Chapter 1

Introduction

1.1 General

Power generation units, transmission systems, and distribution networks are consistently growing to meet increasing energy demands, while also aiming to reduce the environmental footprint of conventional non-renewable energy sources. The ongoing technological evolution of renewable energy-based distributed generation (DG) systems, particularly photovoltaic (PV) arrays and wind energy conversion systems (WECS), is significantly enhancing their energy conversion efficiency, operational reliability, and lifecycle cost competitiveness, thereby promoting their integration into modern power systems. DG, defined as decentralized power generation units with capacities typically ranging from a few kilowatts to several megawatts and located near load centers within distribution networks, has seen substantial advancement [1]. Microgrids, characterized as autonomous electrical subsystems integrating various distributed energy resources (DERs), are increasingly recognized as an effective platform to support the widespread deployment and operational integration of DER technologies into the power grid [2, 3].

Microgrids can be categorized (Fig. 1.1) into AC or DC, depending on the nature of the common bus to which sources and loads are connected. Hybrid AC-DC microgrid is another type where both AC and DC buses are present to interface AC and DC sources and loads with reduced conversion stages. Compared to AC, DC microgrids (Fig. 1.2) have advantages, including reduced conversion stages for modern DC electronic loads [4], increased power transfer capacity, higher efficiency, and less cable loss due to the absence of the skin effect [5, 6, 7]. Further, there is no corona loss, synchronization and reactive

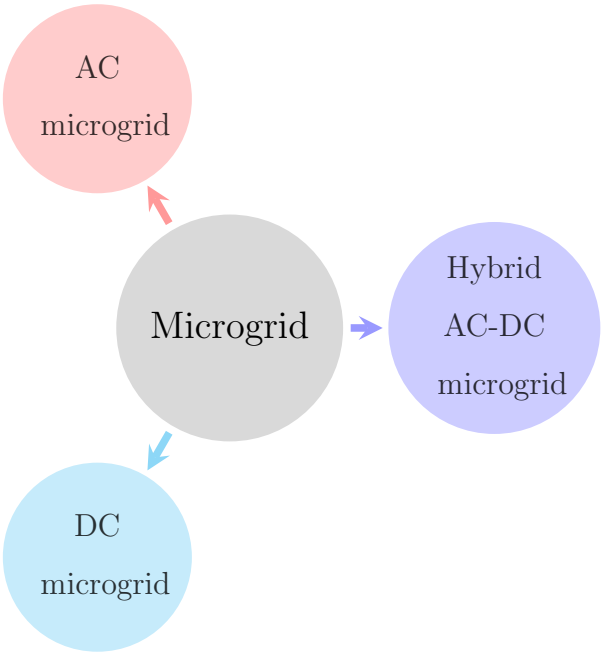

Figure 1.1: Typical classification of microgrid.

power management issue in DC system [8].

A DC microgrid may be unipolar or bipolar. Unipolar system is simple to implement and has no voltage asymmetry, whereas a voltage balancer circuit is required in a bipolar DC microgrid to overcome any potential asymmetry between the two pole voltages [9]. Furthermore, in case of asymmetry between the positive and negative poles, current flows through the neutral. As a result, a neutral conductor is needed since ground currents are typically prohibited because they lead to corrosion [10]. Such configuration is helpful for supplying load at three different voltage levels $V_{dc}, -V_{dc}$, and $2V_{dc}$, as shown in Fig. 1.3. Here, V_{dc} is the magnitude of pole-to-ground voltage. A bipolar DC also increases the reliability of the power supply because, in case of a fault in one pole, the power can still be supplied using the remaining poles [11, 12, 13, 14]. Considering these advantages, a bipolar configuration has been utilized in the DC microgrid with different voltage levels. The major applications include ±190 V for data centers [15], ±170 V for residential complexes [11], ±600 V for electric mobility applications [16], and research and experimental practices [17].

Integrating microgrids with renewable energy sources to the national grid has several advantages. With the increase in inherent DC sources, such as solar power plants, wind power plants [18], and DC electric loads [19], like electric vehicles [20], data centers, and

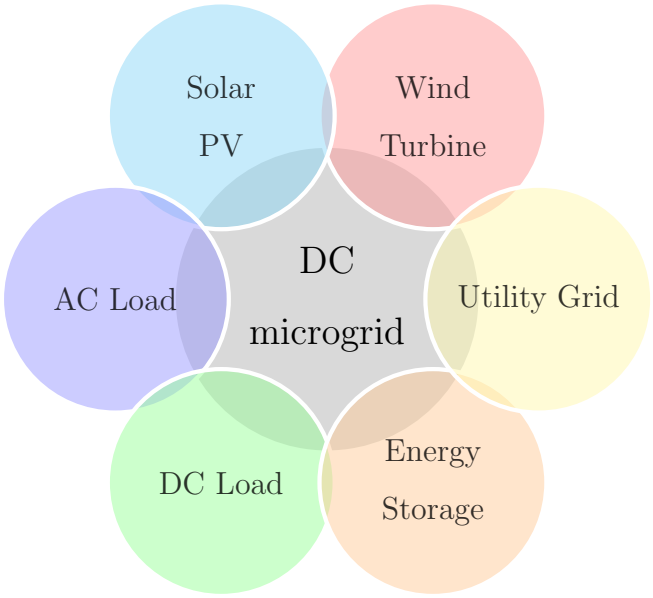

Figure 1.2: Schematic of DC microgrid.

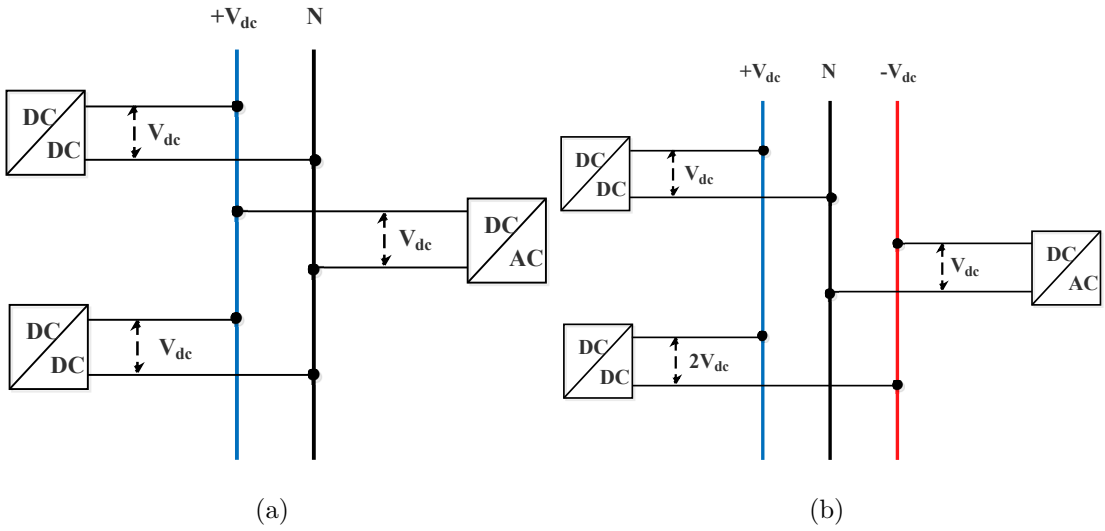

Figure 1.3: Schematic of a unipolar and bipolar DC system (a) unipolar (b) bipolar.

household gadgets, the demand for hybrid AC-DC microgrid is enhanced [21]. A hybrid microgrid is suitable for applications where high power quality is the highest priority, such as data centers [22]. Further, it also finds applications for power quality improvement and voltage profile improvement of the AC microgrid [21]. Increasing the number of electric vehicles on the road also leads to the enhanced demand for DC subgrids for providing the charging facility to electric vehicles [23]. On the other hand, the interconnection of AC and DC subgrids increases the overall operational complexity of the hybrid microgrid.

Besides several advantages of the DC microgrids over those of AC, the deployment

of DC microgrids presents significant technical challenges, particularly in the domain of system protection. Unlike AC systems, where well-established protection techniques exist, DC systems lack natural current zero-crossing points, making it more difficult to interrupt fault currents using conventional circuit breakers. The speed and magnitude of fault currents in DC networks are also much higher due to the instantaneous discharge of energy stored in capacitive components, such as the DC link capacitors. This rapid rise in current can damage equipment and reduce the stability and reliability of the entire microgrid.

Moreover, the increasing integration of distributed renewable energy sources such as solar PV panels and wind turbines further complicates protection schemes. These sources are often interfaced through bidirectional converters, enabling power to flow in both directions. As a result, faults may be fed from multiple points in the network, making it challenging to isolate and locate faults quickly. Complex network topologies, such as meshed or hybrid configurations, exacerbate these issues, as fault current paths are less predictable.

Challenges in DC microgrid protection that need immediate attention include fast and reliable fault detection in complex topologies with the presence of renewable energy sources, bidirectional power flow, high magnitude discharging current from DC link capacitance [24]. A DC microgrid's capacity to operate reliably requires resistance to shunt failures with a short recovery time, which is directly tied to the protection scheme's ability to identify, classify, and localize the fault accurately. Furthermore, the protection devices used to protect DC microgrids faster and more reliable is based on the communication infrastructure and global positioning system (GPS). These devices have the vulnerability to cyber-attack. Moreover, lack of regulatory frameworks and well-developed DC protection devices are also key challenges. The digitalization of DC microgrids in smart grid environment introduces cyber security risks. Protection against potential cyber attacks is crucial for maintaining system integrity [25].

The converter-dominated systems cannot endure overloading for several milliseconds beyond their rating. Control strategies in these systems limit the fault current to twice the rated current [14, 26]. Increased use of converter-based sources and loads can adversely affect the reliability of the protection systems, thereby increasing the risk of cascaded failure [27]. Switching action in the converters produces non-linearity in the V-I relation-

ship, which results in the inclusion of harmonic content to the system and thus causes maloperation of protecting devices. The limited contribution of the fault current from converter-based sources also makes the configuration of protection systems challenging. Considering the complex topology of hybrid microgrids, backup protection serves as a secondary layer of defense, complementing primary protection devices by detecting and isolating faults that primary protection might not operate effectively [28].

This thesis proposed improved protection algorithms for DC and hybrid AC-DC microgrids. A GCN-based protection algorithm is proposed that utilizes the network topology's explicit spatial information with measurement data for fault detection. A unit protection scheme is proposed for bipolar DC microgrids using the superimposed component of the symmetrical domain currents. Symmetrical component decomposition of the measured current at the two ends of the bipolar DC line is used for fault detection and identification of cyber attacks. Furthermore, considering a synchronized cyber attack at both ends of the protected line in the worst-case scenario, a blockchain-enabled protection scheme is proposed to ensure the secure communication of measurements between the two ends of a protected line segment for enhanced security of the protection system against cyber intrusion. A time-domain technique is proposed to isolate the faulted DC and AC subgrids from the point of common coupling (PCC), in a hybrid AC-DC microgrid using AC and DC currents, respectively, in case the primary protection fails. The proposed method is validated in a real-time simulation using RTDS.

1.2 Literature Review

A DC microgrid is an efficient solution for low voltage levels that integrates renewable energy resources, loads, and storage devices through power electronic converters. Numereous literatures are available on the DC system operation and control, however fault detection is of critical importance to the safety of power electronics devices in DC and hybrid AC-DC microgrids. The upcoming subsections provide a comprehensive overview of the current state-of-the-art of the mentioned issues, concentrating on existing research and the corresponding issues and challenges linked with these problem.

1.2.1 Protection of DC microgrids

The DC microgrid protection schemes are categorized into conventional and modern approaches. The conventional approach includes non-unit and unit protection schemes . Non-unit protection schemes [29, 30, 31, 32, 33, 34, 35, 36, 37] make protection decisions using single-end data. Overcurrent protection [34, 38] is one of the often used non-unit protection scheme for DC microgrid . However, the small length of the DC cable and subsequent low resistance cause the coordination of the overcurrent relay to be challenging [39, 40]. Current derivative-based protection schemes were proposed in [32], which has improved sensitivity for low and high impedance faults. However, the values of current derivatives are influenced by line length, loads on the line, fault impedance, and a high sampling rate are required for measuring the current derivative.

Unit protection schemes [6, 14, 41, 42, 43, 44, 45, 46] require data from both ends of the line segment for the protection decision. Current differential and direction-based unit protection schemes are proposed in [24, 41, 44, 47]. High resistance fault that results in low magnitude fault current [48] and cyber attacks [49] are the issues in differential protection methods. In [42], a methodology is proposed based on a unit protection scheme with high sensitivity and faster response but having low sensitivity for high impedance faults. Communication assisted directional overcurrent-based protection scheme was proposed in recent literature [50].

Protection schemes based on impedance measurement at fault locations have attracted significantly in the past. [51] presents a protection method based on voltage measurement and current location fault location. The fault location estimation was performed by calculating the impedance from the measured data with the help of the iterative method and circuit analysis. However, the methodology has less accuracy for high-impedance faults. A communication-based differential protection method was proposed for the protection of a medium voltage DC microgrid in [52]. The proposed method uses a solid-state switch with communication infra for DC line protection. However, the methodology requires a communication infrastructure similar to the AC network and higher costs. A current derivative-based non-unit protection scheme is proposed in [49] for fault detection. Due to the small line length in microgrids, the selectivity is an issue for high resistance faults.

Apart from these, other techniques are also available in the literature for the pro-

tection of DC microgrids. These methods include the traveling wave-based method [53, 54, 55], differential current-based fault localization [56, 57], which requires a fast and reliable communication system. Travelling wave-based technique requires high-performance data acquisition and the microgrid with short line length affects the accuracy. The local measurement-based scheme has less accuracy for high resistance fault [58].

Although unit protection schemes provide better selectivity compared to non-unit protections, these are susceptible to data loss and cyber attacks, such as false data injection (FDI) and time synchronization attacks (TSA). This is due to the vulnerability of attacks in the communication protocols used in the substation, i.e., IEC 61850 [59]. The FDI attackers can manipulate the real-time data by breaking into the local area networks (LANs) of the substation [25]. Further TSA can be introduced by spoofing the GPS signal or by targeting the IEEE 1588 precision timing protocol at a substation [60].

In [25], a passive oscillator circuit (POC) at each converter terminal is used for attack detection in line current differential relay. However, the limitations of POC, such as their sensitivity to frequency and tuning requirements, make the task challenging, especially in the presence of intermittent loading and renewable generations. A solution to the problem of time synchronization error in differential protection is proposed in [43]. However, the protection against FDI attacks was not considered here. A cyber resilient protection scheme for the medium voltage DC (MVDC) microgrid is proposed in [61], which uses the voltage across the current limiting reactor (CLR) to ensure the resiliency of differential protection. Although the method works well for low resistance faults, being voltage dependent, the selectivity of such a method decreases with the increase in fault resistance [62]. Including the CLR in series with the line creates trouble in the circuit breaker operation [14], and also increases the cost of the protection system as the method requires both voltage and current measurements.

Besides these traditional approaches, various signal processing-based methodologies were proposed in the literature for fault diagnosis in DC microgrids. [30] proposed a variational mode decomposition-based technique for a low voltage DC system with a renewable energy interface. However, fault section identification was not performed in this literature. Inductor-voltage observation is utilized for low-resistance fault detection in [14], and the ground current is used to discover high-resistance faults. Fault location is estimated with the use of iterative methods. Oscillation frequency-based novel protection

technique is proposed in [63]. The frequency and transient power of the first oscillation cycle during the fault event are used to determine the relay trip. Decision time is greatly affected by damping level, response characteristics of the renewable energy sources, and hence the fault resistance.

The rising era of artificial intelligence (AI) in electrical engineering has generated enormous interest in data-driven algorithms for detecting and classifying power system faults. These algorithms show more remarkable performance compared to classical methods in the field of fault diagnosis [64, 65]. A wavelet-based data mining approach is used for DC microgrid fault detection in [66]. The proposed method uses wavelet transform for feature extraction from the current signals received at the relay location. A decision tree algorithm is used for fault detection based on independent wavelet coefficients. Artificial Neural Network based fault diagnosis was proposed in [67]. Two different artificial neural networks were used for fault detection and fault localization. A convolutional neural network (CNN) based methodology was proposed in [68] for discrimination between inverter and PV fault in an islanded microgrid. The time domain signal is converted to grayscale images which are used as input to the CNN. In [69] support vector machine (SVMs) based fault localization is proposed by using post fault data in DC microgrid clusters. Single-end current measurement data is used to locate the DC line segment fault.

However, AI-based algorithms discussed above are mainly data-driven approaches and do not consider the system topology as far as DC microgrid fault diagnosis is concerned. A group of studies [70], [71] find a considerable influence of system topology in the power system performance. So, the system topology must be incorporated along with measurement data to make a more accurate fault diagnosis in the DC microgrid. The power system topology itself can be treated as a graph, and edge information in the graph can also be incorporated based on network structure. Based on the topological information of the DC microgrid and the availability of large amounts of measurement data, GCN can be adequately implemented for the fault diagnosis problem. In recent days graph neural network (GNN) has gained the massive interest of researchers for power system problems such as power flow calculation,time-series prediction, fault detection, etc. [72].

The emergence of communication technology is ushering in a new era of industrial innovation and fostering the high-quality advancement of the modern economy. Despite

these advancements, effectively identifying and addressing electrical faults in remote power grids remains difficult due to limited communication infrastructure, high labor expenses, and complex terrain. To address this issue, there is the requirement of enhanced grid fault inspection system by integrating secure and efficient signal transmission strategies.

Distributed DC microgrids are inherently vulnerable to communication limitations and cyber threats, yet limited research has focused on tackling both of these challenges concurrently. In fact, the integration of communication networks inevitably brings about communication limitations and creates potential entry points for malicious cyber attacks [73, 74]. For these reasons, sustained attention and effective solutions are critically needed from the protection perspective to address communication challenges such as time delays and packet loss [75] as well as malicious attacks [76, 77] faced by DC microgrids functioning in non-ideal communication environments.

On the other hand, DC microgrids are increasingly vulnerable to cyberattacks executed through various intrusion methods, such as denial-of-service (DoS) attacks [78, 79], stealth attacks [77], FDI attacks [80, 81] hijacking, replay attacks, and man-in-the-middle attacks. Among these, FDI attacks are particularly concerning due to their sophistication; they are created to inject malicious data into compromised measurements, thereby disrupting microgrid operations without detection [82, 83]. The defense strategy against cyber threats in DC microgrids is typically categorized into four key stages: prevention, monitoring, detection, and mitigation [84]. Substantial progress has been made across these domains, including information-security-driven prevention techniques [85, 86], control-theory-based detection and mitigation strategies [87], and learning-based resilient methods [88, 89].

Recently, to strengthen the security of power system infrastructure, emerging blockchain technology [90] has been adopted to ensure built-in privacy, data integrity, authenticity, and confidentiality in the exchange of control signals and information. A blockchain-based scheme is proposed in [91] for securing the electricity consumption data in smart meters. In [92], a bit-coin based mechanism is proposed for protection of smart meter data. The method utilizes a one-tier architecture for all meters and presents a discussion of successful attack possibilities through different scenarios. A blockchain-based architecture is proposed in [93] to enhance the data transmission security in smart grids.

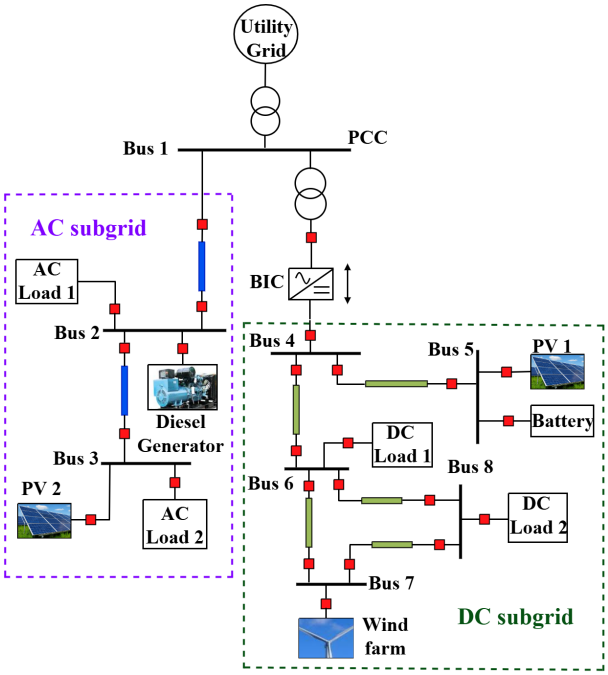

Figure 1.4: Schematic of a hybrid AC-DC microgrid.

1.2.2 Protection of Hybrid AC-DC microgrids

A hybrid microgrid (Fig 1.4) is suitable for applications where high power quality is the highest priority, such as data centers [22]. Further, it also finds applications for power quality improvement and voltage profile improvement of the AC microgrid [21]. Increasing the number of electric vehicles on the road also leads to the enhanced demand for DC subgrids for providing the charging facility to electric vehicles [23]. On the other hand, the interconnection of AC and DC subgrids increases the overall operational complexity of the hybrid microgrid.

The protection schemes for AC distribution systems available in the literature are broadly characterized as differential protection [94], overcurrent protection [95], distance protection [96], and other types of relay characteristics. Similarly, for DC microgrids the protection schemes include unit and non-unit protections [14, 43, 61, 62, 97, 98]. Protection schemes designed solely for AC or DC system may not adequately address all potential fault scenarios in hybrid microgrids. Besides this, the hybrid microgrid protection is in its early stages. In [99], a unified impedance-based protection scheme is proposed for hybrid microgrids that use the frequency analysis of the fault signals to identify the faults. This scheme requires an additional LC circuit in series with the existing relay, which increases the cost. In [100], two different protection schemes, over current

protection (for the AC side) and current derivative-based protection (for the DC side), are proposed and coordinated to make complete protection of the hybrid microgrid. However, in the current derivative-based scheme, selectivity is an issue for high resistance faults due to the small line length in microgrids. A protection scheme for a hybrid microgrid is proposed in [101] using the long short-term memory (LSTM) based classification approach. This method requires large amount of data and retaining of the model with change in the system configuration, which frequently occurs in the microgrids [102].

Increased use of converter-based sources and loads can adversely affect the reliability of the protection systems, thereby increasing the risk of cascaded failure [27]. Limited fault current contribution from converter-based sources also makes the settings of protection systems challenging. Considering the complex topology of the hybrid microgrids, backup protection serves as a secondary layer of defense, complementing primary protection devices by detecting and isolating faults that primary protection might fail to operate effectively [28]. The backup protection methods for DC microgrids available in the literature include [103, 104, 105]. A local measurement-based scheme is provided in [103] that uses derivative and integral characteristics of the current signal to provide backup protection for DC microgrid. In [104], running autoregressive smoothing average of the local voltage and current signals is used to provide backup for centralized primary protection scheme in a DC microgrid. Quickset change detection based scheme is provided in [105], that uses both current and voltage signals to provide backup protection. Similarly, the literatures [27, 28] provides backup protection methods for AC microgrids. The amplitude of positive sequence voltage is used in [27] to provide adaptive backup protection. A superimposed circuit technique is proposed in [28] to derive a linear system of equation for providing wide area backup protection. However, hybrid AC-DC microgrids have different characteristics during fault [99]. The available backup protection methods for DC and AC microgrid may not adequately address all the fault cases in hybrid microgrids.
Time-domain protection methods offer several advantages over other traditional protection techniques, making them increasingly attractive in modern power systems. Time-domain methods exhibit superior sensitivity to transient and high-frequency faults, allowing for improved discrimination between internal and external faults. Their adaptability to diverse system configurations and fault conditions further enhances their effectiveness in complex grid environments. Time-domain protection techniques are well-suited for

digital implementation, enabling seamless integration with advanced communication and control systems [106].

1.3 Motivation and Objectives

An efficiently designed, adaptable, informative, and physically robust energy system is crucial in low-voltage distribution networks to meet future energy needs [107]. DC microgrids present a promising solution, especially with the increasing use of DC-generating renewable energy sources (RESs) and modern electronic loads that operate on DC. For the DC microgrid to function reliably and stably, a protection scheme that is sensitive, selective, and secure is vital. In such systems, power electronic converters employing current control strategies help limit fault currents. However, traditional current-based protection methods, such as overcurrent, differential current, or impedance-based schemes struggle to accurately detect faults. The integration of distributed generation, power electronics for current and voltage regulation, and bidirectional power flow further complicates protection in today's DC distribution systems. A complete shutdown of the DC microgrid can cause inefficiencies, unnecessary outages, and power imbalances. Therefore, protecting the DC microgrid without resorting to full system shutdown is a significant challenge. The focus should be on isolating only the faulted section while maintaining power supply to unaffected areas, highlighting the need for the development of more advanced protection methods for DC microgrids.

In the evolving landscape of modern power systems, hybrid AC-DC microgrids have emerged as a transformative solution, offering enhanced efficiency, flexibility, and resilience. However, the complexity of these systems demands robust protection strategies to ensure uninterrupted power supply and system stability. While primary protection serves as the first line of defense, backup protection plays a crucial motivational role in reinforcing system reliability. It acts as a safeguard when primary systems fail or are compromised, ensuring that faults are swiftly isolated and service continuity is preserved. In hybrid AC-DC networks, where diverse power sources, bidirectional flows, and varying voltage levels coexist, the presence of a well-designed backup protection scheme is not just a redundancy, it's a necessity. Embracing advanced backup protection strategies reflects a proactive commitment to resilient, future-ready energy systems capable of withstanding

challenges and maintaining seamless operation under all conditions.

The main objective of the thesis are:

(i) Incorporating spatial information of the network topology to develop protection algorithm for DC microgrid.

(ii) To develop a cyber-resilient protection scheme for bipolar DC microgrid.

(iii) Enhancing the security of communication-assisted protection method for DC microgrid considering worst-case cyber attack scenario.

(iv) To develop a backup protection algorithm for hybrid AC-DC microgrid using information at the PCC.

1.4 Brief Overview of the Work Done

The work carried out in this research focuses on the protection of DC and hybrid AC-DC microgrids. Different algorithms are developed using voltage and/or current data for network protection tested using PSCAD/EMTDS, RTDS. The proposed methods are validated using RTDS and found to be accurate. The novelty of each algorithm developed in this thesis work is highlighted below.

1.4.1 GCN based fault detection in DC microgrids

The advantages of using DC networks in low-voltage systems support the development of smart grids and encourage greater integration of DG. Accurate detection of the faulted section within a distribution network by an automated system helps minimize power outage duration and enhances the reliability metrics of the network. When a fault occurs in a DC distribution system, information collected by the outage management system (OMS) is used to locate the faulted area. However, the presence of active DG units causes power to flow in both directions, making fault location more complex. Considering the electrical power network as an inherent graph, a method is proposed for the protection of DC microgrids. The proposed method utilizes spatial information from the test system to formulate the fault identification problem as node classification. The experimental results show that the proposed method distinguishes different types of disturbances, including

faults, with high precision. The proposed method is also tested with the existence of bad data and noise in fault data samples and shows better performance.

1.4.2 Cyber resilient protection of bipolar DC microgrids

The vulnerability of communication-assisted protection scheme towards cyber attack may affect the reliability of the protection system. A cyber resilient protection scheme is proposed that addresses internal fault detection and classification of all possible fault types and sensitivity against cyber attacks in bipolar DC microgrids. The proposed method requires current from both ends of the pole segment for (i) discriminating internal and external faults (ii) fault-type classification (iii) distinguishing cyber attacks from faults. The proposed protection method requires only a current sensor at both ends and one IED in each section. Therefore, it provides an economical, and computationally efficient (only change in current) solution for fault detection, fault type classification, and cyber attack distinction in a bipolar DC microgrids. The main strength of the proposed method is its inherent resiliency to single-end cyber attacks in contrast to conventional differential protection. Further, both ends attack and multiple sensors attack at a single end can be correctly identified using the proposed scheme.

1.4.3 Blockchain Enabled protection of bipolar DC microgrids

A novel protection scheme for bipolar DC microgrids, utilizing blockchain technology to enhance security and reliability. An Ethereum-based blockchain network is simulated to ensure the secure transmission of current measurements at the two terminals of the protected DC line. The DC microgrid is simulated in the real-time digital simulator (RTDS), and the measured currents at the remote end of the protected line segment are received through socket protocol (GTNET SKT) using the Python script. The blockchain's decentralized and immutable nature eliminates single points of failure and provides robust protection against tampering.

1.4.4 Backup protection for hybrid AC-DC microgrids

A time-domain backup protection algorithm is developed for a hybrid AC-DC microgrid to detect the fault and isolate the faulty subgrid from the PCC when the primary protection

fails. The proposed scheme requires only currents at the AC and DC terminals of the bidirectional interlink converter (BIC) for protection decision. One cycle moving average of the three-phase currents of the AC subgrid at the BIC terminal detects the ground faults in DC subgrids. The time span between two consecutive zero crossings of the phase currents and pre-fault DC currents identifies the pole-to-pole fault. The superimposed component of mode-1 current at the DC terminal of the BIC is used to detect faults in the AC subgrid. The performance of the proposed method is validated with hardware-in-loop (HIL) simulation in real-time for AC and DC subgrid faults.

1.5 Organisation of the Thesis

There are five chapters in the thesis. In the first introductory chapter, lietrature review on protection of DC and hybrid AC-DC microgrid is presented. Available scope of research including importance and advantages of DC and hybrid AC-DC microgrid are also highlighted. The objective of thesis and brief overview of work done are also provided. The sequence and summary of other chapters are given below:

- **Chapter 2** presents a novel fault detection and identification approach for low voltage DC microgrid having meshed configuration. The proposed methodology is based on Graph Convolutional Network (GCN), which utilizes the network topology's explicit spatial information and measurement data to identify a fault. The method has a more substantial feature extraction ability even in the presence of noise and bad data.

- **Chapter 3** presents a cybere resilient protection scheme for bipolar DC microgrid. The proposed protection method requires only a current sensor at both ends and one intelligent electronic device (IED) in each section. Therefore, it provides an economical, and computationally efficient (only change in current) solution for fault detection, fault type classification, and cyber attack distinction in a bipolar DC microgrids.

- **Chapter 4** presents a real-time simulation of a blockchain-based unit protection scheme. An Ethereum-based blockchain network ensures the secure transmission of current measurements at the two terminals of the protected DC line. The

blockchain's decentralized and immutable nature provides robust protection against cyber attacks. Extensive simulations validate the proposed scheme and demonstrate its effectiveness in the security of communication-assisted protection schemes.

- **Chapter 5** presents a backup protection scheme for hybrid AC-DC microgrids. A time-domain technique is proposed to isolate the faulted DC and AC subgrids from the PCC using AC and DC currents, respectively, in case the primary protection fails. The method requires only current measurement at the PCC to detect fault in either side of the hybrid microgrid.

- **Chapter 6** The last chapter in the thesis provides the conclusions of the work and offers few areas for future research.