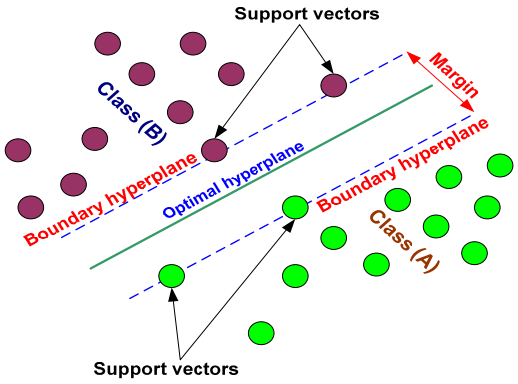

FIGURE 19. SVM protection strategies.

By capturing the transient components that include fault data from the system disturbance signals, WT has been utilized in power engineering to identify fault events. As a result, the recovered transients are divided into a series of wavelets, each of which represents a time-domain signal with specific information that covers a specific frequency range. The authors of [140] provide an intelligent microgrid protection method that combines an Ensemble Bagged Decision Tree (EBDT) classifier for precise fault detection and classification with Discrete Wavelet Transform (DWT) for signal analysis. Utilizing wavelet energy characteristics obtained from voltage and current data as classifier inputs, EBDT hyperparameters are tuned via random search to enhance performance. The effectiveness of the suggested protection method is verified using a modified IEC test microgrid model that includes both synchronous and inverter-interfaced distributed generators (DGs) under various failure scenarios that are simulated in the MATLAB/SIMULINK environment. The suggested approach improves the dependability, flexibility, and real-time fault resilience of contemporary microgrid protection systems by outperforming current classifiers.

Additionally, by examining high-frequency transients rather than steady-state currents, the traveling wave-based method allows for extremely quick fault diagnosis and localization in AC microgrids. They enable precise directional discrimination for selective isolation and offer great sensitivity in inverter-dominated systems with low fault currents. Their performance improves adaptability by remaining dependable in a variety of islanded or grid-connected setups [141]. Generally speaking, a traveling wave-based detection system may identify fault events using signals that are either naturally generated at the fault area or externally injected after the fault inception. The authors of [142] use traveling wave transients assessed by DWT and categorized by Graph Convolutional Networks (GCNs) to provide a quick and reliable fault-finding technique for power distribution systems. Because every node may retrieve a forecast, the GCN models produce a distributed protection strategy. In the protection zones of the IEEE 34-node system, GCNs locate faults within a distributed protection architecture. Voltage measurements are all that are needed to apply the method, which is resilient to communication losses. Tests conducted in real time on a TI F28379D board demonstrate that the technique works in milliseconds, reaching a speed that is on par with sophisticated TW-based transmission protection. Empirical mode decomposition (EMD) and Hilbert spectral analysis (HSA) are two subsequent techniques that underpin HHT, a time-frequency-based method for handling nonlinear and non-stationary time-series data. The input signal of mixed frequencies is processed by the EMD, as shown in Fig. 18, to extract a set of finite components known as intrinsic mode functions (IMFs), which are subsequently utilized to calculate the instantaneous frequency signal by HSA. For accurate fault classification and location in power systems, HHT precisely extracts instantaneous frequency and energy parameters. These methods work very well in systems that are dominated by inverters and have weak or distorted fault currents. Adaptive, real-time, and noise-robust microgrid protection is made possible by integration with AI/ML classifiers [143]. The authors of [144] suggest a smart failure detection method (FDM) for microgrids that combines deep neural networks (DNNs) and HHT. While singular value decomposition (SVD) refines intrinsic mode functions (IMFs) as inputs to the DNN for fault type, phase, and location identification, HHT extracts features from branch current measurements. When compared to earlier methods, the methodology shows improved accuracy and the capacity to locate new faults. Its accuracy, speed, and resilience to measurement errors are validated by simulations on IEEE 34-bus and microgrid systems.

In signal processing, an ST-based protection device is a time-frequency representation of non-stationary signals that combines the advantages of WT and the short-time Fourier transform to provide a time-frequency distribution that is suitable. As a phase-corrected WT, the S-transform provides more accurate information about a signal's local characteristics in the time-frequency domain. The S-transform analyzes nonstationary voltage and current signals in MGs to enable quick and precise problem identification. For accurate fault classification, phase, and location identification, they extract time-frequency characteristics. S-transform's primary benefit is that it offers a multi-resolution analysis (MRA) that is maintained throughout the full phase of single frequency components. The authors of [145] describe how ST with Support Vector Machines (SVM) and Artificial Neural Networks (ANNs) are used to classify power quality issues. Based on TS EN 50160 requirements, the study uses MATLAB to model seven different types of voltage distortions and a pure sine reference. The S-Transform findings are subjected to four feature extraction techniques: frequency-amplitude, time-amplitude, geometric mean, and standard deviation. The classifiers are fed 640 simulation data points in total, and their ability to identify and categorize voltage aberrations is evaluated.

TABLE 4. Comparison of performance of protection strategies for AC microgrid protection devices.

Protection strategies	Accuracy	Robustness	Adaptability	Response time	Scalability	Efficiency/limitation
Wavelet Transform	High	High	Moderate	Fast	Moderate	• Great for short-term detection. • Sensitive to the precision of signal decomposition.
Traveling Wave	Very high	Very high	Low	Ultra-fast	Low	• Ideal for quickly locating faults. • Restricted by reliance on communication.
Hilbert–Huang Transform	High	High	Moderate	Medium	Moderate	• Useful when dealing with non-stationary signals. • Computationally challenging.
Stock-well Transform	High	High	Moderate	Medium	Moderate	• Excellent in noisy settings. • Offers a balanced time-frequency analysis.
Artificial Neural Network	Very high	High	Very high	Fast	High	• Extremely accurate and flexible. • Ideal for training with a variety of datasets.
Fuzzy Logic	High	High	High	Medium	High	• Performs effectively in ambiguous situations. • Optimality is influenced by the rule approach.
Decision Tree	Moderate	Moderate	Moderate	Fast	High	• Easy to understand and simple. • less resilient when the grid is extremely nonlinear.
Support Vector Machine	Very high	High	High	Fast	High	• Ideal for classifying complex faults. • Needs improvement of parameters.

Artificial intelligence and machine learning-based protection techniques have been extensively employed in the context of improved protection strategies to safeguard MGs in order to overcome the difficulties posed by network complexity and data uncertainty. By examining intricate, nonlinear signals, AI and ML-based protection techniques in MGs allow for quick and precise fault detection and categorization. They offer real-time, adaptive protection in the face of shifting topology, load, and DG penetration. Integration with signal processing methods improves robustness to noise, defect location, and type identification. Furthermore, for the MG system to detect and classify faults quickly and reliably, the computing time of AI and ML-based techniques must be considered. MGs have recently been protected using a variety of AI and ML-based methods, including ANN, Fuzzy Logic (FL), Decision Tree (DT), and Support Vector Machine (SVM) [146]. An ANN-based protection device can quickly isolate faults by estimating their locations and enabling adaptive protection settings. Their capacity to generalize guarantees tolerance to noise and weak fault currents, while integration with signal processing techniques improves feature extraction and detection speed. Additionally, ANNs enhance microgrid resilience by supporting intelligent and dispersed protection. The authors of [147] use machine learning methods to enhance microgrid fault classification. For feature selection, pertinent statistical features are extracted from real-time current data using partial least squares (PLS). Accuracy can be improved by up to 10 % when these features are optimized for machine learning models. The model's robustness, adaptability, and overall resilience under various operating situations are further enhanced by utilizing data from nearby microgrid components. FL-based methods manage uncertainty and noisy measurements for accurate defect identification in the context of AI/ML-based protection solutions. Under changing load, DG penetration, and network conditions, they make adaptive fault classification possible. Furthermore, fuzzy logic facilitates distributed protection, guaranteeing resilience, stability, and selective isolation in microgrids controlled by inverters. The authors of [148] describe an enhanced voltage control approach for AC microgrid systems that compares performance using a Fuzzy Logic Controller (FLC) with a traditional Proportional Integral (PI) controller. Uncertainties resulting from discrepancies between mathematical models and actual systems are addressed in the study, especially those pertaining to LC filter components. Under such uncertainties, the FLC is intended to improve system robustness, dependability, and equitable power sharing. The efficiency of the proposed control under different system parameter adjustments is evaluated using the MATLAB/Simulink environment. It contains a number of test scenarios that assess the system's performance in terms of maximum overshoot, rising time, and settling time. The simulations show that the FLC provides more accurate voltage regulation and a quicker reaction than the PI controller. All things considered, the method greatly enhances AC microgrid optimization and disturbance resilience.

Furthermore, decision tree-based protection strategies are arranged hierarchically, with three different kinds of nodes—internal, leaf, and root nodes—connected by branches.

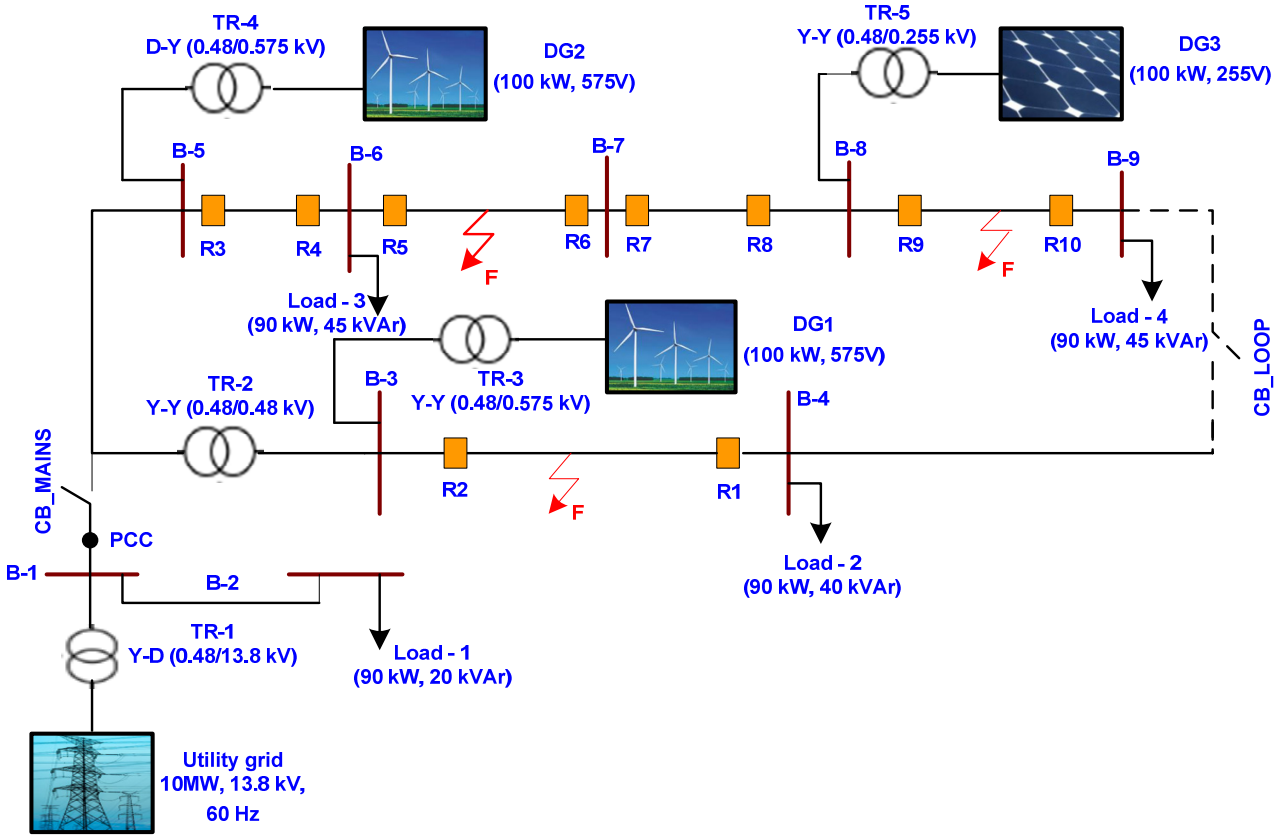

FIGURE 20. Topology of modified CERTS AC microgrid [154].

In power systems, time-frequency signal processing methods are typically used to process voltage and current signals in order to extract features related to fault occurrences. These characteristics are then utilized to train the decision tree for fault detection and classification. Decision tree algorithms facilitate multi-zone coordination, adaptive protection, and fault location estimation in microgrids. Reliability and resilience in inverter-dominated microgrids are improved by their resilience to noise and uncertainty. The authors of [149] provide machine learning (ML)-based protection methods that use local electrical data, take implementation issues into account, and successfully integrate type identification and short-circuit fault detection. Many different failure scenarios are analyzed using a decision tree method. A dataset is created using the PSCAD/EMTDC simulation environment in order to test and train the suggested approach. In PSCAD/EMTDC, a 4-bus microgrid is created with grid-forming first and third inverters and grid-following remaining inverters. A 100 % inverter-based microgrid with four inverters is used to test the efficacy of the suggested techniques under seven different failure types, each with differing fault resistance. Furthermore, support vector machines are supervised machine learning algorithms that are useful for regression, pattern recognition, and classification. As shown in Fig. 19, different characteristics (datasets) are categorized and separated by an iteratively created hyperplane in SVM-based protection approaches in order to maximize the margin between these classes. This approach is frequently applied in power systems, where fault-related features are recorded during the processing of voltage and current signals in order to train the SVM classifier to identify anomalies. SVM's primary benefits are adaptive protection and the ability to identify fault spots for quicker isolation. The authors of [150] suggest a two-level adaptive relay technique to stop nuisance tripping in dynamic grid-connected microgrids. While the second level uses a hybrid, Discrete Wavelet Transform (DWT)–Support Vector Machine (SVM) for fault detection, the first level uses a phase deviation reference block to identify typical operational behavior. This method ensures accurate fault diagnosis by adjusting to changes in energy sources, loads, and fault kinds. OPAL-RT hardware-in-the-loop and Raspberry Pi are used for real-time validation to show their dependability. The resilience of the technique in situations of capacitor switching, EV charging, and renewable variations is confirmed by the results.

It is clear from the reviewed works that establishing adaptive and high-performance fault detection and protection methods in contemporary AC microgrids requires

the successful integration of AI/ML and signal processing methodologies. The effectiveness of protection techniques on the protection devices of AC microgrids based on the best performances, including accuracy, speed, robustness, adaptability, response time, and scalability, is shown in Table 4.

VII. AC MICROGRID PROTECTION STRATEGIES: A CASE STUDY

In the United States, one of the most well-known microgrids is the low-voltage Consortium for Electric Reliability Technology Solutions (CERTS) microgrid. Researchers have used this testbed extensively to benchmark and validate different protection techniques. The network model is used as a testbed to assess several suggested approaches at medium and low voltage levels. Additional distributed generators (DGs) are incorporated into the benchmark system to function as a microgrid. The framework allows for a thorough investigation of microgrid configurations since it is sufficiently flexible to handle the modeling of both radial and meshed network structures. In order to illustrate this adaptability and assess different protection techniques, benchmark systems like the CERTS microgrid [151] and the IEEE standard test feeders [152] have been widely used. The authors of [153] used a modified IEEE 34-bus microgrid to verify their protection plans and to pinpoint the problems and fixes related to each protection technique. In order to address the first problem, the paper suggests a defect detection method based on the feeder current's modified short-time correlation transform (MSTCT). The second problem is addressed by defining a new directional element using the superimposed component of MSTCT. The developed technique is a cost-effective plan because it depends on the IED in each feeder. Through the integration of various distributed generator (DG) types, the IEEE 34-bus radial distribution test feeder was transformed to function as a microgrid. A modified CERTS microgrid is the microgrid system shown in Fig. 20 [154].

The protection measures have been validated by the wide use of the suggested model. Both islanded and grid-connected modes of operation are possible with the updated CERTS microgrid. In grid-connected mode, CERTS is considered a part of the distribution system and is supplied by the secondary of 3-phase distribution transformers rated at 0.48/13.8 kV, or by the DERs in islanded mode. The system model includes one solar source (DG-3), two wind sources (DG-1, DG-2), and three DGs. The system is subject to four loads, which are L1, L2, L3, and L4. Each protection method's relays are represented by R1 through R10, which are separated by 1 km. In the grid-linked or islanded mode, the switch at the Point of Common Coupling (PCC) connects or disconnects the three DGs from the grid. The solar PV and wind sources are connected to the system via a voltage source converter (VSC). The case study of modified CERTS microgrid protection techniques, including fault location, difficulties, problems, and solutions, is shown in Table 5.

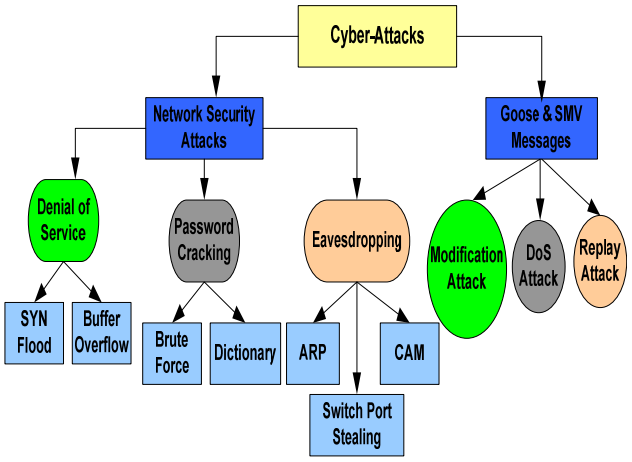

FIGURE 21. Taxonomy of various types of cyberattacks [156].

VIII. TECHNOLOGIES CHALLENGES OF PROTECTION DEVICES: CYBER-ATTACKS

The foundation of PDs in power systems, especially in the complex operational contexts of MGs, is communication technologies. The link between internal and external networks, such as the company network and the Internet, is particularly vulnerable to cyber threats in MGs' communication. Cyberattacks occur when hackers breach the microgrid's power enclaves by exploiting flaws in the system, network, and application levels, thereby jeopardizing vital functions [155]. The most challenging part of microgrid PDs is managing a significantly increased fault current magnitude when switching from grid to islanded mode because of the high reliance on real-time data exchange for proper coordination and operation. In these devices, the loss of proper communication to a relay can be disastrous. A protective strategy would be paralyzed in the case of a cyberattack or communication failure, in which case, relays would be unable to modify overcurrent limits. Especially in islanded mode, relay tripping may require 5–10 times the total load current. Interrupting messages between IEDs is the goal of security attacks in MGs' communication networks. The attacks can be carried out by taking advantage of Generic Object-Oriented Substation Events (GOOSE) and Sampled Measured Values (SMV) communications, or by employing standard network security techniques. Hence, this section explains the many cyberattacks that could affect PDs and stop communication networks from adapting to microgrids' dynamic changes. Fig. 21 shows the taxonomy of different kinds of cyberattacks [156], [157].

A. NETWORK SECURITY ATTACKS

Communication networks are used for network security attacks, which aim to alter, destroy, or gain unauthorized access to user data. Both insider threats and outside attackers are capable of carrying out these attacks. Increased expo-

TABLE 5. Case study of protection methods in CERTS AC microgrid [151], [152], [153], [154].

Protection methods	Fault type/location	Challenges/issues	Solution/mitigations
Overcurrent protection	L-G fault at Bus 4; Fault current = 4.2 kA; relay pick-up = 3.8 kA	High DG penetration causes coordination issues and increases the chance of annoyance tripping.	Use directional OCPD and modify relay settings to prevent miscoordination.
Voltage protection	Due to excessive PV generation, Bus 9 had an overvoltage of 1.0 p.u.	Hazard of tripping with typical swings in voltage from PV and WT.	Employ dynamic voltage restorers (DVRs) or OLTC transformers; configure relay time delays.
Ground fault protection	L-G fault at Bus 2; Fault current = 350 A	High fault impedance decreases sensitivity, whereas low-resistance faults are difficult to detect.	Employ relays with sensitive ground faults and zero-sequence overcurrent relays.
Distance protection	L-L fault on 10 km line between Bus 6–9; Relay reach = 8 km	Reach setting errors in meshed or radial microgrids; erroneous trips.	Employ an adaptive distance relay and modify the settings according to DG injection and topology.
Differential protection	Line differential protection on Bus 3–4; Fault current = 3 kA	CT saturation when fault currents are high; false tripping	Verify CT ratios, apply harmonic constraint, and use dual-slope characteristics.
Communication-based protection	Backup OCPD trip delayed by 50 ms on Bus 9	Loss or latency in GOOSE communications; dispersed relays not being coordinated.	Employ IEC 61850 GOOSE messaging, high-speed fiber optics, and communication redundancy.
Arc flash protection	Arc at transformer Bus 1; Peak current = 20 kA	Equipment can be damaged by high-current arcs; prompt detection is necessary.	Install arc flash relays, integrate current sensors and optical detectors, and adjust the trip time to less than one cycle.
Harmonic protection	5th harmonic = 12 % of fundamental at Bus 8	Inverter harmonics cause false tripping and relay malfunctions.	Installing passive/active filters, modifying trip thresholds, and using digital relays with harmonic blocking
Synchronization protection	Connecting DG at Bus 3 during reconnection; Phase difference = 12°	Reconnecting DGs incorrectly can harm the system.	Utilize synch-check relays; before closing, observe the voltage, frequency, and phase angle.
Adaptive protection	Load change plus DG injection at Bus 6; Fault current varies 2.5–4.5 kA	Static settings fail in a dynamic network with fluctuating load and DGs.	Real-time measuring adaptive relays that automatically modify settings according to topology.

sure to the internet, increased system automation, higher contact with external networks, and the presence of numerous independent systems are all regarded as potential risks to a microgrid. In addition, several network security attack types are covered in the next section [158].

1) DENIAL OF SERVICE

The process of denying access to a service by an authorized user is known as denial of service (DoS). Buffer overflow, SYN (synchronization) flood, and other DoS forms are the primary ones that might impact communication between PDs. The attacker sends a phony SYN request to the target IEDs repeatedly in order to distort the connection between the authorized user and the IEDs. By simultaneously running many protocols, such as FTP, HTTP, SNMP, NTP, and Telnet, on the IEDs, this kind of attack can be coordinated. In a similar vein, the attacker may write too much data to fill the buffer and send malicious code to an IED. Due to IEDs' vulnerability and the lack of security safeguards that would allow them to identify the malicious code, this attack is feasible [159].

2) PASSWORD CRACKING ATTEMPTS

This kind of attack is characterized as an effort to guess a password to obtain access to an IED, another device, or a system. A healthy component of the systems may be disconnected by the CBs as a result of a fake tripping signal sent by attackers with access to an IED. There are two methods for doing this: dictionary attacks and brute force attacks. To find the right password, a brute force approach arranges every potential password combination and attempts each one independently. This procedure may require a lot of time. The only thing involved in a dictionary attack is password guessing. Compared to the latter, this type might require less time. Hackers used FTP, HTTP, SNMP, and Telnet services that were already operational on the IEDs to crack the password in the password cracking attempt [160].

3) EAVESDROPPING ATTACKS

An attempt to steal packets being communicated across networks is known as an eavesdropping attack. Because the communications for FTP, HTTP, SNMP, NTP, and Telnet services are not encrypted, this kind of attack can be conducted from

within the local area network (LAN) and target these services. This attack can be classified into three categories. The first is cache poisoning of the Address Resolution Protocol (ARP). ARP is a communication mechanism that changes an IP address into an inaccurate MAC address (attacker of the MAC address). As a result, the switch forwards all packet addresses to the attacker, allowing the attacker to intercept those packets. The second is the flooding of the content-addressable memory (CAM) table. This is accomplished by inserting fictitious entries into the switch's CAM table. Upon reaching capacity, packets sent to MAC addresses not specified in the CAM table will be broadcast to the whole network, allowing for potential interception by adversaries. Lastly, switch port stealing occurs when the switch modifies the CAM table by receiving phony packets containing the target host's MAC address. This makes it possible for the MAC address to establish a connection with the interface that goes to the attacker [161].

B. GOOSE AND SMV MESSAGES ATTACKS

To communicate data in real time in electrical substations, the IEC 61850 standard specifies two essential communication protocols: GOOSE and SMV. The primary purpose of the GOOSE message is to isolate the problematic component from the system by sending a tripping signal to the CBs. The merging units communicate voltage and current values to the protective devices via SV messages. An Ethernet network that has been switched is used to send both messages. These messages have a four-millisecond transmission time. These protocols are also essential for modern microgrid systems' automation, control, and protection [162]. Several attacks that take advantage of SMV and GOOSE messages are covered in the section that follows.

1) GOOSE AND SMV MODIFICATION ATTACKS

In this kind of attack, the attacker modifies the message sent back and forth between the PDs without the publisher—who sends GOOSE messages—or the subscriber—who receives them—realizing it. There are two kinds of attacks. First, when the attacker intercepts the GOOSE message and replaces it with a different message, they gain control over the CBs. The SMV packet allows an attacker to take control of IEDs and induce a power outage by sending a fake analog value to a control center within the system. The second is that a malware script is used to carry out this kind of attack. The malware can intercept messages sent back and forth between IEDs, modify them, and then reintroduce GOOSE message packets into the IEC 61850 network. Installing the malware on a machine within the network is necessary for it to function. Attackers take advantage of a flaw in GOOSE messaging that prevents the use of digital signatures and encryption since the IEC 61850 standard mandates that GOOSE communications initiate protection actions in less than four milliseconds. It is therefore simple to intercept, alter, and retransmit a packet into the network in the absence of encryption and digital signatures [156], [162].

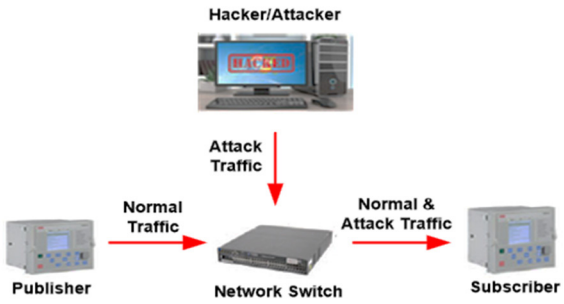

FIGURE 22. Design of the GOOSE poisoning attack [162].

2) GOOSE AND SMV DOS ATTACKS

These attacks prevent IEDs from responding to legitimate messages delivered by other IEDs. This is accomplished by bombarding the target IED with signals so frequent that it is unable to respond to a legitimate request. As illustrated in Fig. 22, GOOSE poisoning attacks are an additional DoS approach. By using a sequence number larger than the publisher, these attacks seek to persuade the subscriber to accept GOOSE messages. This vulnerability may cause subscribers to reject all genuine GOOSE messages from the publisher and start accepting bogus GOOSE messages from the attacker instead. This compromises the safety and integrity of the system by enabling the attacker to manage operations and manipulate protection within the microgrid. Moreover, GOOSE poisoning assaults have three different components: semantic attacks, high status number attacks, and high rate flooding attacks [162].

3) GOOSE AND SMV REPLAY ATTACKS

In this technique, the attacker records and retains GOOSE messages. When an attacker sends a message to trip the CBs during regular operation, it could cause unwanted activity. To launch an SMV message replay attack, the attacker can additionally record an SMV packet with specific power and current values and repeatedly send it to a different substation protection device. Unplanned outages can be caused by SMV packets that circulate across the system with identical power and voltage values [162].

IX. EMERGING TREND: COMMUNICATION TECHNOLOGY AND CYBER SECURITY ISSUES

The inclusion of communication networks and PDs has increased the attack surface of MGs, making them vulnerable to many forms of cyberattacks. Communication flaws that hackers could exploit include wireless communication, heterogeneous communication technologies, internet exposure, access to external networks, and several independent systems. Cyberattacks in MGs result in significant financial losses in addition to problems with data confidentiality and integrity.

Furthermore, the detrimental effects of such attacks could cause the MGs to become unavailable, and because effective mitigation techniques are lacking, the attacks could spread throughout the network. For microgrids to operate efficiently, PDs such as sensors, relays, IEDs, and CBs must communicate their operational data with one another at every node. To achieve data integrity, it is crucial to regularly monitor and analyze the data [163].

A. COMMUNICATION NETWORK

Communication technologies play a crucial role in MGs' protection measures, particularly in the intricate microgrid operating frameworks. Distribution networks cannot operate safely or effectively without communication and remote-control field devices. These technologies include both wired and wireless options to guarantee the defense's response and integrity. In communication networks, IEDs usually have communication ports and established communication protocols such as IEC 60834-1 [164], IEC 61850-9-3 [165], and IEEE 1815-2 [166] to create a direct connection with SCADA systems or remote terminal units (RTUs). Communication protocols describe the flow of data via the transmission channel.

1) WIRED COMMUNICATION NETWORK

In MGs, a wired communication link transfers data between different parts of the system, including sensors, smart meters, DERs, CBs, control centers, and protective relays, via physical wires. Nonetheless, this approach is well-known for its dependability and direct use of the power infrastructure, and it has long been employed in line protection applications. In an islanded microgrid, fiber optic cables may be used to link the inverters and protective relays to the central controller. When a defect occurs, signals are transmitted across the wired link to quickly isolate the problematic area, guaranteeing system security and stability. For microgrid control and protection to be high-performance, secure, and deterministic, wired communication lines are necessary. Despite their cost and stiffness, they are preferred in applications that need real-time performance, such as load control, fault protection, and system synchronization [167].

2) WIRELESS COMMUNICATION NETWORK

In dynamic microgrid contexts, wireless systems such as radio point-to-point communication and cellular networks (including 5G) provide flexibility and ease of deployment. Wireless communication technologies that can be utilized in MGs include Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4), WiMAX (IEEE 802.16), 5G/4G/3G/HSPA, and Radio Frequency (RF). A versatile, scalable, and economical option for microgrid monitoring and control is wireless communication. Although latency and reliability issues make them unsuitable for mission-critical protection, they are great for peer-to-peer energy trading, non-critical data exchange, remote monitoring, and Internet of Things (IoT) applications, particularly in rural or dynamic grid situations. In contrast to wired systems, wireless communication techniques may be more susceptible to latency, interference, and security flaws [167], [168].

B. CYBERSECURITY ISSUES

Many security monitoring and network security technologies that are resistant to cyberattacks have been proposed in recent years. However, the unique characteristics of energy networks and MGs make the use of cyber-protection strategies in the electrical industry necessary. Various security methods, including industry-standard cybersecurity solutions like encryption, access control, anti-malware, and attack detection, can be used to protect the microgrids. A cybersecurity framework is an essential tool for companies, especially those responsible for managing smart grid technology. With the use of such a framework, cybersecurity risks may be recognized, dealt with, and reduced systematically. The system provides a scalable and flexible method of handling cybersecurity threats and is built on five fundamental functions: identify, protect, detect, respond, and recover. To protect microgrid systems from the numerous cyber threats and attacks that could jeopardize their dependability and safety, cybersecurity requires a comprehensive strategy. In addition, cybersecurity should encompass risk management, threat landscape analysis, incident response and recovery, control system security, endpoint security, data security and privacy, awareness and training, and the creation of a secure communication infrastructure [169], [170].

In [171], the authors examine how cyberattacks affect microgrid PDs and suggest corrective actions to lessen these effects. Additionally, the authors suggest several steps to strengthen microgrid PDs' cybersecurity, including intrusion detection and prevention systems. Furthermore, the study does not thoroughly assess false alarm rates, real-time detection delay, or the ability of communication-assisted PDs to withstand coordinated cyber-physical attacks. In [172], the authors examine the effects of cybersecurity threats on microgrid defenses. The many types of cyberattacks that can be used to exploit the weaknesses in microgrid PDs are described by the authors. The usage of a human–machine interface (HMI) allows for both local and distant control and monitoring. The program ACSELERATOR Diagram BuilderSEL-5035 is used to create and manage HMI. Additionally, on an Ethernet-based interface, communication protocols like Modbus, sampled measured values (SMVs), generic object-oriented substation event (GOOSE), and distributed network protocol 3 (DNP3) were developed. These protocols map the correspondence between the corresponding nodes of the cyber-physical layers and synchronize data transmission between the systems. Additionally, they offer a risk assessment approach for analyzing the possible effects of cyberattacks on microgrid security. To show the testbed's capabilities, an attack scenario is also provided.

The aforementioned review studies provide a summary of how cybersecurity issues impact microgrid security, offering solutions to improve the cybersecurity of microgrid power

distribution networks and drawing attention to the potential effects of cyberattacks on these systems.

X. CYBER SECURITY USING ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is highly effective in cybersecurity applications because of its capacity to evaluate billions of data points, spot patterns in the data, and generate accurate predictions. When compared to conventional ways, AI techniques offer numerous benefits. Due to its ability to learn from the past, AI is better able to adapt to the new threats than traditional software-based systems, which have been unable to identify and adapt in response to the fast-expanding diversity of cyberthreats. AI can anticipate impending threats by employing advanced algorithms to identify attack patterns and anomalies in incoming data. AI also has advantages over current methods in terms of fighting botnets, improving endpoint security, and predicting breach risk. The dataset is crucial when utilizing AI for cybersecurity or any other purpose. Since the AI model is trained on the dataset, the dataset preparation creates the groundwork for the AI system to operate effectively. Traditional systems often consider a historical dataset that contains all malware information, attack trends, and event occurrences. It can be costly, challenging, and occasionally deceptive to obtain historical data. Cyber-physical systems (CPS) and MGs in particular use methods for creating synthetic datasets. A synthetic dataset is produced by mathematical models and simulation; the benefits of creating a synthetic dataset include the ability to easily gather data, flexibility in scaling datasets, and the ability to construct edge cases to train the model for outlier identification. Simple systems create their datasets using mathematical models, while more complicated systems create their datasets through simulation [173], [174].

In [175], the authors suggest a technique that combines ANNs and model predictive control (MPC) to detect and mitigate false data injection attacks (FDIA) in microgrids. To find abnormalities, the ANN estimates a reference voltage and compares it with the measured bus voltage after the FDIA targets the bus voltage relay. The technique is evaluated in several scenarios, such as time-varying attacks, load variations, physical events, and communication delays. When compared to a conventional proportional-integral (PI) controller, the MPC-based technique performs better in terms of accuracy and robustness. The authors of [176] investigate how to create an attack mitigation factor in response to FDIA on bus voltage relays by combining MPC and ANNs. The combined MPC–ANN framework allowed for quick mitigation of FDIAs, even when numerous units were the target of simultaneous, high-impact attacks, by continually analyzing input voltage data and identifying anomalous deviations from expected system behavior. Even when unfair, high-impact attacks target all units at once, the suggested approach successfully reduces FDIAs. Simulations using the MATLAB/Simulink environment were used to confirm the technique's efficacy.

Cyber-attack detection in microgrid systems, input-output modeling of nonlinear dynamical systems, and time series data prediction are applications of the nonlinear autoregressive model with exogenous inputs (NARX) ANN, a unique class of recurrent neural networks. In [177], the authors used NARX to identify FDIA in voltage sensor data. Attack data as well as real data are used to train the NARX model. When the output from the NARX model and the real sensor output diverge significantly, an FDIA is detected. A real-time digital simulator (RTDS) is used to illustrate the value of the suggested detection technique. In addition, the authors of [178] suggested an intelligent anomaly detection technique for cyber-physical inverter-based systems that differentiates between physical anomalies (like power system failures) and cyber anomalies (such as fake data injection and DoS assaults). They classified and localized anomalies using data-driven AI methods, particularly multi-class support vector machines (MSVM). The method's efficacy was demonstrated by comparing it with ANNs and Naive Bayes classifiers and validating it using OPAL-RT in real-time digital simulators.

According to all of the aforementioned articles, utilities may improve situational awareness, speed up threat reaction times, and preserve the MGs' dependability and security in the event of a cyber-physical attack by incorporating AI into the cybersecurity infrastructure of microgrid PDs. It is important to combine model-free methods like the ANN model with model-dependent factors like PI controllers. This combination frequently leads to an elevated computational burden and significant design complexity. Furthermore, the operation of the mitigation mechanism is impacted by the PI controllers' decreased efficiency during parametric change. Therefore, to safeguard MGs and lessen cyberattacks, a unified AI-based approach is required.

XI. LIMITATIONS OF ARTIFICIAL INTELLIGENCE

Assessment of power grid stability is essential for guaranteeing the security and dependability of power systems. Over the years, a lot of research has been done on the use of AI approaches in power systems, especially those that contain a sizable amount of RESs. Nonetheless, this section critically looks at several important restrictions that prevent AI from being used in practice to solve the problems in power systems. The percentage of RESs in the grid, the use of synthetic data, the lack of actual measurement data, difficulties with protection coordination and selectivity, and the intrinsic closed box effect of machine learning (ML) models were among the topics covered [179].

One drawback is that the percentage of RESs in a particular power system cannot be precisely measured. Studies that already exist frequently employ ambiguous criteria, like the high penetration of DERs, without offering quantifiable measurements. Experience from the real world shows that power systems can function well with as much as 30 % to 50 % DG from RESs without the need for novel AI-based methods for system protection and stability. Using synthetic

data instead of actual measurement data is another drawback. Most studies employed simulation-generated data to train ML models, which lacked the complexity and realism of real-world situations. Concerns regarding the operability and portability of ML-based protection systems in real power transmission networks are raised by this constraint. Moreover, developing and training machine learning models for power system stability and protection is more challenging in the absence of pertinent real measurement data. Fault incidents are uncommon since power systems are built to function for extended periods of time in steady-state settings. Consequently, the lack of common problem scenarios would make real system data, even if it were accessible, of limited use for training models. In the current state of research on ML-based protection approaches, there is a lack of emphasis on selectivity and coordination across many grid levels. Few studies have looked at how these methods work with protection systems at various voltage levels; hence, there is a dearth of thorough research on protective coordination and selectivity. The practical use of AI in power system protection is hampered by this dearth of research. Moreover, ML models often operate as ''closed boxes'' in the context of power systems, making it difficult for power operators to trust their conclusions. Because power systems must adhere to stringent accountability standards and have open decision-making processes, it may be challenging to understand how these models arrive at conclusions. Due to their lack of transparency, AI-based models may be difficult to validate and accept, making it challenging to support their recommendations and guarantee their use in power systems [180], [181].

Resolving issues with data scarcity and quality can be achieved by incorporating machine learning models influenced by physics. Furthermore, the increasingly advanced explainable artificial intelligence (XAI) can help power grid AI systems overcome the closed box effect. These developments hold promise for a time when sophisticated AI systems might be completely understood and effectively applied to power grid operation and energy system management [182].

XII. STANDARDIZATION AND REGULATION OF PROTECTION DEVICES

Standards developed specifically for microgrid protection must be distinguished from those that are more generally applicable but relevant to microgrids. The IEEE P3004.11 standard is especially pertinent since it covers the protection of switchgear and buses, which are essential parts frequently found in microgrid systems. This standard contributes to the overall safety and dependability of microgrid systems by offering recommendations on implementing complete protection methods against operational anomalies and malfunctions [183]. In microgrid PDs, the communication infrastructure is supported by the IEEE C37.94 and IEC 60834-1 standards. IEEE C37.94 describes interface standards for optical fiber communication between protection and control devices, ensuring fast and reliable data flow. IEC 60834-1 outlines the requirements for teleprotection equipment used over communication channels to guarantee prompt and secure protection signals. These standards work together to guarantee the reliability, speed, and integrity of communication networks that are necessary for coordinated protection in microgrid systems [164].

IEEE 1547 is a standard that specifically addresses MGs and DERs. In microgrid systems, it offers precise criteria for DER interconnection and interoperability. The standard focuses on two important areas: frequency stability and voltage management. The performance standards required to guarantee the safe, dependable, and well-coordinated integration of DERs into islanded and grid-connected microgrid modes [184]. Furthermore, IEC 61850-9-3 is a more general standard that is very pertinent to microgrid systems and was primarily created for substation automation. It makes it possible for monitoring, control, and PDs to operate effectively and communicate with one another. This is necessary for a microgrid's numerous components to be successfully integrated, coordinated, and managed. Security guidelines for the TC 57 series power system communication protocols are established by the International Electrotechnical Commission (IEC) 62351. These protocols provide key security objectives, including data authentication via digital signatures, protection against eavesdropping, spoofing, and replay attacks, and intrusion detection [165]. The NIST cybersecurity framework is a well-known collection of rules that offers a thorough method for controlling and reducing cybersecurity threats and applies to critical infrastructure. NIST 800-82 is a commonly used standard for industrial control system security. It ensures that certain security rules are applied appropriately and efficiently and offers guidance on how to use tools for vulnerability assessment and penetration testing [185].

To address the issues associated with microgrid protection, the IEEE Standard 2030.12-2025, ''Guide for the Design of Microgrid Protection Systems,'' was developed by the IEEE Power System Relaying and Control Committee (IEEE-PSRCC). An IEEE standard on microgrid protection systems was recently approved. It covers grid-connected and islanded modes, DER fault profiles, safe and dependable fault detection and clearing, and comprehensive support for selecting PDs and organizing microgrid-specific protective mechanisms.

XIII. DISCUSSION

Protective devices are crucial to a reliable and high-quality power supply. The device architecture also evolves as the power system is upgraded. However, as technology has advanced and the demand for greener and cleaner energy has grown, RESs have become increasingly important, and microgrids are becoming more popular. A thorough overview of the development of protective devices in power system setups is first presented in this work. This manuscript describes the progression from a centralized grid to a distributed power system, a further smart grid system, and device development. The first components in the power system are fuses and mechanical CBs. The CB is more dependable than

fuses because of its reusability, response time, and manual replacement. When electromechanical relays were introduced in the middle of the 20th century, protective devices saw a significant overhaul. As a combination of mechanical and electrical logic systems, it offers improved dependability and coordinated control. Later, in the late 20th century, more precise and excellent protection was offered by digital relays with communication and signaling capabilities. PLC-based and SCADA technologies were later developed to safeguard power systems. But since DERs were introduced, the difficulties in designing devices have multiplied. To guarantee dependable microgrid operation, the AC microgrid models rely on real-time monitoring, communication, and sophisticated control. Furthermore, its combination with AI, ML, signal processing, and adaptive control improves fault mitigation's selectivity, sensitivity, scalability, and resilience. Several mathematical modeling equations are used in this study to highlight the difficulties in microgrid safety related to different operating modes. Because of its versatility and operating range, overcurrent relays are utilized in AC microgrids. It performed effectively in both standalone and grid-connected modes. The main issues with overcurrent protection devices are selectivity and sensitivity to specific fault types. Voltage protection devices are then used in microgrids since they have the ability to regulate power quality and protection. This paper describes how to improve the traditional approach by using an advanced zone-based mechanism, an active power-based scheme, and a contemporary decision tree algorithm. The most dependable ways to deal with mode swings are isolation devices that are sensitive and interoperable. It is appropriate for AC microgrid protection by combining the most cutting-edge power electronics components with communication and machine learning methods. Furthermore, one of the main forms of AC microgrids, ground faults, can be addressed with innovative technologies to prevent significant damage. In this work, the significance, implications, and difficulties are thoroughly examined. In this paper, differential protective devices are subsequently reviewed. This study reviews the development of the synchro phasor and discusses the difficulties associated with inrush current and CT calibration. Similarly, in AC microgrids, the distance protection devices use the fundamental idea of impedance to reduce the fault. The use of DERs causes low current values to be a problem. The basic characteristics of an AC system are phase angle, frequency, current, and voltage. On the other hand, the directional device employs phase angle to identify faults. The ROCOF technique is used by frequency-based devices to coordinate and mitigate the problem because the penetration of various sources affects the frequency of the entire system. The main issues with these devices are frequency drift and integration with other schemes; however, they are particularly good at handling brief load-shedding situations. Under the constantly shifting operational conditions of AC microgrids, adaptive protective devices play a crucial role in this study as intelligent, self-tuning protection mechanisms that provide dependable fault detection, coordination, and system stability. They provide a link between the variable, data-driven requirements of contemporary distributed power systems and conventional fixed protection. According to this study, a communication protection device is essential to the equipment's durability and continued effectiveness. They facilitate quick fault isolation, adaptive coordination, real-time system awareness, and smooth integration with intelligent algorithms and renewable energy systems. However, communication protective devices must overcome the problems of low-latency, dependable, secure, and interoperable data exchange under scattered and dynamic operational situations. With the increasing use of DER in-power systems, harmonic, arc flash, and synchronization protection devices are therefore cutting-edge innovations. Protect against harmonic disturbances induced by nonlinear loads and inverter-based sources by identifying, evaluating, and reducing them. By preventing equipment damage, false tripping, and system inefficiencies, these technologies guarantee the reliable and safe functioning of contemporary microgrids. However, new types of harmonic distortion are introduced by the greater integration of IIDGs, non-linear loads, and complex network topologies, which also have an impact on the accuracy, coordination, and stability of fault detection. Arc flash contributes to device and individual safety. Synchronization devices aid in maintaining voltage, frequency, and phase angle synchronization between the DER and the main grid. Modern equipment and technologies make it possible for AC microgrids to run smoothly.

This paper provides a detailed evaluation of the integration problems, opportunities, and developments in each area of AC microgrid protection devices. In order to increase the device's power and, eventually, efficiency, several futuristic ideas and workable methods for fusing traditional legacy mechanics with cutting-edge contemporary techniques are presented in the next section.

XIV. FUTURE DIRECTION OF PROTECTION DEVICES

With the high penetration of RESs, the futuristic PDs' structure might change. Future power systems are predicted to have more linked RESs, such as solar and wind. As the demand for electrical energy rises, the protection and dependability of the power system will become increasingly crucial. For this reason, a central controller and a complete protective system are needed, and intelligent systems are used to handle the data for the central control system.

A. WIDE AREA PROTECTION

Wide Area Protection (WAP) is a control and protection system that can handle the protection issues of the future. The study of WAP systems has gained increasing attention because of its focus on wide-area longitudinal protection, wide-area current differential protection, and wide-area sequence components protection. WAP's performance is determined by power system data obtained via network communication. The WAP system synchronizes protective relays and enhances stability and dependability performance. It can swiftly and selectively identify and fix the problem. During

a malfunction, a WAP system's performance time is crucial. Furthermore, the WAP system employs the proper control methods and evaluates the impact of power system stability following the disconnection of fault components [186]. Security and stability control and relay protection are the two main areas of study for WAPS. According to the authors of [187], WAPS is primarily utilized in the security and stability control domain to avert long-term voltage collapse. It is based on the SCADA system, which has slow data refresh rates, non-real-time data collecting, and centralized decision-making mechanisms. The WAP system is positioned as an alternative to SCADA/EMS and traditional protection for system control and protection. Fast and real-time data sharing is not necessary for the communication system. Automatic reactive power control, flexible AC transmission (FACTS), remote load shedding, low-frequency and voltage load shedding, generator shedding, and system splitting are among the control measurements.

WAP systems may offer high-precision synchronous data acquisition, meet real-time requirements, and ensure data transmission reliability as a result of the growing availability of data synchronization, phasor measurement, and communication technologies used in microgrid systems. According to research, WAP appears to have a lot of promise for combining with communication-based IEC61850 protocol, adaptive protection, and multi-agent technology.

B. IMPORTANT RESEARCH AREA TO ENHANCE MICROGRID PROTECTION DEVICES

This section identifies some research areas that will impact the expansion of MG's protection plans. To fully realize PD's potential in the global energy transition, the following areas should be the focus of future research:

- Future research should prioritize the development of advanced microgrid protection systems that account for communication link time delays.
- Future studies should concentrate on creating strong cybersecurity plans to reduce the dangers associated with digital communication channels and protect company information from internet attacks.
- Future research should focus on developing standardized practices that address every microgrid security concern.
- Future research should examine fault detection in inverter-based microgrids with and without communication networks that are running in islanded mode.
- Future research should leverage AI and ML to provide predictive and fast failure reaction, which will increase the effectiveness and reliability of protection mechanisms.

XV. CONCLUSION

The protective devices are crucial for the interruption and high-quality power flow of the system. In light of the evolving DER and microgrid concepts, this study has provided a comprehensive examination of protection device advancements in AC microgrids, highlighting the vital role these devices play in maintaining grid integrity as the number of DERs rises. This study offers instances of the historical development and integration of diverse technologies over time to fill the research gap and offer context. The study's comprehensive results are presented along with a critical assessment of the contemporary issues surrounding AC microgrid security and its traditional solutions. This study was further enhanced by doing a case study using a system that demonstrated the difficulties, problems, and fixes of every protection technique. This study has emphasized the significance of AI and computational intelligence in cybersecurity based on microgrid protection. By examining the integration of AI in microgrid PDs, it is possible to increase the system's efficiency because of their superior endpoint protection, remarkable pattern recognition, and learning capabilities. This study also highlighted the importance of communication infrastructure in supporting PDs' responsiveness and dependability.

The study concludes by urging more research and development to improve these protective tactics, even though there has been a lot of improvement. It promotes a comprehensive method for creating microgrid protection plans that considers cybersecurity concerns, economic feasibility, and technical performance. The knowledge offered lays the groundwork for future study and application in this crucial area of power system engineering.

REFERENCES

[1] J. A. Rohten, J. J. Silva, J. A. Muñoz, F. A. Villarroel, D. N. Dewar, M. E. Rivera, and J. R. Espinoza, "A simple self-tuning resonant control approach for power converters connected to micro-grids with distorted voltage conditions," *IEEE Access*, vol. 8, pp. 216018–216028, 2020.

[2] K. H. Youssef, "Microgrid reliability considering directional protection failure and optimal load shedding," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 877–887, Mar. 2022.

[3] X. Li, Z. Li, L. Guo, J. Zhu, Y. Wang, and C. Wang, "Enhanced dynamic stability control for low-inertia hybrid AC/DC microgrid with distributed energy storage systems," *IEEE Access*, vol. 7, pp. 91234–91242, 2019.

[4] J. Lei, L. Yu, Y. Bie, Z. Xu, and Y. Xiao, "Review of energy management systems for islanded microgrids," *Power Gener. Technol.*, vol. 46, no. 2, pp. 370–385, Apr. 2025.

[5] J. S. Farkhani, M. Zareein, A. Najafi, R. Melício, and E. M. G. Rodrigues, "The power system and microgrid protection—A review," *Appl. Sci.*, vol. 10, no. 22, p. 8271, Nov. 2020.

[6] A. Srivastava, R. Mohanty, M. A. F. Ghazvini, L. A. Tuan, D. Steen, and O. Carlson, "A review on challenges and solutions in microgrid protection," in *Proc. IEEE Madrid PowerTech*, Madrid, Spain, Jun. 2021, pp. 1–6.

[7] N. Mazibuko, K. T. Akindeji, and K. Moloi, "A review on the impact of transmission line compensation and RES integration on protection schemes," *Energies*, vol. 17, no. 14, p. 3433, Jul. 2024.

[8] F. Alasali, H. Mustafa, A. S. Saidi, N. El-Naily, S. Abeid, W. Holderbaum, E. Omran, and S. M. Saad, "The recent development of protection coordination schemes based on inverse of AC microgrid: A review," *IET Gener., Transmiss. Distribution*, vol. 18, no. 1, pp. 1–23, Jan. 2024.

[9] P. T. Mana, K. P. Schneider, W. Du, M. Mukherjee, T. Hardy, and F. K. Tuffner, "Study of microgrid resilience through co-simulation of power system dynamics and communication systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1905–1915, Mar. 2021.

[10] T. S. Menezes, D. V. Coury, and R. A. S. Fernandes, "Dual-layer based microgrid protection using voltage synchrophasors," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT EUROPE)*, Oct. 2023, pp. 1–5.

[11] H. Karimi, B. Fani, and G. Shahgholian, "Multi agent-based strategy protecting the loop-based micro-grid via intelligent electronic device-assisted relays," *IET Renew. Power Gener.*, vol. 14, no. 19, pp. 4132–4141, Dec. 2020.

[12] R. A. G. Burbano, M. L. O. Gutierrez, J. A. Restrepo, and F. G. Guerrero, "IED design for a small-scale microgrid using IEC 61850," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7113–7121, Nov. 2019.

[13] A. Summers, T. Patel, R. Matthews, and M. J. Reno, "Prediction of relay settings in an adaptive protection system," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Apr. 2022, pp. 1–5.

[14] M. I. Abdelwanis and M. I. Elmezain, "A comprehensive review of hybrid AC/DC networks: Insights into system planning, energy management, control, and protection," *Neural Comput. Appl.*, vol. 36, no. 29, pp. 17961–17977, Aug. 2024.

[15] O. Azeem, M. Ali, G. Abbas, M. Uzair, A. Qahmash, A. Algarni, and M. R. Hussain, "A comprehensive review on integration challenges, optimization techniques and control strategies of hybrid AC/DC microgrid," *Appl. Sci.*, vol. 11, no. 14, p. 6242, Jul. 2021.

[16] S. C. Vegunta, M. J. Higginson, Y. E. Kenarangui, G. T. Li, D. W. Zabel, M. Tasdighi, and A. Shadman, "AC microgrid protection system design challenges—A practical experience," *Energies*, vol. 14, no. 7, p. 2016, Apr. 2021.

[17] X. Zhang and S. P. Azad, "A review of the protection of microgrids with converter-based resources," in *Proc. CIGRE Canada Conf. Expo*, 2020, pp. 1–8.

[18] A. Dagar, P. Gupta, and V. Niranjan, "Microgrid protection: A comprehensive review," *Renew. Sustain. Energy Rev.*, vol. 149, Oct. 2021, Art. no. 111401.

[19] S. Sarangi, B. K. Sahu, and P. K. Rout, "Review of distributed generator integrated AC microgrid protection: Issues, strategies, and future trends," *Int. J. Energy Res.*, pp. 1–28, Apr. 2021.

[20] D. Gutierrez-Rojas, P. H. J. Nardelli, G. Mendes, and P. Popovski, "Review of the state of the art on adaptive protection for microgrids based on communications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1539–1552, Mar. 2021.

[21] T. S. S. Senarathna and K. T. M. U. Hemapala, "Review of adaptive protection methods for microgrids," *AIMS Energy*, vol. 7, no. 5, pp. 557–578, 2019.

[22] M. W. Altaf, M. T. Arif, S. N. Islam, and Md. E. Haque, "Microgrid protection challenges and mitigation approaches–A comprehensive review," *IEEE Access*, vol. 10, pp. 38895–38922, 2022.

[23] B. Patnaik, M. Mishra, R. C. Bansal, and R. K. Jena, "AC microgrid protection—A review: Current and future prospective," *Appl. Energy*, vol. 271, Jun. 2020, Art. no. 115210.

[24] M. Usama, H. Mokhlis, M. Moghavvemi, N. N. Mansor, M. A. Alotaibi, M. A. Muhammad, and A. A. Bajwa, "A comprehensive review on protection strategies to mitigate the impact of renewable energy sources on interconnected distribution networks," *IEEE Access*, vol. 9, pp. 35740–35765, 2021.

[25] P. R. Satpathy, V. K. Ramachandaramurthy, and S. Padmanaban, "Advanced protection technologies for microgrids: Evolution, challenges, and future trends," *Energy Strategy Rev.*, vol. 58, Mar. 2025, Art. no. 101670.

[26] T. E. Sati, M. A. Azzouz, and M. F. Shaaban, "Harmonic dual-setting directional overcurrent protection for inverter-based islanded microgrids," *IEEE Access*, vol. 11, pp. 34630–34642, 2023.

[27] S. Sadeghi and H. Hashemi-Dezaki, "Optimal communication-free protection of meshed microgrids using non-standard overcurrent relay characteristics considering different operation modes and configurations based on N-1 contingency," *Sustain. Cities Soc.*, vol. 106, pp. 1–20, Jul. 2024.

[28] A. K. Erenoğlu, O. Erdinc, and A. Taıcıkaraoğlu, "History of electricity," in *Pathways to a Smarter Power System*. New York, NY, USA: Academic, 2019, pp. 1–27.

[29] C. Luo, Z. Xue, L. Wu, Z. He, D. Chen, and D. Liu, "Design of main wiring diagram drawing system of relay protection device," in *Proc. 16th Annu. Conf. China Electrotech. Soc.*, in Lecture Notes in Electrical Engineering. Singapore: Springer, Jan. 2022, pp. 511–518.

[30] M. Ginocchi, T. Penthong, F. Ponci, and A. Monti, "Statistical design of experiments for power system protection testing: A case study for distance relay performance testing," *IEEE Access*, vol. 12, pp. 27052–27072, 2024.

[31] M. Abbasi, E. Abbasi, L. Li, R. P. Aguilera, D. Lu, and F. Wang, "Review on the microgrid concept, structures, components, communication systems, and control methods," *Energies*, vol. 16, no. 1, p. 484, Jan. 2023.

[32] F. Norouzi, T. Hoppe, L. R. Elizondo, and P. Bauer, "A review of socio-technical barriers to smart microgrid development," *Renew. Sustain. Energy Rev.*, vol. 167, pp. 1–17, Oct. 2022.

[33] A. Vosughi, S. K. Sadanandan, and A. K. Srivastava, "Synchrophasor-based event detection, classification, and localization using koopman, transient energy matrix, best worth method, and dynamic graph," *IEEE Trans. Power Del.*, vol. 37, no. 3, pp. 1986–1996, Jun. 2022.

[34] C.-C. Deng, M.-F. Ge, Z.-W. Liu, and Y.-D. Wu, "Prescribed-time stabilization and optimization of CPS-based microgrids with event-triggered interactions," *Int. J. Dyn. Control*, vol. 12, no. 7, pp. 2522–2534, Dec. 2023.

[35] J. Zhao, Y. Zhang, Y. Yuan, and Y. Li, "Microgrid line protection method using the cosine similarity of the time domain traveling waveform," *Int. J. Electr. Power Energy Syst.*, vol. 153, pp. 1–12, Nov. 2023.

[36] S. Baidya and C. Nandi, "A comprehensive review on AC/DC microgrid protection devices," *Elect. Power Syst. Res.*, vol. 210, Sep. 2022, Art. no. 108051.

[37] R. R. Ferreira, P. J. Colorado, A. P. Grilo, J. C. Teixeira, and R. C. Santos, "Method for identification of grid operating conditions for adaptive overcurrent protection during intentional islanding operation," *Int. J. Electr. Power Energy Syst.*, vol. 105, pp. 632–641, Feb. 2019.

[38] A. K. Soni, A. Mohapatra, and S. N. Singh, "Protection coordination in AC microgrid via novel voltage-supervised directional overcurrent relays," *IEEE Trans. Power Del.*, vol. 39, no. 3, pp. 1549–1562, Jun. 2024.

[39] L. F. Serna-Montoya, S. D. Saldarriaga-Zuluaga, J. M. López-Lezama, and N. Muñoz-Galeano, "Optimal microgrid protection coordination for directional overcurrent relays through mixed-integer linear optimization," *Energies*, vol. 18, no. 8, p. 2035, Apr. 2025.

[40] R. Tiwari, R. K. Singh, and N. K. Choudhary, "Coordination of dual setting overcurrent relays in microgrid with optimally determined relay characteristics for dual operating modes," *Protection Control Modern Power Syst.*, vol. 7, no. 1, pp. 1–18, Dec. 2022.

[41] L. Ji, Z. Cao, Q. Hong, X. Chang, Y. Fu, J. Shi, Y. Mi, and Z. Li, "An improved inverse-time over-current protection method for a microgrid with optimized acceleration and coordination," *Energies*, vol. 13, no. 21, p. 5726, Nov. 2020.

[42] B. Fani, G. Shahgholian, H. Haes Alhelou, and P. Siano, "Inverter-based islanded microgrid: A review on technologies and control," *e-Prime Adv. Electr. Eng., Electron. Energy*, vol. 2, Sep. 2022, Art. no. 100068.

[43] H. Kilic, "Distributed cooperative fault tolerant optimal active power control in AC microgrid," *ISA Trans.*, vol. 142, pp. 98–111, Nov. 2023.

[44] P. Bishop and N. K. C. Nair, *Principles and Applications to Electric Power Systems*. Cham, Switzerland: Springer, 2023.

[45] A. N. Sheta, G. M. Abdulsalam, B. E. Sedhom, and A. A. Eladl, "Comparative framework for AC-microgrid protection schemes: Challenges, solutions, real applications, and future trends," *Protection Control Modern Power Syst.*, vol. 8, no. 1, pp. 1–40, May 2023.

[46] T. M. Thamizh Thentral, R. Palanisamy, S. Usha, A. Geetha, A. Reagan, and T. R. B. Ramanathan, "Implementation of protection circuit for over voltage and under voltage protection," *Mater. Today, Proc.*, vol. 45, pp. 2460–2464, Jan. 2021.

[47] P. T. Manditereza and R. C. Bansal, "Protection of microgrids using voltage-based power differential and sensitivity analysis," *Int. J. Electr. Power Energy Syst.*, vol. 118, Jun. 2020, Art. no. 105756.

[48] G. P. Santos, A. Tsutsumi, and J. C. M. Vieira, "Enhanced voltage relay for AC microgrid protection," *Electric Power Syst. Res.*, vol. 220, pp. 1–16, Jul. 2023.

[49] W. M. Hamanah, M. I. Hossain, M. Shafiullah, and M. A. Abido, "AC microgrid protection schemes: A comprehensive review," *IEEE Access*, vol. 11, pp. 76842–76868, 2023.

[50] H. J. Jun and H. S. Yang, "Performance of the XMPP and the MQTT protocols on IEC 61850-based microgrid communication architecture," *Energies*, vol. 14, no. 16, pp. 1–13, Aug. 2021.

[51] S. P. Gautam, M. Jalhotra, L. K. Sahu, A. H. Chander, and V. V. S. K. Bhajana, "A highly resilient fault tolerant topology of single phase multilevel inverter," *IEEE Access*, vol. 11, pp. 136934–136946, 2023.

[52] R. Chintakindi and A. Mitra, "WAMS challenges and limitations in load modeling, voltage stability improvement, and controlled island protection—A review," *Energy Rep.*, vol. 8, pp. 699–709, Apr. 2022.
[53] B. Fan, T. Liu, F. Zhao, H. Wu, and X. Wang, "A review of current-limiting control of grid-forming inverters under symmetrical disturbances," *IEEE Open J. Power Electron.*, vol. 3, pp. 955–969, 2022.
[54] M. Z. Isdy, T. Basak, and F. Nina, "Study of ground fault protection system in the medium voltage panel of the main powerhouse at the airport," *J. Airport Eng. Technol. (JAET)*, vol. 3, no. 2, pp. 89–95, Jun. 2023.
[55] Y. Bai, B. Yan, C. Zhou, T. Su, and X. Jin, "State of art on state estimation: Kalman filter driven by machine learning," *Annu. Rev. Control*, vol. 56, pp. 1–16, Oct. 2023.
[56] A. D. Scaife, "Improve predictive maintenance through the application of artificial intelligence: A systematic review," *Results Eng.*, vol. 21, pp. 1–24, Mar. 2024.
[57] V. E. Quincozes, S. E. Quincozes, D. Passos, C. Albuquerque, and D. Mossé, "Towards feature engineering for intrusion detection in IEC–61850 communication networks," *Ann. Telecommun.*, vol. 79, nos. 7–8, pp. 537–551, Feb. 2024.
[58] A. M. Joshua and K. P. Vittal, "Superimposed current based differential protection scheme for AC microgrid feeders," *Appl. Energy*, vol. 341, pp. 1–22, Jul. 2023.
[59] A. H. N. Tajani, A. Bamshad, and N. Ghaffarzadeh, "A novel differential protection scheme for AC microgrids based on discrete wavelet transform," *Electric Power Syst. Res.*, vol. 220, pp. 1–12, Jul. 2023.
[60] S. Sanati, I. Kamwa, B. Cao, B. Sheng, and X. Minghui, "A comprehensive review on differential protection schemes in IBR-dominated microgrids," *IEEE Access*, vol. 12, pp. 1–23, 2024.
[61] G. Wang, M. Huang, H. Bai, J. Li, R. Yao, H. Wang, and C. Li, "A current differential protection scheme for distribution networks with inverter-interfaced distributed generators considering delay behaviors of sequence component extractors," *Electronics*, vol. 12, no. 23, p. 4727, Nov. 2023.
[62] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 2, pp. 1294–1335, Mar. 2023.
[63] J. P. Desai, "Microgrid harmonic-restrained dual slope differential protection," *J. Inst. Engineers (India): Ser. B*, vol. 105, no. 2, pp. 297–308, Jan. 2024.
[64] K. Islam, D. Kim, and A. Abu-Siada, "A review on adaptive power system protection schemes for future smart and micro grids, challenges and opportunities," *Electric Power Syst. Res.*, vol. 230, pp. 1–17, May 2024.
[65] C. C. Nzeanorue and B. C. Okpala, "Smart grids and renewable energy integration: Challenges and solutions," *Path Sci.*, vol. 10, no. 9, pp. 3050–3060, Sep. 2024.
[66] D. Pansari, P. Sharma, M. S. Sonwani, R. Kumar, C. Sinha, and S. Dass, "Analysis of distance protection scheme for detecting HIF and various faults in power system," *Int. J. Electr. Electron. Eng.*, vol. 11, no. 6, pp. 70–75, Jun. 2024.
[67] J. D. Hernández-Santafé and E. Sorrentino, "Problems and solutions concerning the distance protection of transmission lines connected to inverter-based resources," *Energies*, vol. 18, no. 6, pp. 1–23, Mar. 2025.
[68] Y. Liang, W. Li, and W. Zha, "Adaptive mho characteristic-based distance protection for lines emanating from photovoltaic power plants under unbalanced faults," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3506–3516, Sep. 2021.
[69] M. Gilany, A. Al-Kandari, and J. Madouh, "A new strategy for determining fault zones in distance relays," *IEEE Trans. Power Del.*, vol. 23, no. 4, pp. 1857–1863, Oct. 2008.
[70] S. Sarangi, B. K. Sahu, and P. K. Rout, "High-impedance fault identification and location by using mode decomposition integrated adaptive multi-kernel extreme learning machine technique for distributed generator-based microgrid," *Electr. Eng.*, vol. 105, no. 1, pp. 383–406, Feb. 2023.
[71] U. Uzubi, A. Ekwue, and E. Ejiogu, "An adaptive distance protection scheme for high varying fault resistances: Updated results," *Scientific Afr.*, vol. 9, Sep. 2020, Art. no. e00528.
[72] A. K. Soni, A. Kumar, R. K. Panda, A. Mohapatra, and S. N. Singh, "Adaptive coordination of relays in AC microgrid considering operational and topological changes," *IEEE Syst. J.*, vol. 17, no. 2, pp. 3071–3082, Jun. 2023.
[73] K. E. Ojo, A. K. Saha, and V. M. Srivastava, "Review of advances in renewable energy-based microgrid systems: Control strategies, emerging trends, and future possibilities," *Energies*, vol. 18, no. 14, p. 3704, Jul. 2025.
[74] A. J. Taveras-Cruz, D. Mariano-Hernández, E. Jiménez-Matos, M. Aybar-Mejia, P. A. Mendoza-Araya, and A. Molina-García, "Adaptive protection based on multi-agent systems for AC microgrids: A review," *Appl. Energy*, vol. 377, pp. 1–16, Jan. 2025.
[75] N. Hussain, Y. Khayat, S. Golestan, M. Nasir, J. C. Vasquez, J. M. Guerrero, and K. Kauhaniemi, "AC microgrids protection: A digital coordinated adaptive scheme," *Appl. Sci.*, vol. 11, no. 15, p. 7066, Jul. 2021.
[76] A. A. Memon and K. Kauhaniemi, "An adaptive protection for radial AC microgrid using IEC 61850 communication standard: Algorithm proposal using offline simulations," *Energies*, vol. 13, no. 20, p. 5316, Oct. 2020.
[77] A.-H. Ataee-Kachoee, H. Hashemi-Dezaki, and A. Ketabi, "Optimized adaptive protection coordination of microgrids by dual-setting directional overcurrent relays considering different topologies based on limited independent relays' setting groups," *Electr. Power Syst. Res.*, vol. 214, Oct. 2022, Art. no. 108879.
[78] S. D. Saldarriaga-Zuluaga, J. M. López-Lezama, and N. Muñoz-Galeano, "Optimal coordination of over-current relays in microgrids considering multiple characteristic curves," *Alexandria Eng. J.*, vol. 60, no. 2, pp. 2093–2113, Apr. 2021.
[79] R. Kumari and B. K. Naick, "Enhancing protection in AC microgrids: An adaptive approach with ANN and ANFIS models," *Comput. Electr. Eng.*, vol. 115, pp. 1–18, Apr. 2024.
[80] *IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems*, IEEE Standard IEEE Standard 519-2022, IEEE, New York, NY, USA, 2022.
[81] D. Gonçalves, J. V. M. Farias, H. A. Pereira, A.-S.-A. Luiz, M. M. Stopa, and A. F. Cupertino, "Design of damping strategies for LC filter applied in medium voltage variable speed drive," *Energies*, vol. 15, no. 15, p. 5644, Aug. 2022.
[82] A. Rajamallaiah, S. P. K. Karri, M. L. Alghaythi, and M. S. Alshammari, "Deep reinforcement learning based control of a grid connected inverter with LCL-filter for renewable solar applications," *IEEE Access*, vol. 12, pp. 22278–22295, 2024.
[83] M. Zhang, J. Wang, S. Zhang, L. Gao, X. Guo, L. Chen, and Y. Xu, "Harmonic resonance analysis and impedance remodeling method of multi-inverter grid-connected system," *Electronics*, vol. 12, no. 17, p. 3684, Aug. 2023.
[84] Z. Liu, Y. Xu, H. Jiang, and S. Tao, "Study on harmonic impedance estimation and harmonic contribution evaluation index," *IEEE Access*, vol. 8, pp. 59114–59125, 2020.
[85] D. Wang, J. Zhang, and Y. Liu, "A communication-assisted distance protection for AC microgrids considering the fault-ride-through requirements of distributed generators," *J. Electr. Eng. Technol.*, vol. 18, no. 6, pp. 2545–2556, Dec. 2023.
[86] J. Cisneros Saldana and M. M. Begovic, "On communication-assisted line protection for multi-inverter microgrids," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2024, pp. 2917–2925.
[87] A. C. Adewole, A. D. Rajapakse, D. Ouellette, and P. Forsyth, "Centralized protection of networked microgrids with multi-technology DERs," *Energies*, vol. 16, no. 20, p. 7080, Oct. 2023.
[88] P. Arévalo, "A data-driven approach to microgrid fault detection and classification using Taguchi-CNN," *Neurocomputing*, vol. 451, pp. 1–11, Jan. 2025.
[89] E. D. Ayele, J. F. Gonzalez, and W. B. Teeuw, "Enhancing cybersecurity in distributed microgrids: A review of communication protocols and standards," *Sensors*, vol. 24, no. 3, p. 854, Jan. 2024.
[90] C. Tian, Z. Xu, L. Wang, and Y. Liu, "Arc fault detection using artificial intelligence: Challenges and benefits," *Math. Biosciences Eng.*, vol. 20, no. 7, pp. 12404–12432, 2023.
[91] *IEEE Guide for Performing Arc-Flash Hazard Calculations*, Standard IEEE 1584.1:2022, IEEE, New York, NY, USA, 2022.
[92] A. O. Friday, A. C. Nonso, and I. Simon, "Electrical arc flash safety detection in power distribution network," *J. Eng. Stud. Res.*, vol. 28, no. 4, pp. 61–70, Dec. 2022.
[93] K. Nowak, J. Janiszewski, and G. Dombek, "A new short-circuit hybrid device for the protection of low-voltage networks from the effects of an arc fault," *IEEE Access*, vol. 10, pp. 88678–88691, 2022.

[94] S. Nikolovski, D. Mlakic, and H. R. Baghaee, "Arc flash incident energy simulation in PV power plant connected to distribution network," in *Proc. Int. Conf. Smart Syst. Technol. (SST)*, Oct. 2018, pp. 171–178.

[95] G. Kou, J. Deverick, K. Phelps, T. Nguyen, and F. G. Velez-Cedeno, "Impact of distributed energy resources on arc flash incident energy," *IEEE Trans. Power Del.*, vol. 35, no. 2, pp. 531–539, Apr. 2020.

[96] S. R. K. Joga, P. Sinha, and M. K. Maharana, "Performance study of various machine learning classifiers for arc fault detection in AC microgrid," in *Proc. IOP Conf. Ser. Mater. Sci. Eng.*, Apr. 2021, vol. 1131, no. 1, pp. 1–6.

[97] M. Litwin, D. Zielinski, and K. Gopakumar, "Remote micro-grid synchronization without measurements at the point of common coupling," *IEEE Access*, vol. 8, pp. 212753–212764, 2020.

[98] X. Wang, M. G. Taul, H. Wu, Y. Liao, F. Blaabjerg, and L. Harnefors, "Grid-synchronization stability of converter-based resources—An overview," *IEEE Open J. Ind. Appl.*, vol. 1, pp. 115–134, 2020.

[99] M. Naderi, Q. Shafiee, F. Blaabjerg, and H. Bevrani, "Synchronization stability of interconnected microgrids with fully inverter-based distributed energy resources," *J. Modern Power Syst. Clean Energy*, vol. 11, no. 4, pp. 1257–1268, 2023.

[100] L. Fan, Z. Miao, and D. Ramasubramanian, "Transient algebraic impedance derivations and applications for PLL-synchronized IBRs," *IEEE Trans. Power Del.*, vol. 39, no. 1, pp. 683–686, Feb. 2024.

[101] A. Ghulomzoda, M. Safaraliev, P. Matrenin, S. Beryozkina, I. Zicmane, P. Gubin, K. Gulyamov, and N. Saidov, "A novel approach of synchronization of microgrid with a power system of limited capacity," *Sustainability*, vol. 13, no. 24, pp. 1–17, Dec. 2021.

[102] A. Vukojevic and S. Lukic, "Microgrid protection and control schemes for seamless transition to island and grid synchronization," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 2845–2855, Jul. 2020.

[103] A. V. Christopher, D. Samiappan, and R. Rengaswamy, "Automatic adaptive synchronization (A2S): A demand-based automatic synchronization for distribution generators in islanding mode," *Knowledge-Based Syst.*, vol. 275, pp. 1–15, Sep. 2023.

[104] A. A. Memon and K. Kauhaniemi, "Real-time hardware-in-the-loop testing of IEC 61850 GOOSE-based logically selective adaptive protection of AC microgrid," *IEEE Access*, vol. 9, pp. 154612–154639, 2021.

[105] J. S. Farkhani, M. Zareein, A. Naja, R. Melicio, and E. M. Rodrigues, "The power system and microgrid protection: A review," *Appl. Sci.*, vol. 10, no. 22, Nov. 2020, Art. no. 8066.

[106] S. Baloch and M. S. Muhammad, "An intelligent data mining-based fault detection and classification strategy for microgrid," *IEEE Access*, vol. 9, pp. 22470–22479, 2021.

[107] D. Lagos, V. Papaspiliotopoulos, G. Korres, and N. Hatziargyriou, "Microgrid protection against internal faults: Challenges in islanded and interconnected operation," *IEEE Power Energy Mag.*, vol. 19, no. 3, pp. 20–35, May 2021.

[108] N. Hussain, M. Nasir, J. C. Vasquez, and J. M. Guerrero, "Recent developments and challenges on AC microgrids fault detection and protection systems–A review," *Energies*, vol. 13, no. 9, p. 2149, May 2020.

[109] U. Markovic, D. Chrysostomou, P. Aristidou, and G. Hug, "Impact of inverter-based generation on islanding detection schemes in distribution networks," *Electric Power Syst. Res.*, vol. 190, pp. 1–9, Jan. 2021.

[110] S. D. Godwal, K. S. Pandya, S. C. Vora, C. R. Mehta, and V. R. Rajput, "Optimal overcurrent relay coordination for interconnected power systems: A proper approach and improved technique," *e-Prime Adv. Electr. Eng., Electron. Energy*, vol. 5, Sep. 2023, Art. no. 100248.

[111] M. W. Altaf, M. T. Arif, S. Saha, S. N. Islam, M. E. Haque, and A. M. T. Oo, "Effective protection scheme for reliable operation of multi-microgrid," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Dec. 2020, pp. 1–6.

[112] *Electrical Installations (Wiring Rules)*, Standard AS/NZS 3000:2018, Standards Australia/Standards New Zealand, Sydney, NSW, Australia, 2018.

[113] H. Laaksonen, K. Kauhaniemi, and S. Voima, "Protection system for future LV microgrids," in *Proc. CIRED 21st Int. Conf. Elect. Distrib.*, Frankfurt, Germany, Jun. 2020, pp. 1–4.

[114] J. I. D. Cisneros-Saldana, S. Samal, H. Singh, M. Begovic, and S. R. Samantaray, "Microgrid protection with penetration of DERs–A comprehensive review," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, College Station, TX, USA, Feb. 2022, pp. 1–6.

[115] J. E. Santos-Ramos, S. D. Saldarriaga-Zuluaga, J. M. López-Lezama, N. Muñoz-Galeano, and W. M. Villa-Acevedo, "Microgrid protection coordination considering clustering and metaheuristic optimization," *Energies*, vol. 17, no. 1, pp. 1–30, Dec. 2023.

[116] H. Q. Shah, J. Chakravorty, and N. G. Chothani, "Protection challenges and mitigation techniques of power grid integrated to renewable energy sources: A review," *Energy Fuels*, vol. 37, no. 8, pp. 4600–4619, Apr. 2023.

[117] M. B. Atsever and M. H. Hocaoglu, "Mitigation of sympathy trips in highly cabled non-effectively earthed radial distribution systems via MINLP," *Electric Power Syst. Res.*, vol. 220, Jul. 2023, Art. no. 109377.

[118] K.-Y. Choi, S.-I. Kim, S.-H. Jung, and R.-Y. Kim, "Selective frequency synchronization technique for fast grid connection of islanded microgrid using prediction method," *Int. J. Electr. Power Energy Syst.*, vol. 111, pp. 114–124, Oct. 2019.

[119] N. P. Gupta and P. Paliwal, "Novel droop integrated technique for regulation of islanded and grid connected hybrid microgrid," *Int. J. Power Energy Convers.*, vol. 12, no. 2, pp. 89–114, 2021.

[120] L. Ward, A. S. Subburaj, A. Demir, M. Chamana, and S. Bayne, "Analysis of grid-forming inverter controls for grid-connected and islanded microgrid integration," *Sustainability*, vol. 16, no. 5, p. 2148, Mar. 2024.

[121] A. B. Nassif, "A protection and grounding strategy for integrating inverter-based distributed energy resources in an isolated microgrid," *CPSS Trans. Power Electron. Appl.*, vol. 5, no. 3, pp. 242–250, Sep. 2020.

[122] S. Sanati, M. Azzouz, and A. S. A. Awad, "Adaptive auto-reclosing and active fault detection of lines emanating from wind farms in microgrids," *IEEE Trans. Energy Convers.*, vol. 39, no. 1, pp. 389–399, Mar. 2024.

[123] A. Aggarwal, A. S. Siddiqui, and S. Mishra, "Bi-directional power flow through an interlinking converter in an autonomous hybrid micro-grid," in *Proc. IEEE 4th Int. Conf. Comput., Power Commun. Technol. (GUCON)*, Greater Noida, India, Sep. 2021, pp. 1–6.

[124] K. P. Bharti, H. Ashfaq, R. Kumar, and R. Singh, "Designing a bidirectional power flow control mechanism for integrated EVs in PV-based grid systems supporting onboard AC charging," *Sustainability*, vol. 16, no. 20, p. 8791, Oct. 2024.

[125] A. Shobole, M. Baysal, M. Wadi, and M. R. Tur, "An adaptive protection technique for smart distribution network," *Elektronika ir Elektrotechnika*, vol. 26, no. 4, pp. 46–56, Aug. 2020.

[126] R. Jain, D. L. Lubkeman, and S. M. Lukic, "Dynamic adaptive protection for distribution systems in grid-connected and islanded modes," *IEEE Trans. Power Del.*, vol. 34, no. 1, pp. 281–289, Feb. 2019.

[127] M. Karimi, M. Farshad, Q. Hong, H. Laaksonen, and K. Kauhaniemi, "An islanding detection technique for inverter-based distributed generation in microgrids," *Energies*, vol. 14, no. 1, p. 130, Dec. 2020.

[128] B. Sujatha, J. P. Roselyn, and P. Sundaravadivel, "Enhancing microgrid protection through adaptive decentralized relay coordination: A solution to blinding and sympathetic tripping," *IEEE Access*, vol. 1, pp. 1–17, 2025.

[129] E. Gómez-Luna, J. De La Cruz, and J. C. Vasquez, "New approach for validation of a directional overcurrent protection scheme in a ring distribution network with integration of distributed energy resources using digital twins," *Energies*, vol. 17, no. 7, p. 1677, Apr. 2024.

[130] M. A. Hajahmed, M. Hawa, L. A. Shamlawi, S. Alnaser, Y. Alsmadi, and D. Abualnadi, "Cognitive Radio_Based backup protection scheme for smart grid applications," *IEEE Access*, vol. 8, pp. 71866–71879, 2020.

[131] S. Baloch, S. S. Samsani, and M. S. Muhammad, "Fault protection in microgrid using wavelet multiresolution analysis and data mining," *IEEE Access*, vol. 9, pp. 86382–86391, 2021.

[132] E. Abbaspour, B. Fani, I. Sadeghkhani, and H. H. Alhelou, "Multi-agent system-based hierarchical protection scheme for distribution networks with high penetration of electronically-coupled DGs," *IEEE Access*, vol. 9, pp. 102998–103018, 2021.

[133] H. S. Samkari and B. K. Johnson, "Time-domain protection scheme for microgrids with aggregated inverter-based distributed energy resources," *IEEE Access*, vol. 11, pp. 13232–13242, 2023.

[134] L. Tightiz and H. Yang, "Resilience microgrid as power system integrity protection scheme element with reinforcement learning based management," *IEEE Access*, vol. 9, pp. 83963–83975, 2021.

[135] M. A. Dawoud, D. K. Ibrahim, M. I. Gilany, and A. El'Gharably, "Robust coordination scheme for microgrids protection based on the rate of change of voltage," *IEEE Access*, vol. 9, pp. 156283–156296, 2021.

[136] M. W. Altaf, M. T. Arif, S. Saha, S. N. Islam, Md. E. Haque, and A. M. T. Oo, "Effective ROCOF-based islanding detection technique for different types of microgrid," *IEEE Trans. Ind. Appl.*, vol. 58, no. 2, pp. 1809–1821, Mar. 2022.

[137] F. Alsaeidi, C.-C. Liu, and L.-A. Lee, "Graph-theoretic partitioning for differential zone protection in an islanded microgrid," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Jan. 2023, pp. 1–5.

[138] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the Internet of Things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," *Computers*, vol. 9, no. 2, p. 44, May 2020.
[139] S. Bhaumik, A. Chattopadhyaya, and J. N. Bera, "Detection and classification of faults in renewable energy penetrated stand-alone microgrids using SVM and DWT techniques," *Elect. Power Syst. Res.*, vol. 245, pp. 1–16, Mar. 2025.
[140] N. Giri, P. Nayak, R. Kumar Mallick, S. Mishra, A. Flah, H. Kraiem, L. Prokop, and M. Kanan, "Wavelet-based ensembled intelligent technique for a better quality of fault detection and classification in AC microgrids," *Energy Convers. Management: X*, vol. 24, pp. 1–16, Oct. 2024.
[141] Y. Han, R. Ma, T. Li, W. Zeng, Y. Liu, Y. Wang, C. Guo, and J. Liao, "Fault detection and zonal protection strategy of multi-voltage level DC grid based on fault traveling wave characteristic extraction," *Electronics*, vol. 12, no. 8, pp. 1–26, Apr. 2023.
[142] M. Jiménez-Aparicio, J. Hernández-Alvidrez, A. Y. Montoya, and M. J. Reno, "Embedded, real-time, and distributed traveling wave fault location method using graph convolutional neural networks," *Energies*, vol. 15, no. 20, p. 7785, Oct. 2022.
[143] J. A. Vasquez, M. Jaramillo, and D. Carrión, "An intelligent framework for multiscale detection of power system events using Hilbert–Huang decomposition and neural classifiers," *Appl. Sci.*, vol. 15, no. 12, p. 6404, Jun. 2025.
[144] A. R. Aqamohammadi, T. Niknam, S. Shojaeiyan, P. Siano, and M. Dehghani, "Deep neural network with Hilbert–Huang transform for smart fault detection in microgrid," *Electronics*, vol. 12, no. 3, p. 499, Jan. 2023.
[145] E. Güney, O. Çakmak, and Ç. Kocaman, "Classification of stockwell transform based power quality disturbance with support vector machine and artificial neural networks," *J. Intell. Systems, Theory Appl.*, vol. 5, no. 1, pp. 75–84, Mar. 2022.
[146] M. Singh, O. Singh, and M. A. Ansari, "Analysis of intelligent machine learning techniques for the protection of AC microgrid," *J. Electr. Syst.*, vol. 20, no. 9, pp. 1482–1498, Jun. 2024.
[147] T. A. Azizov, E. Tulovov, M. Khalmirzaev, O. Mukhitdinov, A. N. Nizamov, I. Sapaev, T. Rakhmonov, M. Y. S. Yunusova, B. B. M. Bobokulov, O. K. U. Bobojonov, U. Tulakov, and R. Kholikov, "Machine learning based fault detection and classification in microgrid," *J. Oper. Autom. Power Eng.*, vol. 12, pp. 43–52, Dec. 2024.
[148] S. Adiche, M. Larbi, and D. Toumi, "Optimizing voltage control in AC microgrid systems with fuzzy logic strategies and performance assessment," *Electr. Eng. Electromechanics*, no. 3, pp. 11–17, May 2025.
[149] M. Beikbabaei, M. Lindemann, M. H. Kapourchali, and A. Mehrizi-Sani, "Machine learning-based protection and fault identification of 100 % inverter-based microgrids," in *Proc. IEEE 33rd Int. Symp. Ind. Electron. (ISIE)*, Jun. 2024, pp. 1–7.
[150] D. S. Nair, T. N. Rajeev, and S. Miraj, "Enhanced fault identification in grid-connected microgrid with SVM-based control algorithm," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 36, no. 1, pp. 115–126, Oct. 2024.
[151] B. Somda, A. K. Jain, H. B. Ashraf, C.-C. Liu, R. Zhang, A. K. Bharati, F. Tuffner, K. Schneider, and D. Ton, "Testbed demonstration of a microgrid building block prototype," in *Proc. 50th Annu. Conf. IEEE Ind. Electron. Soc.*, Chicago, IL, USA, Nov. 2024, pp. 1–6.
[152] H. Chang and L. Vanfretti, "Power hardware-in-the-loop smart inverter testing with distributed energy resource management systems," *Electronics*, vol. 13, no. 10, p. 1866, May 2024.
[153] K. Allahdadi, I. Sadeghkhani, and B. Fani, "Protection of converter-interfaced microgrids using modified short-time correlation transform," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5172–5175, Dec. 2020.
[154] F. Xie, J. Wang, S. Ganguly, S. Singh, W. Wang, J. Baum, and R. R. Jha, "Controller hardware-in-the-loop evaluation of a microgrid controller for a microgrid system with multiple grid-forming inverters," in *Proc. IEEE Energy Convers. Congr. Exposit. (ECCE)*, Oct. 2024, pp. 804–811.
[155] S. Koduru, V. S. P. Machina, and S. Madichetty, "Cyber-attacks in cyber-physical microgrid systems: A comprehensive review," *Energies*, vol. 16, no. 4573, pp. 1–36, Jun. 2023.
[156] S. H. Rouhani, C.-L. Su, S. Mobayen, N. Razmjooy, and M. Elsisi, "Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions," *Energy*, vol. 309, Nov. 2024, Art. no. 133081.
[157] C. Li, X. Wang, X. Chen, A. Han, and X. Zhang, "Data-driven attack detection mechanism against false data injection attacks in DC microgrids using CNN-LSTM-attention," *Symmetry*, vol. 17, no. 7, p. 1140, Jul. 2025.
[158] A. S. Alqahtani, O. A. Altammami, and M. A. Haq, "A comprehensive analysis of network security attack classification using machine learning algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 4, pp. 1269–1280, 2024.
[159] I. Ortega-Fernandez and F. Liberati, "A review of denial of service attack and mitigation in the smart grid using reinforcement learning," *Energies*, vol. 16, no. 2, p. 635, Jan. 2023.
[160] A. Awelewa, E. Ezenwanne, K. Ojo, I. Samuel, and P. Olawale, "Impact of a Web based crowdfunding application for renewable energy projects in Nigeria," in *Proc. Int. Conf. Smart Appl., Commun. Netw. (SmartNets)*, Istanbul, Turkey, Jul. 2023, pp. 1–8.
[161] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Syst. Res.*, vol. 215, Feb. 2023, Art. no. 108975.
[162] O. A. Tobar-Rosero, O. A. Roa-Romero, G. D. Rueda-Carvajal, A. Leal-Piedrahita, J. F. Botero-Vega, S. A. Gutierrez-Betancur, J. W. Branch-Bedoya, and G. D. Zapata-Madrigal, "GOOSE secure: A comprehensive dataset for in-depth analysis of GOOSE spoofing attacks in digital substations," *Energies*, vol. 17, no. 23, p. 6098, Dec. 2024.
[163] C. Yan, Y. Han, P. Yang, and C. Wang, "Microgrid cybersecurity: Addressing challenges and ensuring resilience," in *Proc. IEEE 4th China Int. Youth Conf. Electr. Eng. (CIYCEE)*, Dec. 2023, pp. 1–12.
[164] *Teleprotection Equipment of Power Systems—Performance and Testing—Part–1: Command Systems, Gulf Standard, Current Edition*, Standard IEC 60834 1:2014, GSO, Geneva, Switzerland, Dec. 25, 2014.
[165] *Communication Networks and Systems for Power Utility Automation—Part 9-3: Precision Time Protocol Profile for Power Utility Automation, Gulf Standard, Current Edition*, Standard IEC/IEEE 61850 9 3:2025, GSO, Apr. 22, 2025.
[166] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, IEEE Standard P1815.2-2019, IEEE, New York, NY, USA, 2019.
[167] J. I. D. Cisneros-Saldana, S. Samal, M. M. Begovic, and S. R. Samantaray, "On protection schemes for AC microgrids: Challenges and opportunities," *IEEE Trans. Ind. Appl.*, vol. 60, no. 3, pp. 4843–4854, May 2024.
[168] R. Zurawski, *The Industrial Communication Technology Handbook*. Boca Raton, FL, USA: CRC Press, 2015.
[169] F. Nejabatkhah, Y. W. Li, H. Liang, and R. R. Ahrabi, "Cyber-security of smart microgrids: A survey," *Energies*, vol. 14, no. 1, p. 27, Dec. 2020.
[170] K. E. Ojo, A. K. Saha, and V. M. Srivastava, "Microgrids' control strategies and real-time monitoring systems: A comprehensive review," *Energies*, vol. 18, no. 13, p. 3576, Jul. 2025.
[171] K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg, and P. Popovski, "On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids," *Energies*, vol. 14, no. 16, pp. 1–30, Aug. 2021.
[172] A. Mohammad Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin, and E. F. El-Saadany, "Anomaly-based detection of cyberattacks on line current differential relays," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4787–4800, Nov. 2022.
[173] M. L. T. Zulu, R. P. Carpanen, and R. Tiako, "A comprehensive review: Study of artificial intelligence optimization technique applications in a hybrid microgrid at times of fault outbreaks," *Energies*, vol. 16, no. 4, pp. 1–32, Feb. 2023.
[174] H. Ahmad, M. M. Gulzar, G. Mustafa, A. Q. Khan, S. Habib, and I. Ahmed, "AI-enabled frequency synchronization control considering FDI attack using metaheuristic algorithm," *Neural Comput. Appl.*, vol. 37, no. 22, pp. 17541–17570, Jan. 2025.
[175] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragicevic, "Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1487–1498, Mar. 2022.
[176] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragicevic, and F. Blaabjerg, "Decentralized coordinated cyberattack detection and mitigation strategy in DC microgrids based on artificial neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4629–4638, Aug. 2021.
[177] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5294–5310, Oct. 2021.
[178] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Electric Power Syst. Res.*, vol. 193, pp. 1–13, Apr. 2021.

[179] A. E. Rhatrif, B. Bouihi, and M. Mestari, "Challenges and limitations of artificial intelligence implementation in modern power grid," *Proc. Comput. Sci.*, vol. 236, pp. 83–92, Jan. 2024.
[180] J. Pateras, P. Rana, and P. Ghosh, "A taxonomic survey of physics-informed machine learning," *Appl. Sci.*, vol. 13, no. 12, p. 6892, Jun. 2023.
[181] W. Fu, Y. Yan, Y. Chen, Z. Wang, D. Zhu, and L. Jin, "Temporal false data injection attack and detection on cyber-physical power system based on deep reinforcement learning," *IET Smart Grid*, vol. 7, no. 1, pp. 78–88, Feb. 2024.
[182] W. Saeed and C. Omlin, "Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities," *Knowledge-Based Syst.*, vol. 263, pp. 1–12, Mar. 2023.
[183] *IEEE Draft Recommended Practice for Bus and Switchgear Protection in Industrial and Commercial Power Systems*, IEEE Standard P3004.11/D1e, Jun. 2019.
[184] *IEEE Draft Guide To Using IEEE Standard 1547™ for Interconnection of Energy Storage Distributed Energy Resources With Electric Power Systems*, IEEE Standard P1547.9/D5.4, Feb. 2022.
[185] S. Deshpande and M. Damle, "Enhancing IoT security: A pursuit of excellence through the NIST 800–53 cybersecurity framework," in *Proc. 7th Int. Conf. Comput. Intell. andCommunication Technol. (CCICT)*, Apr. 2025, pp. 337–344.
[186] H. Rezapour, S. Jamali, and P. Siano, "Wide-area protection system for radial smart distribution networks," *Appl. Sci.*, vol. 14, no. 11, p. 4862, Jun. 2024.
[187] R. He, S. Yang, J. Deng, T. Feng, L. L. Lai, and M. Shahidehpour, "Reliability analyses of wide-area protection system considering cyber-physical system constraints," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3458–3467, Jul. 2021.

KAYODE EBENEZER OJO received the B.Tech., M.Tech., and Ph.D. degrees in electrical and electronic engineering from Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He is currently a Postdoctoral Researcher with the Department of Electrical, Electronic, and Computer Engineering with the University of KwaZulu-Natal, Durban, South Africa. He is a Registered Electrical Engineer. His research interests include power and control, system modeling, and instrumentation.

AKSHAY KUMAR SAHA (Senior Member, IEEE) is a Professor and an Academic Leader of research and higher degrees with the School of Engineering, University of KwaZulu-Natal, Durban, South Africa. He has published more than 85 articles in top-tier international journals and more than 100 international conference papers in relevant areas. His research interests include the advancement of power systems in various areas, including engineering education. He is a Registered Professional Engineer with the Engineering Council of South Africa. He is a fellow of South African Institute of Electrical Engineers and South African Academy of Engineering, a member of the Academy of Sciences of South Africa, a Senior Member of SAIMC, an Individual Member of Cigre, and a Life Member of IEEE-HKN. He was awarded the Best Lecturer in electrical engineering by the School of Engineering, University of KwaZulu-Natal, from 2013 to 2014 and from 2016 to 2019. He was also awarded the Research Excellence Award, from 2015 to 2024 and Top-30 Publishing Research Award, from 2020 to 2022, by the University of KwaZulu-Natal. He is the Editor-in-Chief of a top-tier international journal along with an associate/academic/guest editor and an editorial board member for several top-tier international journals.

VIRANJAY M. SRIVASTAVA (Senior Member, IEEE) received the bachelor's degree in electronics and instrumentation engineering, in 2002, the master's degree in VLSI design, in 2008, and the Ph.D. degree in RF microelectronics and VLSI design, in 2012. He has worked on the fabrication of devices and the development of circuit design. He is currently with the Department of Electronic Engineering, Howard College, University of KwaZulu-Natal, Durban, South Africa. He has more than 18 years of teaching and research experience in the areas of VLSI design, RFIC design, and analog IC design. He has supervised various bachelor's, master's, and doctoral theses. He is the author/co-author of more than 220 scientific contributions, including articles in international refereed journals and conferences, and also the author of various books. He is a Professional Engineer with ECSA, South Africa. He is a Senior Member of SAIEE and a member of IET, IEEE-HKN, and IITPSA. He has worked as a reviewer for several journals and conferences, both national and international.