Chapter 6

Conclusions and Future Scope of Study

The adoption of DC-based renewable energy sources (RESs) and DC-compatible loads is driving the development of DC microgrids in low-voltage distribution systems. As the presence of native DC sources, such as PV systems continues to grow, along with the increasing use of DC loads like electric vehicles, data centers, and modern household devices, the need for hybrid AC-DC microgrids is also becoming more prominent. In such systems, power electronic converters employing current control strategies restrict fault current levels, making it challenging for traditional current magnitude-based protection schemes to detect faults effectively. This thesis addresses these protection challenges by exploring and proposing novel algorithms for fault detection and location in DC and hybrid AC-DC microgrids. This chapter presents a summary of the key contributions made in this research and outlines potential directions for future work.

6.1 Contributions

This thesis presents a set of improved protection algorithms for enhancing the reliability and security of DC and hybrid AC-DC microgrids. One of the key contributions is a Graph Convolutional Network (GCN)-based algorithm that utilizes both the spatial structure of the network topology and real-time measurement data for accurate fault detection. By modeling the power network as a graph, the fault detection task is framed as a node classification problem, allowing the system to effectively leverage topological and

measurement-based information to identify faults with high accuracy.

Another protection method is proposed for bipolar DC microgrids, which requires only current measurements from both ends of a protected line for protection decision. Using symmetrical component decomposition, this method enables the detection of faults and identification of potential cyber attacks. It is inherently more resilient to single-ended attacks and has proven effective in detecting high-resistance faults. The performance and robustness of the method have been validated through real-time simulations using RTDS, confirming its ability to withstand single-ended cyber attacks.

To further improve the cybersecurity of communication-assisted protection systems, a blockchain-based protection scheme is developed and tested in a real-time simulation environment. The decentralized and tamper-proof nature of blockchain technology provides strong defense mechanisms against cyber threats. Simulation results confirm the method's effectiveness in ensuring secure and reliable communication-based protection for DC microgrids, enhancing resiliency against cyber intrusions.

For hybrid AC-DC microgrids, which combine the benefits of both AC and DC systems but face protection challenges due to reduced fault current levels and the widespread use of power electronic interfaces, a time-domain backup protection scheme is proposed. This method is specifically designed to isolate the faulty subgrid from the point of common coupling (PCC) using only current sensors at both ends of the bidirectional interlinking converter (BIC). Its effectiveness is demonstrated through real-time hardware validation.

6.2 Conclusions

The proposed algorithms contribute significantly to advancing protection strategies for DC and hybrid AC-DC microgrids. The GCN-based approach introduces a data-driven framework that combines spatial and real-time information for intelligent fault detection. The current-based protection method for bipolar DC microgrids offers a simple and robust alternative for detecting faults and mitigating cyber threats. The integration of blockchain technology further enhances the security of communication-assisted protection systems, ensuring tamper-proof and reliable operation. In hybrid AC-DC microgrids, the time-domain backup protection method addresses the limitations of conventional techniques, offering an effective solution using minimal sensing requirements.

All proposed methods have been validated through simulations or hardware testing, confirming their practicality and reliability. Collectively, these algorithms provide a strong foundation for the next generation of intelligent, secure, and resilient microgrid protection systems. They can be seamlessly integrated into the processing units of IEDs, enabling automated and dependable protection decision-making in modern power networks. The proposed algorithms are useful for protection decision in a DC and hybrid AC-DC microgrids. For reliable operation and enhanced performance, these algorithms can be incorporated in the processing unit of the IEDs.

6.3 Future scope

The scope for future advancements in this research lies in building upon the findings of this thesis, with several promising directions outlined below-

(i) The proposed GCN based method effectively uses spatiotemporal data for fault detection but is limited by its dependency on a fixed adjacency matrix tied to the grid topology. Any change in topology requires retraining with a new matrix. Future work may address this limitation by exploring dynamic graph structures to handle frequent system changes.

(ii) The blockchain based algorithm can be further enhanced in terms of latency, data handling and computational complexity. As the number of devices and events increases, the blockchain grows in size, potentially leading to storage and synchronization issues.