Preface

Over the last decade, the growing trend toward renewable energy has led to a new paradigm in electrical power distribution. DC microgrid is a solution in low voltage levels that integrates renewable energy resources, loads, and storage devices through power electronic converters. Compared to AC, DC microgrids have advantages, including reduced conversion stages for modern DC electronic loads, increased power transfer capacity, and higher efficiency. Despite the obvious benefits of DC microgrid, creating a suitable protection system for micro-DC networks is still an area of interest. The operational complexity and fault current characteristics in a DC microgrid make the traditional protection paradigm fall short in ensuring the system's reliability and security. Furthermore, the protection devices used to protect DC microgrids faster and more reliably are based on the communication infrastructure and GPS, and therefore vulnerable to cyberattacks.

In this thesis, protection algorithms are developed, using local and both end data for DC and hybrid AC-DC microgrids. A graph convolutional network-based fault diagnosis algorithm for a low-voltage DC microgrid is proposed. The proposed algorithm utilizes the network topology's explicit spatial information and measurement data to identify a fault. Considering the vulnerability of the communication-assisted protection scheme against cyber attacks, another method is proposed using current measurements at both ends of the protected line for bipolar DC microgrids. 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 attack. The proposed method is validated on a real-time simulation environment using real-time digital simulator (RTDS), and found to be inherently resilient against single-ended cyber attacks.

Further, considering a synchronised 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. 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 proposed method is validated in real-time simulation using RTDS.

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, and DC electric loads, like electric vehicles, data centers, and household gadgets, the demand for hybrid AC-DC microgrid is enhanced. A hybrid microgrid is suitable for applications where high power quality is the highest priority, such as data centers. Further, it also finds applications for power quality improvement and voltage profile improvement of the AC microgrid. 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. A time-domain technique is proposed to isolate the faulted DC and AC subgrids from the point of common coupling using AC and DC currents, respectively, in case the primary protection fails. The proposed protection scheme is validated on a hybrid AC-DC microgrid, simulated using RTDS and a TMS320f28379d-based digital signal processor in a hardware-in-loop scenario for different faults on either side of the microgrid.

Keywords: *Blockchain, DC microgrids, Graph Convolutional Network, Hardware-in-loop Validation, Hybrid AC-DC microgrids, Real-time Simulation, Symmetrical Component Decomposition, Time-domain Backup Protection.*