Network and System Management for the Security Monitoring of Microgrids using IEC 62351-7

Mark Karanfil

A Thesis

in

The Department

of

Concordia Institute for Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Applied Science (Information Systems Security) at

Concordia University

Montréal, Québec, Canada

April 2019

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Mark Karanfil**

Entitled: **Network and System Management for the Security Monitoring of Microgrids using IEC 62351-7**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Information Systems Security)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Walter Lucia

_____ External Examiner
Dr. Otmane Ait Mohamed

_____ Examiner
Dr. Jun Yan

_____ Supervisor
Dr. Mourad Debbabi

_____ Co-supervisor
Dr. Aiman Hanna

_____ Co-supervisor
Dr. Marthe Kassouf

Approved by _____
Abdessamad Ben Hamza, Director
Concordia Institute for Information Systems Engineering (CIISE)

Friday, May 10th, 2019 _____
Amir Asif, Dean
Gina Cody School of Engineering and Computer Science

Abstract

Network and System Management for the Security Monitoring of Microgrids using IEC 62351-7

Mark Karanfil

Interest in adding renewable energy sources to the power grid has risen substantially in recent years. As a response to this growing interest, the deployment of microgrids capable of integrating renewable energy has become more widespread. Microgrids are independent power systems that deliver power from different kinds of Distributed Energy Resources (DERs) to local energy consumers more efficiently than the conventional power grid. The microgrid leverages advanced information and communication technologies for vital protection, monitoring, and control operations as well as for energy management. With the use of information technology comes the need to protect the microgrid information layer from cyberattacks that can impact critical microgrid power operations. In this research, a security monitoring system to detect cyberattacks against the microgrid, in near-real time, is designed and implemented. To achieve this, the system applies Network and System Management (NSM) for microgrid security monitoring, as specified by the IEC 62351-7 security standard for power systems. The specific contributions of this research are (i) an investigation on the suitability of NSM for microgrid security monitoring; (ii) the design and implementation of an NSM platform; (iii) the design and implementation of a security analytics framework for NSM based on deep learning models; (iv) the elaboration of a comprehensive microgrid simulation model deployed on a Hardware in the Loop (HIL) co-simulation framework; and (v) an experimental evaluation on the effectiveness and scalability of the NSM security monitoring platform for detection against microgrid attack scenarios, with a methodology being used to systematically generate the scenarios. The experimental results validate the usefulness of NSM in detecting attacks against the microgrid.

Acknowledgments

I express my gratitude to all those that have contributed towards my thesis and to those who have supported my progression towards its completion.

I am grateful to my supervisors, Dr. Mourad Debbabi, Dr. Aiman Hanna, and Dr. Marthe Kassouf, for the time and commitment they have invested in my research. Their vast experience and insight within the domain of my research has truly expanded my understanding and appreciation of the field, both from a theoretical and practical perspective.

I extend my gratitude to Dr. Jun Yan, Dr. Walter Lucia, and Dr. Otmane Ait Mohamed for being part of the examination committee for my thesis.

I would like to acknowledge the fruitful collaboration with Ms. Chantale Robillard, Mr. Abdullah Albarakati, Mr. Dhiaa Rebbah, Mr. Abolfazl Rahiminejad, Dr. Rachid Hadjidj, and Dr. Mohsen Ghafouri throughout this research. In addition, I would like to acknowledge the rest of my colleagues for their support and encouragement during my studies, as well as the many professors who have offered their own insights during the regular meetings concerning the research progress on smart grid security. In particular, I am thankful to Dr. Bassam Moussa for his comments on an earlier version of this thesis.

Finally, I am deeply grateful to my family for their immense support and encouragement throughout my academic studies. My parents and siblings in particular have shown me vast amounts of patience as I progressed through my studies, always ready to welcome me even after long periods of study. For this I am truly thankful, and I love you all dearly.

Contents

List of Figures

List of Tables

List of Acronyms

AC	Alternating Current
AMI	Advanced Metering Infrastructure
APCI	Application Protocol Control Information
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARP	Address Resolution Protocol
ASDU	Application Service Data Unit
CHP	Combined Heat and Power
COT	Cause of Transmission
DC	Direct Current
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DG	Distributed Generation
DNN	Deep Neural Network
DNP3	Distributed Network Protocol
DoS	Denial of Service
DPI	Deep Packet Inspection
DRTS	Digital Real-time Simulator

EPS	Electric Power System
ESS	Energy Storage System
GOOSE	Generic Object Oriented Substation Event
GPS	Global Positioning System
HFAC	High Frequency Alternating Current
HIL	Hardware in the Loop
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEC 104	IEC 60870-5-104
IED	Intelligent Electronic Device
IOA	Information Object Address
IP	Internet Protocol
ISO	International Organization of Standardization
IT	Information Technology
LSTM	Long Short-Term Memory
MAC	Message Authentication Code
MGCC	Microgrid Central Controller
MIB	Management Information Base
MitM	Man in the Middle
MMS	Manufacturing Message Specification

NME	Network Management Entity
NSM	Network and System Management
NTP	Network Time Protocol
OPNET	Optimized Network Engineering Tool
OSI	Open System Interconnection
P&C	Protection and Control
PCC	Point of Common Coupling
PDU	Protocol Data Unit
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PTP	Precision Time Protocol
PV	Photovoltaic
RBAC	Role-Based Access Control
RFC	Request for Comments
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Network
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SNMPTT	SNMP Trap Translator
SV	Sampled Value
SVM	Single Vector Machine

TAL	Time Allowed to Live
TCP	Transmission Control Procotol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VM	Virtual Machine
WT	Wind Turbine

Chapter 1

Introduction

1.1 Motivations

Microgrids are independent power infrastructures capable of providing electricity to a small nearby community [1]. Compared to the main utility grid, microgrids are able to distribute energy more efficiently by being situated closer to energy consumers and by integrating multiple renewable energy sources for energy management [1], [2]. Microgrids can operate in grid-connected mode, where they are connected to the main grid and have power from the main grid flow through them. Alternatively, microgrids can operate in islanded mode, where they are disconnected from the main grid and run as stand-alone autonomous systems. Running in islanded mode is beneficial when faults significantly degrade the power quality within the main grid [3]. In such a case, microgrids maintain adequate power delivery through the use of renewable energy sources and energy storage units [1].

The microgrid is increasingly seeing deployment as part of the larger smart grid system. In June 2016, the power capacity of microgrids worldwide exceeded 1,600 MW, and its capacity is projected to reach 7,500 MW by 2024 [4]. The smart grid is a modernization of the traditional power system infrastructure. It leverages information and communication technologies as well as automation tools to support the generation, transmission, and distribution of power across the grid. A key element of both the microgrid and the larger smart grid is the use of digital communications enabled by the integration of information technology. The use of digital communications enables the smart grid

to exert greater control over power distribution. For example, digital communications are a vital component of the Advanced Metering Infrastructure (AMI), which measures energy consumption at consumer sites and transmits the measured consumption to the Supervisory Control and Data Acquisition (SCADA). The use of AMI enables demand response, giving some control to consumers over their own energy consumption and improving the efficiency of energy distribution [1].

The use of digital communications in the microgrid provides many benefits and is vital for several microgrid functions. They enable microgrid to perform measurement collection, protection, control, demand response, and load shedding [2]. In particular, the digital communication infrastructure interconnecting the microgrid control centre with the dispersed consumer loads and energy sources greatly improves the capability of the microgrid to maintain stability in the face of sudden power flow changes in a load or energy source [1]. In addition, digital communications provide a means to achieve the coordination required to move the microgrid from grid-connected to islanded mode and vice-versa.

The reliance on digital communication exposes the microgrid to cyberattacks that can compromise the availability, integrity, and confidentiality security properties of the microgrid. Power and energy management concerns for microgrids has motivated the deployment of centralized microgrid controllers, which introduce more communication links that can act as potential entry points for attacks [5]. Among the largest threats to the microgrid communication network are cyberterrorists and state-sponsored attackers. In addition, the microgrid can face inadvertent threats that can impact physical operations and digital communication. The sophisticated cyberattack that caused the major power outage in Ukraine in December 2015, resulting in approximately 225,000 people losing power [6], highlights the danger that cyberattacks pose on the availability of power in the utility grid at large. Being part of the critical infrastructure, the microgrid must be resilient in the face of both inadvertent and deliberate threats.

1.2 Problem Statement

The purpose of this research is to design, implement, and evaluate a new platform for microgrid security monitoring that applies Network and System Management (NSM). In particular, the

suitability and effectiveness of the NSM data objects defined in the IEC 62351-7:2017 standard for cyberattack detection is investigated.

1.3 Objectives

The objectives of this research are:

- To assess the benefits of using the NSM specifications in IEC 62351-7:2017 as a solution for microgrid security monitoring, with a focus on assessing the potential of NSM data objects to enhance threat detection in the microgrid.
- Design and implement a monitoring platform applying IEC 62351-7:2017 NSM to enhance the visibility and security of microgrid operations, with the design addressing concerns of integration into real microgrids.
- Elaborate detection capabilities that act on the data objects collected with NSM.
- Evaluate the scalability and effectiveness of the NSM platform when used for attack detection, with the evaluation being done on a representative microgrid model.

1.4 Contributions

The contributions of this research are as follows:

(1) An investigation is made on the suitability and effectiveness of NSM for microgrid security monitoring. Specifically, the NSM specifications given in the IEC 62351-7:2017 standard are studied.

(2) An NSM platform providing microgrid security monitoring is designed and implemented. The design makes use of the NSM data objects defined in IEC 62351-7:2017.

(3) A microgrid anomaly detection framework used to analyze the collected NSM data for threat detection is designed and implemented. The module combines rule-based detection with

machine learning models for anomaly detection, which are applied on IEC 62351-7 NSM data objects.

(4) A microgrid simulation model is elaborated, with the model being deployed on a HIL smart grid co-simulation testbed. The model includes separate systems for the power, control, protection, and communication functions of the microgrid.

(5) The effectiveness and scalability of the NSM platform when detecting attacks are evaluated experimentally by subjecting the microgrid model to attack scenarios. A methodology for systematically generating attack scenarios is elaborated and applied to build the set of attack scenarios used for the evaluation.

1.5 Thesis Structure

Chapter 2 of this thesis provides background information on the microgrid, its network communication protocols, and NSM. Chapter 3 presents related work on microgrids, cybersecurity threats that target them, and cybersecurity solutions against such threats. Chapter 4 describes the core design of the proposed NSM platform and details on IEC 60870-5-104, the primary digital communication protocol used in the studied microgrid. It also describes the methodology used for generating attack scenarios to launch against the microgrid. Chapter 5 details the microgrid simulation testbed architecture and its communications. Moreover, it details the attack scenarios implemented and launched against the simulated microgrid. The experimental results on the effectiveness of the proposed NSM platform at detecting the attacks are also presented. To conclude the thesis, Chapter 6 discusses the implications and insights gained in this research, along with ideas on which to base future research in this area.

Chapter 2

Background

This chapter gives an overview of the concepts that are pertinent to this research. First, the concepts related to microgrid architecture are discussed. Second, the cyberattack threats that can impact the microgrid are described. Finally, the specifications for Network and System Management (NSM) given by the IEC 62351-7:2017 standard are presented.

2.1 Microgrid Architecture

This section describes the concepts related to the architecture of the microgrid, and is broken down into three parts. The first part discusses the role that the microgrid plays as part of the smart grid. The second part describes the physical architecture of the Industrial Control System (ICS) used in the microgrid. The third part describes the architecture of the digital communications within the microgrid, the devices that support its management, and its communication protocols used for monitoring and control. The physical system and the communication system found in the microgrid cooperate together to form a cyber-physical system.

2.1.1 Role in Smart Grid

Microgrids are designed to connect a power supply network to loads within nearby small communities [1].The microgrid can supply loads using the power delivered by the main utility grid or by local DERs. Microgrid DERs are typically located close to consumer loads. They help improve the

reliability and efficiency of power delivery [7]. Microgrids are expected to be capable of running while in grid-connected mode, where power from the main utility grid is distributed to local loads, and in islanded mode, where the microgrid is disconnected from the main utility grid and distributes power to its loads using its own local energy sources [1].

Microgrids offer a means of decentralized power distribution that can integrate DERs with distributed storage to better maintain energy balances [8]. Some examples of DERs used by microgrids include Wind Turbine (WT), Solar Photovoltaic (PV) panels, diesel generators, and Energy Storage Systems (ESSs) such as batteries and flywheels [9], [10]. The system arising from the interconnection of DERs will be similar to the conceptual model of the microgrid presented in Figure 2.1.

While connected to the main utility grid, the microgrid can store excess energy from the main grid into energy storage units or transfer its own excess energy into the main grid. The flow of excess energy between the microgrid and the main grid depends on the power balance between the loads and the energy generation. Microgrids also act as a backup energy distributor for the energy consumers it supplies after disconnecting from the main grid when the main grid experiences faults, blackouts, or maintenance [2], [11], [12]. By being able to provide power while there are faults in the main grid, microgrids add resiliency to the smart grid in terms of its capability to maintain the quality of power delivery.

2.1.2 Physical System Architecture

Microgrids are often connected to the main utility grid through one connection point, known as the Point of Common Coupling (PCC). It is at this connection point where the microgrid connects to or disconnects from the main grid to switch into grid-connected mode or islanded mode, respectively. When in islanded mode, the microgrid cannot rely on the main grid to absorb excess power generated from the microgrid, nor can the main grid supply power to address deficits in microgrid power generation. The islanded microgrid needs to balance the power it generates with the load demand [13].

At a high level, the physical system of the microgrid has a set of buses, lines, and transformers that connect consumer loads to the DERs and the main grid. The IEEE 1547 [14] standard gives rules and guidelines for the interconnection and integration of DER island systems with Electric

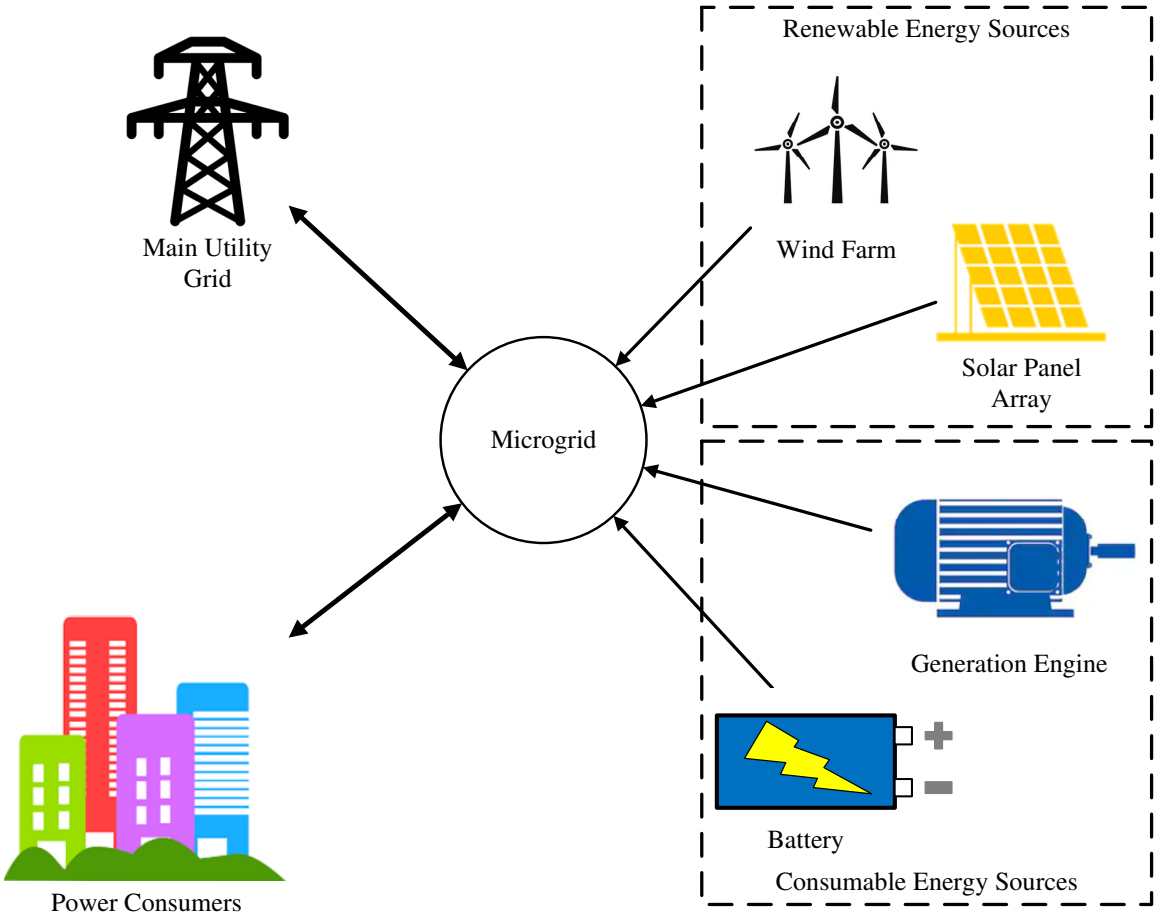

Figure 2.1: Microgrid conceptual view

Power Systems (EPSs) as well as specifications for the design, operation, maintenance, and testing of the system interconnecting DERs and EPSs.

Patrao *et al.* **[10]** classified microgrid architectures into six main groups encompassing both Alternating Current (AC) architectures and Direct Current (DC) architectures: AC-microgrid, DC-microgrid, hybrid AC-DC microgrid, AC-microgrid with DC-storage, DC-zonal microgrid, and solid-state transformer-based microgrid. All of these architectures have AC power flowing through the PCC that connects the main grid to the microgrid as part of their design, with the voltage level being reduced by a transformer before reaching the microgrid. The microgrid frequency should match the frequency used in the main grid **[8]**. The microgrid model studied in this research is an AC-microgrid, but the proposed microgrid security platform is mostly independent of the power system architecture being used.

Different sets of equipments are used in the smart grid for measurement and control purposes. Sensor equipment used to support microgrid operations includes voltage and current instrument transformers, Phasor Measurement Units (PMUs), and AMI [1]. The instrument transformers connect the power system components to voltage and current measurement equipment while reducing voltage and current to a level that can be safely measured [15]. The PMUs enhance the observability of grid stress by measuring the voltage, phase angle, and frequency of the power system, adding timestamps to each measurement so that phasor measurements from different sources can be synchronized [16]. The AMI is a system composed of digital hardware and software that allows information to be exchanged between customer sites and service providers [1]. Some of the control equipment found in microgrids includes tap changers in transformers, protection relays, and circuit breakers [1].

2.1.3 Communication System

Various points in the microgrid power network need protection from undesirable electrical flows. This protection is provided by having a measurement Intelligent Electronic Device (IED), a circuit breaker control IED, and a protection and control IED deployed at each protection point [17]. Measurement IEDs take voltage and current samples from the microgrid and report these sample measurements to the protection and control equipment [17]. Circuit breaker IEDs are responsible for controlling microgrid circuit breakers, which interrupt the current flowing through power lines and equipment such as electrical transformers [15]. Protection and control IEDs provide functionalities that maintains the safe operation of the microgrid, such as over-current protection, under-voltage protection, and differential protection [18]. There are also IEDs that are responsible for the control of DERs and energy storage devices [19].

Together, these IEDs monitor and control the state of the devices they manage while engaging in communication with microgrid controllers. Microgrid controllers are responsible for overall microgrid management as well as monitoring of the main utility grid and the flow of electricity between the main grid and the microgrid [2].

The distributed nature of microgrids makes it so that monitoring and control equipment is scattered across a wide area and require long distance communication technologies. There are various

technologies that digital devices in the microgrid can use to transmit messages. These include wired connection technologies like Ethernet cables, optic fiber, broadband over power line, and leased telephone lines [9]. Ethernet cables allow industrial Ethernet protocols, such as the IEC 61850 Generic Object Oriented Substation Event (GOOSE) and Sampled Value (SV) protocols, to be used for communication between IEDs and other components [19]. Microgrid devices can also communicate over wireless technology such as Wi-Fi, WiMAX, and ZigBee [1] [17]. Compared to wired physical communication links, wireless links tend to have lower message transfer reliability and higher susceptibility to signal interference but have lower installation costs and higher data transfer speeds [18]. Wireless communication is also appropriate for microgrids located in hazardous environments and microgrids that use a large number of remote measurement devices [18]. Wired and wireless communication technology can nevertheless be combined to help optimize the effectiveness and availability of the overall information system network.

2.1.4 Communication Layer Protocols

The microgrid makes use of software communication protocols to perform monitoring and control operations across devices through wired or wireless technology. Some of the more commonly used protocols for this purpose are Modbus, IEC 60870-5-104, the Distributed Network Protocol (DNP3), and the IEC 61850 GOOSE and SV protocols [18].

2.1.4.1 Modbus Protocol

Modbus is a legacy communication protocol used in power systems for process control and data exchange between clients and servers [2] [18]. In microgrids using Modbus, the Human Machine Interfaces (HMIs) act as Modbus servers while DERs, loads, and circuit breakers act as Modbus clients [18]. Modbus traffic can be transmitted across wired mediums such as serial links (RS-232 or RS-485) and industrial Ethernet as well as across wireless communication links such as WIMAX and ZigBee [18]. The specifications for use of Modbus across different media is provided openly by the Modbus Organization [20].

2.1.4.2 IEC 60870-5-104 Protocol

The IEC 60870-5-104 standard **[21]** is part of the IEC 60870-5 standard. The IEC 60870-5-104 standard describes a protocol designed for remote transmission of serial data between controlling stations and controlled stations, also known as masters and slaves respectively **[22]**. Slaves are also sometimes referred to as "outstations". IEC 60870-5-104 specifies how messages using the application layer specified in IEC 60870-5-101, a companion standard for IEC 60870-5 **[23]**, can be transmitted over a TCP/IP profile. It aims at standardizing the transmission of messages between geographically separated equipment that support control operations and are interconnected with permanent data links **[22]**, **[24]**.

2.1.4.3 DNP3 Protocol

DNP3 is a communication protocol used by SCADA systems in the utility grid **[18]**. DNP3 is based on IEC 60870-5 and its specification is given in IEEE 1815 **[25]**. DNP3 follows a master and slave model, with a master device that can send commands to slave devices or poll slave devices for monitored data that the slave sends within a solicited response. Slave devices can also send unsolicited messages to master devices that contain relevant data. Like Modbus, DNP3 traffic can be transmitted across serial links or Ethernet but unlike Modbus it supports the inclusion of timestamps to messages **[18]**.

2.1.4.4 IEC 61850 Standard Protocols

The IEC 61850 standard **[26]** provides a suite of protocols designed for use in power utility automation systems. It was developed in order to standardize the communication protocols and data objects used by automation systems in power utilities, with a focus on interoperability and interchangeability between IEDs **[26]**. The communication protocols defined in the IEC 61850 standard include the Manufacturing Message Specification (MMS) protocol specified in IEC 61850-8-1:2011 **[27]** as well as the Generic Object Oriented Substation Event (GOOSE) and Sampled Value (SV) protocols specified in IEC 61850-7-2:2010 **[28]** and IEC 61850-9-2:2011 **[29]**, respectively. The MMS protocol is designed for communications between IEDs and control devices over TCP/IP.

The GOOSE protocol follows a publisher-subscriber model for message transmissions between IEDs over Ethernet communication links. It can be used to publish trip commands to circuit breakers that will cause them to open or close, as well as for circuit breakers publishing their current state to protection and control (P&C) relays. The relays in turn send GOOSE messages to power network servers [30]. The SV protocol is also transmitted over Ethernet, and is used to send measured values of current and voltage in the power network to other IEDs such as relays. In addition to Ethernet communication, there are versions of GOOSE and SV that are routable and therefore can be transmitted over IP networks. These versions are defined in IEC 61850-90-5:2012 [31], and are suitable transmitting GOOSE and SV packets as well as IEEE C37.118-2005 [32] synchrophasor data collected by PMUs.

2.2 Cybersecurity Threats in Microgrids

The critical importance of the microgrid makes it an attractive target for attackers. The use of information systems in microgrid increases the surface area for entry points that attackers can use to compromise the microgrid. Rather than just being restricted to harming microgrid operations through physical access to microgrid assets, attackers can launch cyberattacks against the information system of the microgrid in order to cause damage. The intertwined nature of the physical and digital operations of the microgrid makes it possible for cyberattacks against the microgrid to impact physical operations. Negative impacts resulting from such cyberattacks include power interruption for local consumers, microgrid instability, and damage to equipment [33]. Attacks whose attack steps or impacts involve both the physical and digital operations of the microgrid can be labelled as "cyber-physical attacks" to reflect this expanded scope.

There are various reasons for attackers to compromise the microgrid. These reasons include, but are not limited to, the desire to perform vandalism, theft, or terrorism [34]. In addition, there is room for inadvertent failures and human error to appear in the microgrid information system network.

Veitch *et al.* [12], in a report published by Sandia Laboratories, describe various sources of

vulnerabilities in the microgrid information system network that can lead to failures due to non-deliberate events or when exploited by cyberattackers. These vulnerabilities spread across the communication network.

The possible threats to the communication network that Veitch *et al.* describe in the Sandia Laboratories report include the following [12]:

- **Denial of Service (DoS)**

  An adversary prevents or prohibits a component in the communication network from performing normal operations.

- **Eavesdropping**

  An adversary monitors and records the traffic passing through the network without making any changes to the content and the behaviour of the traffic. The adversary can perform traffic analysis to extract key information from the monitored data.

- **Man in the Middle (MitM)**

  An adversary intercepts messages between two legitimate parties while making the legitimate parties believe their communication is not compromised and that they are talking directly to each other. The adversary can then monitor, modify, insert, delay, and drop traffic being exchanged by the legitimate parties.

- **Masquerading**

  An adversary impersonates a trusted party, fooling users to interact with the adversary as if the adversary is a legitimate user.

- **Message modification**

  An adversary modifies the contents of messages being sent across the network.

- **Message replay**

  An adversary retransmits a message through the network that was previously recorded as having been transmitted through the network.

- **Unauthorized access**

  An adversary gains access to a resource in the network that they do not have permission to access.

Veitch *et al.* also elaborate on possible sources of security gaps within the microgrid ICS in the Sandia Laboratories report. These possible vulnerabilities include the following [12]:

- **Attacks on field devices**

  An adversary accesses field devices that are not write-protected.

- **Backdoor or malicious software installations**

  An operator, inadvertently or deliberately, installs malicious software on ICS equipment.

- **Database attacks**

  An adversary writes values to a database that may impact operations and data collection.

- **Devices lacking security features**

  An adversary accesses the network through a device that does not have adequate security protection mechanisms.

- **Improper configuration of actors**

  An adversary accesses the network by finding a user's poorly protected credentials or by finding default credentials that are in use.

- **Improper cybersecurity procedures or training**

  An adversary accesses the network through security gaps introduced by misconfiguration of security measures.

- **Inadequate network perimeter definitions**

  An adversary compromises a corporate/enterprise network and accesses an ICS information system that is not properly isolated from the compromised corporate/enterprise network.

- **Inadequate patching of software and firmware**

  An adversary compromises a device that has not been updated with the latest firmware and as a result the device has not received important security updates.

- **Improper coding techniques**

  An adversary compromises the ICS network due to security flaws that were introduced by programming errors.

- **Lack of security tools specific to ICS**

  An adversary accesses the network by taking advantage of security gaps in areas specific to the ICS that are not adequately protected.

- **Lack of redundancy for critical actors**

  The microgrid operation is negatively impacted due to faults at a single point of failure.

- **Unauthorized personnel have access to ICS actors**

  An adversary is given the opportunity to access the ICS network in an undesirable way due to proper security measures and policies not being in place.

- **Vulnerabilities in ICS protocols**

  An adversary exploits known vulnerabilities in ICS digital communication protocols that are not being addressed by security measures.

2.3 Network and System Management

The complexity and size of digital networks has made it challenging for human operators to observe and manage these digital networks manually [35]. Automated tools have become more and more necessary to provide adequate network monitoring.

2.3.1 Network Management Systems

A network management system is composed of tools that allow for network monitoring and control [35]. These tools can be integrated into a single operator interface that acts as the access

point to the network management system functions for operators. The goal of these tools is to provide human users with a powerful and user-friendly interface to perform needed network management tasks [35].

The responsibilities of an integrated network management system can be separated into several categories. The International Organization of Standardization (ISO) has categorized network management tasks into the following key areas [35]:

- **Fault management**

  Fault management involves the detection, isolation, and correction of abnormal operations.

- **Accounting management**

  Accounting management involves the identification of costs related to network components and actions.

- **Configuration management**

  Configuration management involves the monitoring and control of network components.

- **Performance management**

  Performance management involves the evaluation of network behaviour and the effectiveness of network communication activities.

- **Security management**

  Security management involves the protection of the network from security threats.

Network management systems are designed to consider the state of the network as a whole [35]. This is enabled by monitoring software placed across the entire network that report on the state of network resources at regular intervals. By having visibility on the status of resource nodes across the network, the network management system can view snapshots of the network state as a whole.

Stallings describes the architecture of a network management system. The described architecture has network management entities (NMEs) deployed across the network that communicate with a central network control centre [35]. The NMEs collect and store statistics and status information of

the network nodes they monitor. The NMEs transmit the collected statistics and status information to the network control centre. The information can be transmitted upon request, or spontaneously as a response to significant events being observed. A NME can also change their configuration upon request from the network control centre. The network control centre is comprised of a set of management applications that include interfaces for human operators to manage the network and the capability to issue commands to NMEs across the network [35].

Stallings also describes a network management system architecture as having NMEs that respond to a separate network manager system that is not necessary located within the network control centre, and these NMEs are referred to as "agents" [35].

2.3.2 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a digital communication protocol through which network management tasks are performed [36]. The SNMP architecture consists of SNMP managers deployed on network management stations and SNMP agents deployed on managed stations [35], [36]. The manager exchanges SNMP messages with the agents on the managed stations deployed across the network. SNMP is widely supported by equipment from major vendors [35].

The data within the SNMP messages is transmitted as a data object name associated with a monitored element in the network and a value that corresponds to the data object. The following are the key operations supported by SNMP [35]:

- `Get` request

  The SNMP manager sends an SNMP message to the SNMP agent requesting that the agent return the value of the data object specified in the message by the manager. The agent responds by sending SNMP message to the manager that contains the requested object value.

- `Set` request

  The SNMP manager sends an SNMP message to the SNMP agent requesting that the agent update its value for the data object specified in the message. The SNMP agent updates the value of the specified object with the value provided by the manager in the request.

- `Trap` notification

  The SNMP agents sends an unsolicited SNMP message to the SNMP manager. The message contains a value of a data object that corresponds to a significant event which took place at the managed station where the agent is deployed. This is used to notify the manager of changes at the managed station.

The SNMP `Get` operation allows the management station to monitor the state of the monitored stations, while the SNMP `Set` operations allows the management station to perform control actions on the managed stations. The SNMP `Trap` messages are used to allow the SNMP agent to inform the management station of significant events that it observed without needing to receive an SNMP `Get` request. This allows important events to be reported outside of the polling cycle.

The data objects used in SNMP are defined according to the Management Information Base (MIB) shared by the SNMP-enabled devices in the network. The format used to define the MIB is specified in the Structure of Management Information (SMI) described in RFC-1155 **[37]**. The MIB has a hierarchical tree structure, with each leaf of the MIB representing a unique object. Each unique objects corresponds to the state of a network element. The values of the MIB objects can be transmitted or set through SNMP operations. Each SNMP agent only holds one value for each object defined in the MIB at any time. The MIB structure itself cannot be changed dynamically during operation, and SNMP-enabled devices can only access one leaf object in the MIB per SNMP `Get` and `Set` operation **[35]**. The standard MIB supported by the base version of SNMP is defined in RFC-3418 **[38]**.

Multiple versions of SNMP have been developed over time. The original SNMP was enhanced by Simple Network Management Protocol Version 2 (SNMPv2). SNMPv2 supports a distributed network management architecture that can have network nodes assume the role of both an SNMP agent and an SNMP manager **[35]**. Such a node will act as an SNMP agent when responding to a higher level network manager and act as an SNMP manager when requesting information from a subordinate SNMP agent. SNMPv2 also expanded on the SNMP SMI to include new data types and redefined how rows in a conceptual table are created and deleted. New SNMP operations were defined in SNMPv2 as well. These operations are the `GetBulkRequest` operation that allows

SNMP managers to request large blocks of data in one request and the `InformRequest` operation that allows information to be exchanged between two SNMP managers [35].

Both SNMP and SNMPv2 lack measures to defend against cybersecurity threats that compromise the confidentiality and integrity of messages exchanged through SNMP. To address these concerns, Simple Network Management Protocol Version 3 (SNMPv3) was developed. SNMPv3 adds encryption and message integrity check mechanisms to SNMP messages sent across the network. This is accomplished by the sharing of authentication and encryption keys between the management station and the monitored station, with the authentication key being used to cryptographically sign SNMPv3 messages and the encryption key being used to encrypt snmpv3 messages. Using these keys, SNMPv3 is capable of defending against message content modification, masquerade, message stream modification, and disclosure attacks. However, SNMPv3 does not provide effective defense against DoS attacks and traffic analyzes [35].

2.4 IEC 62351 Standard

The power industry is moving towards widespread adoption of the IEC 62351 standard to enhance the security of its systems. The IEC 62351 [39] standard consists of multiple parts. It gives specifications for information security measures to be used by several International Electrotechnical Commission (IEC) protocols used in power utilities. It was developed by Working Group 15 (WG15) of the IEC Technical Committee 57 (TC57) and intended to accompany some of the communication standards specifying protocols defined by the Technical Committee. The scope of the IEC protocols covered by IEC 62351 include the protocols defined in IEC 60870-5, IEC 60870-6, IEC 61850, and IEC 61970.

The IEC 62351 standard aims to address gaps in the end-to-end security of the information protocols in its scope. The standard considers both deliberate and inadvertent threats. Deliberate threats considered by the IEC 62351 standard include disgruntled employees, industrial espionage, vandalism, cyber hackers, computer viruses, theft, and terrorism. Inadvertent threats include safety failures, equipment failures, human error or carelessness, and natural disasters [39].

The definition of "end-to-end security" for information systems given by IEC 62351 is security that protects the information exchanged within telecommunication systems from the point of origin all the way to the point of destination [39]. According to IEC 62351, end-to-end security involves the use of security policies, access control mechanisms, key management, audit logs, and the protection of the information infrastructure itself [34].

2.5 Device and Communication Security in IEC 62351-7:2017

The goal of the IEC 62351-7:2017 standard [34] is to enhance the end-to-end security of power systems by covering security of devices, data transmissions, and communication traffic. Specifically, the standard describes the role that NSM plays in achieving the overall goal of the IEC 62351 standard to provide end-to-end security for power utilities. The monitoring and management actions specified for NSM can be performed in real-time alongside the monitoring and control actions done by the SCADA. The security functions performed by NSM are configuration management, performance monitoring, hardware equipment monitoring, software monitoring, communication network monitoring, and intrusion detection [34].

2.5.1 NSM Data Objects Specification in IEC 62351-7:2017

The IEC 62351-7:2017 standard specifies a set of NSM data objects to be used within an NSM platform for power system operations [34]. The data objects hold values, which are a representation of the current state of a corresponding system element. The data objects support health monitoring, performance monitoring, and intrusion detection. While the majority of data objects are meant to be provided to a manager application on request, some data objects are event notification objects. Event notification objects are transmitted by end devices to monitoring entities when certain data objects have their values updated. The event notification may include several data object values bundled into the same notification.

The set of NSM data objects specified in IEC 62351-7:2017 supports the management of performance, configuration, faults, and security for devices connected to the communication network of the power system. The NSM data objects are abstract data objects, and can be mapped to several

different protocols such as IEC 61850, IEC 60870-5, and SNMP [34].

A security monitoring system can use NSM data objects as a basis for security alert generation. However, the IEC 62351-7:2017 standard does not specify what actions are to be taken if an alert is raised based on collected NSM data objects. It is up to the designers of an NSM implementation for security monitoring to set procedures to perform in the event of alerts being generated based on NSM data.

2.5.2 IEC 62351-7:2017 Requirements

The IEC 62351-7:2017 standard provides a list of requirements that should be met by an NSM implementation. It is important to note that IEC 62351-7:2017 does not give specifications regarding the architecture or technologies to be used when implementing NSM. Other than the specific data to be collected, it is up to the developer of the NSM platform to design the architecture and components of the platform.

The IEC 62351-7:2017 requirements for NSM monitoring are described in the following subsections, and are grouped into several categories [34].

2.5.2.1 Network Configuration Requirements

An NSM implementation should have a means to monitor and modify the network configuration of the system. The IEC 62351-7:2017 standard gives the following examples for data regarding the network configuration that an NSM system should collect [34]:

- Network configuration information about connected end systems
- Commands related to power network equipment, such as on/off and reset commands
- Established paths to end devices through the network
- Switching commands to network equipment
- Changes related to access control lists and Role-Based Access Control (RBAC) rules, and
- Parameter changes to automated network actions

2.5.2.2 Network Backup Requirements

It is important that backup equipment and redundant paths be available in the power system to reduce downtime when a failure in operations equipment occurs. The IEC 62351-7:2017 standard gives the following requirements for what data related to backup equipment in the network is to be monitored **[34]**:

- The status of backup equipment
- The status of backup communication links, including their available bandwidth
- Failovers to alternative or backup network equipment that have already taken place
- The time when failovers to backup equipment have taken place, and
- Transitions to alternate or backup communication links

2.5.2.3 Communication Failures and Degradation Requirements

Performance monitoring is part of network management, and being able to monitor the health of network communication equipment and communication links is an essential part of performance monitoring. Many vendor IEDs provide data applicable for communication network monitoring in Information Technology (IT) environments. However, the communication network found in power systems tends to differ substantially from IT networks in that the power system network uses many point-to-point direct communication links between the control centre and controlled stations. The IEC 62351-7:2017 standard gives the following requirements for what data related to communication link failure and degradation is to be monitored **[34]**:

- Temporary or permanent failures in network equipment
- Network equipment resets
- Communication link failures
- Communication link degradation (lower than expected throughput)

- Network routing degradation, and
- Logging equipment failures

2.5.2.4 Communication Protocol Monitoring Requirements

Data collection on the usage and statistics of communication protocols used in the power system network is important for security monitoring that can detect threats within the network. This data collection must be tailored to provide relevant information about the specific ICS protocols being used for power system operations. The IEC 62351-7:2017 standard gives the following requirements for what data related to the protocol stacks in the network should be collected using NSM data objects **[34]**:

- Communication protocol version and status
- Mismatches between protocol versions
- Malformed protocol messages or message tampering
- Inadequately synchronized time clocks across networks
- Evidence of resource exhaustion (DoS)
- Evidence of buffer overflow (DoS)
- Physical access disruptions
- Invalid network access attempts
- Protocol statistics on network equipment (average message delivery times, size of messages, counter for number of messages received)
- Audit logs and records
- Protocol timeouts, and
- Statistics on invalid sequence numbers of application messages

2.5.2.5 End System Management Requirements

Centralized monitoring of the health of end devices such as IEDs is important for performance and security monitoring of the network as a whole. Issues local to end devices should be detected to help determine what corrections need to be made to restore the device to its top performance and what security threats may have compromised the device. Some of this information can be obtained through a direct enquiry on the device itself by a remote entity, while other information may need to be inferred from device behaviour and traffic flows that is observable by an external entity. The IEC 62351-7:2017 standard gives the following requirements for what data from end devices in the network should be collected by monitoring and control entities **[34]**:

- Use of invalid application data
- Invalid requests and commands that have been received
- Command messages that are out of sequence
- Status of the end device (running, stopped, suspended, error state, etc.)
- Status of network connections established by the end device
- Status of keep-alive messages
- Status and statistics on backup mechanisms and their usage history
- Status on data reporting
- Data access anomalies
- Number and times of starts and stops for end devices and applications
- Event logs, and
- Recovery indications after correcting failures

2.5.3 Required NSM Data Objects for Support of Intrusion Detection

Support of intrusion detection in the network is an essential security feature of IEC 62351-7:2017 NSM. The detection capabilities provided by NSM should be capable of detecting obvious intrusions as well as subtle intrusions signalled by changes in the state of system assets **[34]**. The NSM data objects defined in IEC 62351-7:2017 are designed to capture the state of system assets to monitor any changes in the configuration or communications of the assets. IEC 62351-7:2017 lists several data objects that are required in order for NSM to be capable of detecting the various intrusions considered by the standard.

2.5.3.1 Detection of Unauthorized Access

Among the key security threats to detect through intrusion detection is use of the system by an unauthorized entity. IEC 62351-7:2017 lists the following as being requirements for data that must be captured by NSM data objects to detect unauthorized access **[34]**:

- Instances of an unauthorized user attempting to open a connection or transmit a message, based on a whitelist of authorized users for each connections, and
- The identity of any unauthorized users

IEC 62351-7:2017 additionally requires that the list of authorized users is updated regularly, though this process is not required to utilize the NSM data objects and is up to the discretion of system operators.

2.5.3.2 Detection of Resource Exhaustion

According to IEC 62351-7:2017, power system networks, where IEC communication protocols are used, tend to have lower network bandwidth availability than traditional IT protocols and may support fewer concurrent connections **[34]**. This means that the amount of network resource consumption required for an attacker to degrade the network as part of a DoS attack is significantly lower than is required in enterprise networks. Detection of resource exhaustion within power system networks needs to be custom tuned to the available network resources for the monitored power

system. IEC 62351-7:2017 gives the following list of requirements for what data is to be captured by NSM data objects for the detection of resource exhaustion [34]:

- Instances of the maximum number of permitted network connections being exceeded
- Current number of connections open in the network
- Instances of the maximum number of simultaneous network connections being exceeded
- The current number of connections used simultaneously in the network
- Instances of an equipment CPU load limit being exceeded, and
- Instances of an equipment memory usage limit being exceeded

2.5.3.3 Detection of Invalid Buffer Access

An attack against a digital device may cause it to experience a buffer overflow or underflow. Buffer errors are observable within the application layer of the attacked device, and should have a means of reporting such errors as part of NSM. IEC 62351-7:2017 lists the following requirements of data to be collected through use of NSM data objects to detect buffer access issues [34]:

- Number of buffer overflows detected
- Number of buffer underflows detected, and
- Indicators for the source that caused buffer overflows or underflows

2.5.3.4 Detection of Malformed Packets

Deliberately malformed packets, or Protocol Data Units (PDUs) as they are sometimes called, can be transmitted over the network to cause undesirable behaviour in the device that receives a malformed PDU. Malformed packets can be identified by the application layer of the device that receives them, and this awareness of malformed packets by the device can be leveraged by NSM to detect the transmission of malformed packets across the network. IEC 62351-7:2017 gives the following list of information about malformed packets to be collected by NSM data objects [34]:

- Number of malformed PDUs detected
- Number of tampered PDUs detected, and
- Indicators for the source that transmitted malformed or tampered PDUs

2.5.3.5 Detection of Physical Access

An attacker having physical access to power system devices is particularly dangerous, as this allows the attacker to directly disconnect or power down the device to disable its operation functions. In order to support end-to-end security, it is necessary for NSM to be able to determine if physical access of a device is currently under way. IEC 62351-7:2017 lists the following data as being necessary to detect physical access of equipment through NSM data object collection **[34]**:

- The time at which power to equipment was lost
- The time at which power to equipment was restored
- The time at which a media device was disconnected from equipment, and
- The time at which a media device was reconnected to equipment

2.5.3.6 Detection of Invalid Network Access

Firewalls can restrict access to network by a specified set of Internet Protocol (IP) addresses as well as restrict port usage and filter out messages with certain characteristics. However, firewalls are less effective at preventing invalid network access between devices internal to the firewall and malicious sources external to the firewall. External parties can transmit invalid or malicious payloads to internal ones, with mitigations against such payloads requiring application-level protections within recipient devices **[34]**. There are still potential indicators of such invalid network access in the network that can be observed through NSM in order to assist in the detection of network misuse. IEC 62351-7:2017 gives the following list of data to be collected with NSM data objects for supporting the detection of invalid network access **[34]**:

- Unusual frequency of communication between network devices

- Unusual volume of network traffic between network devices, and
- Suspicious message payload

2.5.3.7 Detection of Coordinated Attacks

Coordinated attacks that aim to disrupt multiple utility grid operation systems can have much more dramatic impacts than would be expected from an attack on a single such system. NSM, as described in IEC 62351-7:2017, offers some means of detecting that a coordinated attack has been launched. In order to support the detection of coordinated attacks, IEC 62351-7:2017 requires that following set of data is collected with NSM **[34]**:

- All instances of communication failures
- All instances of end system failures, and
- All instances of DoS attacks that have been detected

In order to have a clear understanding of the sequence of events during coordinated attacks, it is required that all NSM data objects have timestamps with millisecond precision awhile being time-synchronized **[34]**.

2.5.4 NSM Data Objects Packages

The NSM data objects defined in the IEC 62351-7:2017 standard are grouped into several packages within the standard, with the data objects within the same packages being related to the same area of the cyber-physical system. The following are the NSM data objects packages defined in IEC 62351-7:2017 **[34]**:

- **Environmental Data Objects**

  The data objects, in this package, cover data regarding physical access of monitored IEDs as well as the state of their power supply.

- **IED Data Objects**

The data objects, in this package, cover data regarding the configuration and operational state of monitored IEDs.

- **Interfaces Data Objects**

  The data objects, in this package, cover data regarding the various different interfaces available in monitored IEDs. This includes serial, Ethernet, analogue, keyboard, and Universal Serial Bus (USB) interfaces.

- **IEEE 1815 and IEC 60870-5-104 Data objects**

  The data objects in this package cover data regarding the usage of the IEEE 1815 DNP3 protocol and the IEC 60870-5-104 protocol in the monitored network. These two protocols are very similar due to being founded on the same basic research **[25]**. This allows most of the data objects in this package to be applicable to both protocols. The data objects in this package are further distinguished as being applicable to master or slave applications.

- **IEC 61850 Data Objects**

  The NSM data objects in this package cover data regarding the usage of the IEC 61850 suite of protocols, which are designed for use in the electric substation, in the monitored network. These data objects are further broken down into subpackages depending on the specific IEC 61850 protocol to which they are applicable. This includes subpackages for the GOOSE, SV, and MMS protocol.

- **Clock Data Objects**

  The NSM data objects in this package cover data regarding the status and health of clock synchronization devices.

In addition to the packages it defines above, IEC 62351-7:2017 specifies that data objects related to the usage of Transmission Control Procotol (TCP), User Datagram Protocol (UDP), and IP in the network be monitored for NSM. Several existing Request for Comments (RFC) documents already give specifications on the collection of data concerning these protocols. Rather than define its own NSM data objects to cover data collection for them, IEC 62351-7:2017 specifies that these RFCs are to be used for the monitoring of these protocols for NSM.

2.6 Conclusion

In is chapter, an overview of the concepts related to this research is given. Among these concepts is the microgrid. This overview covered the role that the microgrid plays in the smart grid, the architecture of physical and communication layers in the microgrid, the microgrid communication protocols, and the microgrid cybersecurity threats. This chapter also covered the concept of NSM and its application in power systems. Specifically, the focus is on the use of NSM as specified in the IEC 62351-7:2017 standard for power system security. The protection and data model requirements given in IEC 62351-7:2017 are listed and the security reasons for these requirements are explained.

This chapter presents the context to the problem of microgrid security monitoring that this research seeks to address. It specifically describes the problem domain of the microgrid system, and highlights microgrid cybersecurity concerns. It also describes the core components of IEC 62351-7:2017, which is used to reach the research objective of enhancing microgrid security monitoring. With this background information, the achievements and insights of the related work on microgrids and their cybersecurity can be better understood.

Chapter 3

Related Work on Microgrid Architecture and Security

This chapter describes related work on the topics of microgrid architecture and microgrid cybersecurity. These topics are core elements of the background knowledge required for this research. Figure 3.1 presents an overview of the topics covered in this chapter across the presented body of related work.

Related work on microgrid architecture describes the various technologies used for microgrid power distribution and control. The microgrid is composed of a power network layer and a communication. The power network contains the power generation and distribution equipment as well as protection and control equipment that ensure safety of the power network. The communication network provides a medium for the central microgrid control centre to monitor and control the microgrid power equipment. This involves the deployment of networked devices that exchange messages with the microgrid control centre over digital communication channels and which exert control over the power network based on command messages received from the control centre.

The focus of related work on microgrid cybersecurity in related work is split between discussion on microgrid vulnerability to cyberattacks and proposed mitigations for those cyberattacks. Research on microgrid cybersecurity vulnerabilities explore both the nature of the cyberattacks and

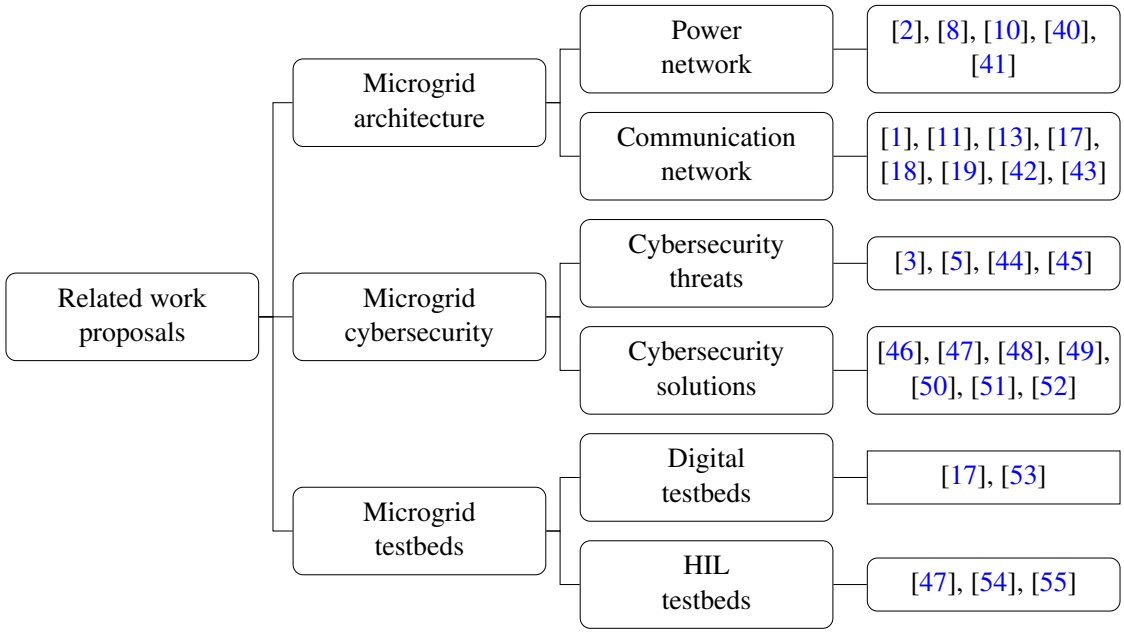

Figure 3.1: Related-work proposals

their potential impact on the microgrid. Regarding cybersecurity mitigation, several different strategies have been explored for cybersecurity solutions in the related work proposals.

The use of a microgrid simulation testbed in this research makes contributions pertaining to the development of microgrid experimental testbed development an important reference source. The microgrid testbeds discussed in this chapter are used to study microgrid power and control operations, as well as being used to evaluate the effectiveness of proposed cybersecurity solutions at mitigating attacks.

3.1 Microgrid Architecture

Microgrid technology is still advancing, and different microgrid architectures continue to be explored. Microgrids consist of both a power system network and digital communication network. The power system architecture considers the kind of power that is delivered to consumers and how the various power sources and loads are interconnected. The communication network architecture considers the flow of information, the technologies and protocols used to exchange messages, and how communication devices are linked to each other.

The related work on the microgrid focuses on either the power network or the communication network. This can be explained by the expertise involved in understanding the power network differing considerably from that of the communication network. The related work on microgrid architecture presented here is separated into contributions the power network and ones for the communication network. Nevertheless, both networks are essential to the operation of the microgrid.

3.1.1 Power Network

This section presents the related work on assessments made for various microgrid power network architectures. The advanced proposals discuss the design behind these architectures and their impact on system reliability, efficiency, and power quality. Also, the related work proposals on control operations in the microgrid power network are discussed. The related work on microgrid power networks is presented is presented in Figure 3.2.

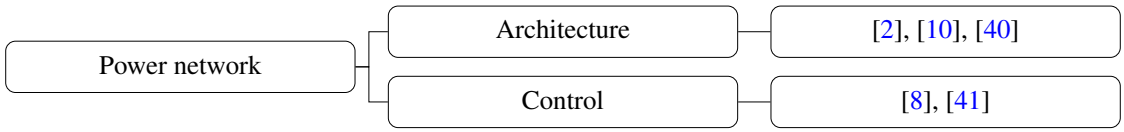

Figure 3.2: Related work on power network architecture and control

3.1.1.1 Architecture

Microgrid power network architecture refers to the placement and interconnectedness of the various components in the microgrid. Among these components are the DERs, the consumer loads, and the electrical equipment. Examples of electrical equipment are circuit breakers, protection relays, measurement meters, converters, and transformers. An important consideration for a given microgrid system is whether it delivers electricity using AC or DC. Microgrids will often have some sections providing AC and other sections providing DC, depending on the type of DER. For example, wind turbines provide AC, while PV arrays provide DC. However, the consumer loads are generally compatible with either AC or DC exclusively. In the case of a mismatch between the type of current supplied by a DER and the type accepted by a load, a converter is needed to change the type of current. A converter is also needed if there is a mismatch in frequency between two connecting AC sections of the microgrid.

Patrao *et al.* [10] give an overview on the various microgrid power network architectures that are most commonly deployed. The microgrid systems they consider provide enough power to fulfill the energy needs of a local area even when operating in islanded mode, disconnected from the main grid. The considered microgrid systems are composed of Distributed Generations (DGs) units, ESSs, intelligent circuit breakers, and local loads. Regarding DGs unit, Patrao *et al.* claim that a generator is widely defined as being distributed if it provides less than 50 MW. As examples of DGs, they mention micro turbines, fuel cells, wind generators, photovoltaic generators, and Combined Heat and Power (CHP) generators. Patrao *et al.* propose a microgrid architecture classification consisting of six main groups: AC-microgrid, DC-microgrid, hybrid AC-DC microgrid, AC-microgrid with DC-storage, DC-zonal microgrid, and Solid State Transformer (SST) based microgrid [10]. These main groups are compared with one another with consideration of factors such as the number of series connected power converters, the required number of power electronic interfaces, and the difficulty of managing energy storage. When assessing the advantages of each architecture, Patrao *et al.* find that AC-microgrids systems connecting to the main grid through a static switch have the most reliability, due to consumers having a direct connection to the main grid when AC-microgrids are in grid-connected mode. They add that AC-microgrids are easy to integrate into existing AC power systems [10]. Patrao *et al.* also find that microgrid reliability increases as the number and complexity of power electronic interfaces decreases, with SST and hybrid AC-DC microgrids having the least complexity. For microgrids requiring high power quality, they recommend SST, DC, and DC-zonal microgrids. The focus of the work done by Patrao *et al.* is on the power network architecture, with the communication architecture and protection schemes of microgrids not being part of the scope.

Fu *et al.* [2] provide a detailed review on microgrid systems that considers microgrid systems with AC, DC, and hybrid architectures. The authors list power reliability demands, the need for energy security, integration of renewable energy, and overall higher system efficiency as some of the motivations for the development and deployment of microgrid technology. One of the key challenges mentioned regarding microgrid deployment is the need for fast and reliable supervision and monitoring. Fu *et al.* describe the increasingly popular three-layer natural droop control that is

being used to address these challenges. The three-layer droop control has a lower layer that provides autonomous control of power, a dispatch layer that monitors and controls active and reactive power, and an optimization layer capable of unit commitment and optimization based on contextual information such as that gained from load forecasting. Fu *et al.* also describe the role of IEDs and the microgrid controller in addressing these challenges. Different digital communication protocols that can be used for microgrid monitoring and control are also mentioned. Among them is Modbus, which used as a legacy protocol capable of transmitting messages over serial and TCP that is easy to design and implement but does not scale well. Also mentioned is DNP3, a communication protocol used between components in process automation systems. In addition, Fu *et al.* state that the protocols defined in the IEC 61850 standard could become a key solution to microgrid control and communication. While not originally aimed at the microgrid, some of the protocols proposed in the IEC 61850 standard could be used in a microgrid context. As an example model, Fu *et al.* also give some details on the U.S. military Fort Sill microgrid with ratings of 480 V, 60 Hz, and 715 KW **[2]**.

Mariam *et al.* **[40]** present a literature review on the trends being followed for microgrid architectures and the policies surrounding them. They gathered technical information from 45 different microgrids and microgrid testbeds across Europe, USA, and Asia. Among those microgrids, three DC-microgrids, two real-time emulation studies, one High Frequency AC (HFAC), and 39 50Hz AC-microgrids. They compare DC-microgrids to AC-microgrids and find that DC-microgrids have fewer power quality problems and lower power losses. However, AC-microgrids are easier to integrate with the main utility grid and have lower cost to deploy. The HFAC microgrid has increased efficiency due to minimizing current harmonics and can field smaller power transformers, but suffers from increased power loss across large transmission distances and requiring more complex equipment. Mariam *et al.* also study the popularity of the different DG sources used in the microgrid, finding that the most commonly used DG sources are PV, WT, micro-hydro, and diesel. In addition, they discuss the relevance of the IEEE 1547 standard for the interconnection of DER with EPS. The authors do not present any economic information concerning the studied microgrids, but emphasize the importance of optimizing the economical aspects of the microgrid in addition to the technical aspects. They also propose that the improved power quality of DC-microgrids over AC-microgrids warrants further development efforts to be invested in DC-microgrids **[40]**. As part of a different

literature review, Mariam *et al.* **[9]** study the architectures of existing and simulated microgrid systems. This literature review highlights that the majority of microgrid testbeds reviewed had an AC architecture. They attribute the popularity of AC architectures to the ease in the integration of AC-microgrids into the main grid due to the use of AC systems in main grids and most loads.

3.1.1.2 Control

Microgrid power network control refers to the microgrid functions responsible for dynamically changing the configuration of the microgrid. This is often done with the goal of maintaining the stability of the microgrid. Control operations include the disconnecting of a DER, the changing the reference setpoints of DERs to change their power output, and changing the microgrid operation mode from grid-connected to islanded mode or vice-versa. Proper control requires a means of information flow across sections of the microgrid, as control operations are generally performed as a response to an observation. For example, the power output of a microgrid energy source may be changed based on the measured microgrid frequency.

Guerrero *et al.* **[8]** discuss the findings from their study on different control techniques for microgrids. Included in the study is the research conducted for decentralized, distributed, and hierarchical control in microgrids operating in grid-connected and islanded modes. They investigate some key microgrid concerns. These concerns include inverter control, power stability, time synchronization, and transition between grid-connected and islanded modes. The study focuses on microgrids with radial architectures, which they define as a system where each energy source is connected to at most two other sources. They chose to study radial architectures because of a large body of prior research being available for radial microgrids. More complex architectures, such as meshed architectures that have more interconnections between energy sources than radial architectures, have more room open for research **[8]**.

Davison *et al.* **[41]** discuss how the adoption of an enhanced microgrid design helps address the issues related to the widespread use of DG, focused around the context of the Australian electricity industry. The issues related to the use of DG include voltage fluctuations, power quality resonance, reverse power flows, reduced protection coordination, difficulty in detecting high impedance faults, and energy transmission losses due to current harmonics. In addition, DGs struggle to incorporate

end users in the electricity market as intermittent generation sources. According to Davison *et al.*, the benefits of microgrid adoption include increased supply reliability, reduced customers electricity prices, reduced transmission losses, and a reduced carbon footprint. The microgrid design that Davison *et al.* propose has a decentralized architecture with a three-level hierarchy. The three-level hierarchy has a primary level for direct voltage and current control, a secondary level for reference adjustments and synchronization across the microgrid, and a tertiary level for coordination with the rest of the power grid. They also propose that a bidirectional power converter be used in place of a static switch at the PCC, providing benefits such as the controlled importation and exportation of energy as well as the capability for galvanic isolation. They identify several concerns for the microgrid that required further research to address adequately. Among these concerns are the economic viability of the proposed design, the optimal bidirectional power converter topology, and the development of mechanisms for the microgrid to control the decentralized electricity market **[41]**.

3.1.2 Communication Network

This section presents the research on the design and the application of microgrid communication network architectures. Specifically, it presents the related work on microgrid control and on the use of particular communication technologies such as the IEC 61850 protocols. Because of the reliance on digital communication between remote devices and the main grid for vital control and monitoring operation, the microgrid communication network is an important topic to cover. Figure 3.3 presents the focus of the related works on microgrid communications.

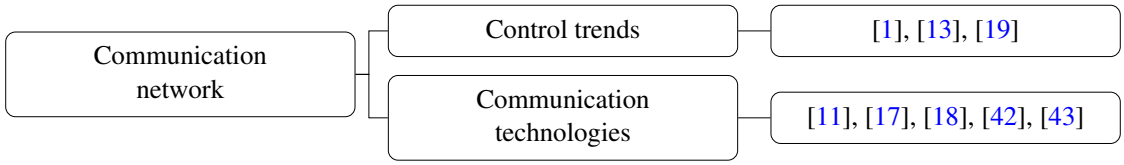

Figure 3.3: Related work on microgrid communication networks

3.1.2.1 Control Trends

The microgrid communication network provides a means for information necessary for control operations to flow from one device to another. This flow of information is important for the

coordination of the scattered microgrid DERs and loads in order to achieve the goals of optimization, maintaining system stability, and security. Control operation are separated into three levels: primary, secondary, and tertiary. The role performed by each level is presented in Figure 3.4, as described by Olivares *et al.* **[13]**. The primary level controls voltage and current at a local level within the power network. The communication network is required for secondary and tertiary level control used for coordination within one microgrid and across multiple microgrids, respectively. The discussion of microgrid control focuses on strategies being adopted for microgrid control and what the control operations are trying to achieve as an end goal.

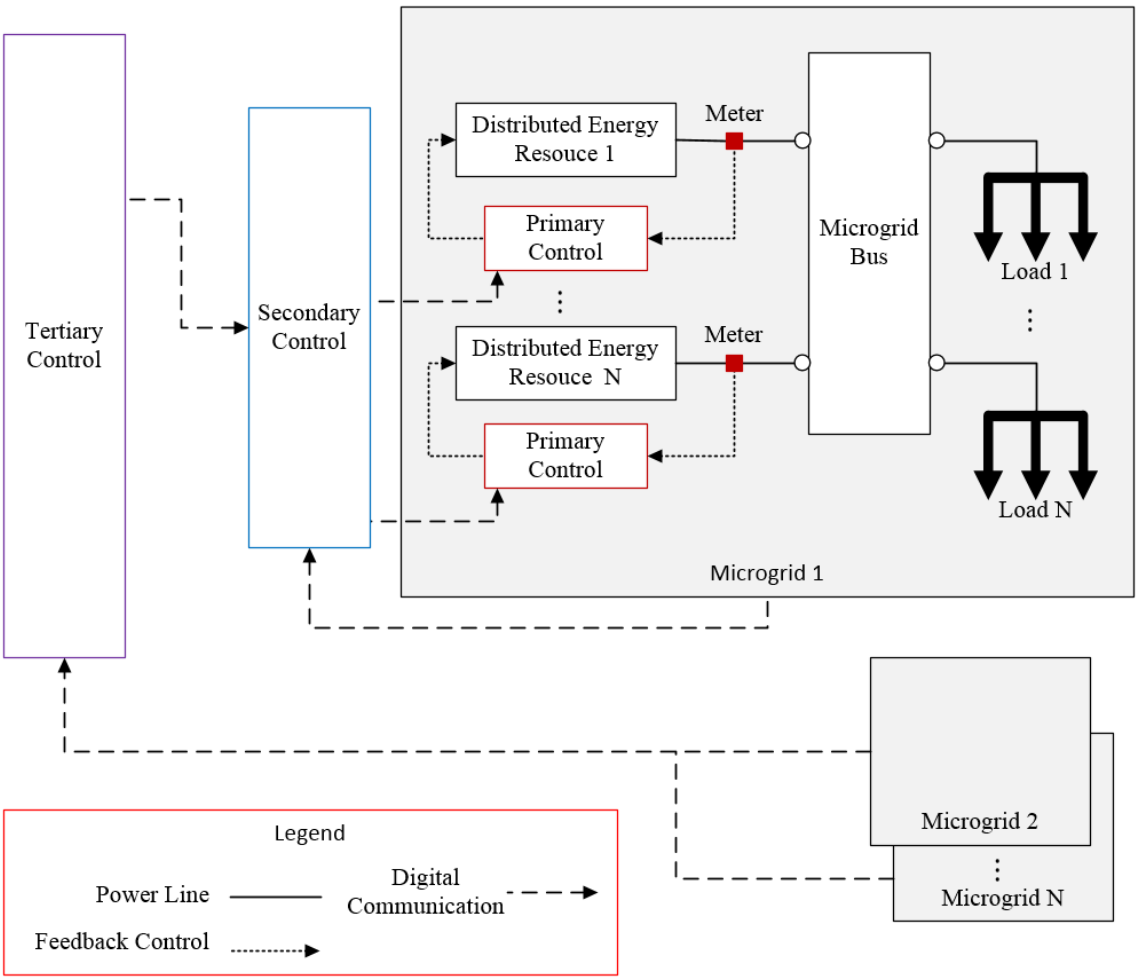

Figure 3.4: Primary, secondary, and tertiary control levels

Safdar *et al.* **[1]** present the findings of their survey on microgrid communication infrastructures.

In this survey, they describe many of the requirements commonly shared by microgrids. These include the need to deliver reliable power quality, respond rapidly to faults for self-healing, and be resilient to cyberattacks as well as physical attacks. Safdar *et al.* break down some of the core components that make up the microgrid management system and communication infrastructure. They discuss the variety of technologies used in the microgrid communication infrastructure, such as wireless, Ethernet, and fiber communication lines. They also explain how the communication infrastructure is divided into home area, field area, and wide area networks. They highlight some of the important issues relevant to microgrid communications. This includes bandwidth issues, time-critical applications, network security, low computational capacity of some sensor devices, and efficiency concerns **[1]**.

In their survey, Olivares *et al.* **[13]** discuss trends in microgrid control. They explore options for microgrid protection and control functions that allow microgrids to address several challenges that face their operation. Some of these challenges include power stability issues, bidirectional power flows, electrical frequency deviations, and uncertain load demands. Olivares *et al.* classify microgrid control functions into three levels, which together form a hierarchy: primary, secondary, and tertiary. Primary control involves local control operations and includes output control, islanding detection, and power balance. Secondary control operates across the entire microgrid, coordinating between the geographically dispersed DERs and their primary control to enhance the reliability and efficiency of the microgrid. Tertiary control is used for coordination of the microgrid with the main grid and other microgrids in order to accomplish high level smart grid objectives **[13]**.

Bani-Ahmed *et al.* **[19]** explore the state-of-the-art on microgrid communications. They describe how microgrid operations have a feedback loop involving IEDs that monitors the power system data from the DER and passes that information to the microgrid controller. The microgrid controller responds to the IEDs with control commands and the IEDs in turn issue commands to the DERs. The loop described can include HMIs that allow human operations to be part of the monitoring and control functions. According to Bani-Ahmed *et al.*, Modbus and the IEC 61850 protocols can be used for digital communications between IEDs and microgrid controllers, while DNP3 is popular for messages between master SCADA systems and slave devices. They emphasize that microgrid communications have more need for reliability and fault tolerance than traditional IT

communications because the microgrid plays a more critical role to consumers overall. How to best design the microgrid communication system to optimize reliability and delay of time-sensitive data and how to extend IEC 61850 data models to more traditional data models like DNP3 are issues that Bani-Ahmed *et al.* left for future research **[19]**.

3.1.2.2 Communication Technologies

When discussing communication technology, the focus is on how information flows between devices. This includes the specific medium used to transmit information, with Ethernet cables being but one example. It also includes the structure of the information being transmitted and the protocols being followed by devices engaging in information exchange.

Islam and Lee **[17]** propose a mapping of microgrid monitoring and control to the protocol suite given in the IEC 61850 standard. They argue that some of the protocols described in IEC 61850 can be applied to meet microgrid communication requirements. They present the need for a communication network that allows digital communication between remote agents and a microgrid control centre. The control centre is responsible for monitoring and managing microgrid energy sources and loads. It also provides voltage and frequency references as well as the setpoints for active and reactive power of DERs. Islam and Lee describe the need to deploy IEDs at each protection point of the microgrid. In particular, they specify that each protection point should have a circuit breaker IED, a measurement IED, and a protection and control (P&C) IED. As for the communication medium, they describe the suitability of Wi-Fi and WiMAX as technologies to enable digital communications. They also describe the potential to use integrated wired and wireless technologies to build a microgrid communication network, with wired links enabling communication between local devices and wireless links enabling remote device communications. Islam and Lee describe the performance analysis of the microgrid network adopting IEC 61850 that was simulated using Optimized Network Engineering Tool (OPNET) for both grid-connected and islanded modes. The simulation uses WiMAX for wireless communication and had two main feeders, two sub-feeders, one storage unit, seven DG units, and nine load points. The simulation also makes use of wired network links for communications between local agent devices that model IEDs. However, Islam and Lee note that the transmission delays within wired network links are negligible compared to

those found in wireless links, with wired link delays only reaching several microseconds. For this reason, their performance study only considers the wireless network. Through experiments on the OPNET simulation testbed, Islam and Lee measured the rate of traffic in the microgrid communication network when using IEC 61850 protocols. The results of their simulations suggest that an integrated network of wired and wireless communication can meet the time constraints of the raw messages and was sufficiently reliable **[17]**.

Ruiz-Alvarez *et al.* **[42]** present a microgrid management system based on IEC 61850 automation. They explain that DERs require active network management to be properly integrated into the grid, and that automation technologies are needed to efficiently control them. They use the three microgrid emulators commissioned by the Catalonia Institute for Energy Research to test their proposed management system. Each emulator consists of a wind generator, a battery, and a variable load. The management systems is composed of three layers. The top layer is composed of a remote management unit that manages the microgrid at a high level. The middle later consists of an iNode controller that sets the active and reactive power of all microgrid nodes so as to maintain microgrid stability. The bottom layer consists of iSocket controllers that set the active and reactive power of their respective microgrid unit in a way that ensures their safety. The remote management unit, iNode, and iSockets are all connected to the same local network using Ethernet cables. Communication between the remote management unit and the iNode is performed over Telnet, while communication between the iNode and iSOckets is performed across the Ethernet cables in accordance with IEC 61850. Ruiz-Alvarez *et al.* apply IEC 61850 to their proposed system by extracting the useful information being used in their system and mapping that information to Logical Nodes and Logical Devices defined in IEC 61850. The three layer architecture can switch between centralized mode and distributed mode. The iNode controls the power of each microgrid unit in centralized mode, while only the iSockets control them in distributed mode. Ruiz-Alvarez *et al.* cite several reasons for pursuing the use of IEC 61850 in their proposed management system. These include code reuse and maintainability, the speed of the IEC 61850 MMS protocol, and the definition of a structured data model within IEC 61850 **[42]**.

Deng *et al.* **[43]** propose another solution for a microgrid system with operation based on the

IEC 61850 standard protocols. They describe the difficulties faced by SCADA systems when managing equipment with multiple protocols. These issues are especially relevant during the transition from grid-connected mode to islanded mode and vice-versa. Deng *et al.* argue that a microgrid with "plug and play" functionality can reduce the configuration and integration time for equipment. The microgrid model with the proposed "plug and play" functionality allows the microgrid control system to communicate with the IEDs managing the microgrid monitoring and control equipment through the IEC 61850 MMS, GOOSE, and SV protocols. The model that Deng *et al.* propose has status information, measured values, controls, and settings exchanged through IEC 61850 protocols. The model also uses IEC 61850 to perform the transition between grid-connected mode and islanded mode. Deng *et al.* verify their solution on a microgrid test platform with real equipment for the power and information devices. The microgrid tested model has a power system network composed of various DER sources, loads, and energy storage systems. The information system used in this microgrid is composed of IEDs that controlled the power system components and exchanges information with the microgrid control system **[43]**.

Gu *et al.* **[11]** propose a design for a Microgrid Protection Management System (MPMS). The IEDs and the SCADA system that are part of the MPMS use IEC 61850 protocols to protect the microgrid against power system faults. The design that Gu *et al.* propose has the MPMS separated into an information center, an operation center, and a policy center. The Information center gathers monitoring data from IEDs through IEC 61850 and detects microgrid topology with depth-first search. The operation center calculates the forward and reverse current of IEDs based on the data received by the information center. The policy center decides on the switching strategy for moving between grid-connected mode and islanded mode, using IEC 61850 protocols for communication with IEDs. The proposed model has the IEDs synchronized with a Network Time Protocol (NTP) server. Gu *et al.* performed experiments on a microgrid simulation model built in MATLAB Simulink and the Elipse Power Studio software. The experimental model is based on a microgrid model from the Institute of Nuclear Energy Research in Taoyuan, Taiwan. The simulation results show that it is feasible for the proposed MPMS to be capable of preventing some microgrid failure scenarios **[11]**.

In their article, Bui *et al.* **[18]** present a wide range of microgrid technologies and communication standards for the purpose of deciding on an appropriate unified standard to apply for building

microgrids in Taiwan. They also outline a set of practical tests for critical microgrid applications. They explore the kinds of communication links that can be used in the microgrid, which includes both wired technologies such as Ethernet and wireless technologies such as WiMAX. In regards to communication protocols, Bui *et al.* consider the IEC 61850, DNP3, and Modbus protocols. They also consider the IEEE 1547 standard that covers the operation of the static switch located at the PCC. To study the effectiveness of different microgrid technologies and standards, they perform tests on the microgrid testbed built by the Institute of Nuclear Energy Research in Taiwan **[18]**. The testbed consists of a 380V AC microgrid and uses the IEC 61850 series of protocols for communication between IEDs. It also uses devices enabled with DNP3 and Modbus communication passing through gateways that them with the IEC 61850 communication. Bui *et al.* propose practical tests for IEC 61850 that cover IED protection functions across different manufacturers, information exchange between DERs that control microgrid power flow, microgrid energy management, and the performance of different microgrid communication technologies. They also propose practical tests for the IEEE 1547 standard, DER installations, and power electronic interfaces **[18]**.

3.2 Microgrid Cybersecurity

This section presents the related work on microgrid cybersecurity. The related proposals are categorized into the topics of cybersecurity threats and solutions.

3.2.1 Cybersecurity Threats

This section presents studies on the current state of cybersecurity in the microgrid within the context of the smart grid. These contributions uncover various attack vectors that can be used when attacking the microgrids. Among these vectors are Distributed Denial of Service (DDoS), malware, and packet tampering.

Chlela *et al.* **[5]** explore possible cyberattacks against islanded microgrids, which use controllers to coordinate DERs and their associated control loops. They focus of the impacts of attacks against the availability and integrity of the microgrid. Chlela *et al.* discuss how DoS attacks that block, delay, or corrupt information flow lead to loss of availability in the microgrid. They also

explain that the loss of integrity in the microgrid occurs as the result of attacks that perform malicious modification the information flowing the network, without making the information look illegitimate or corrupt. Chlela *et al.* consider the DERs, the microgrid controller, and the communication network used for information exchange between microgrids to be the three main access points for cyberattacks in their study. Cyberattacks examples discussed by Chlela *et al.* include modification of the isochronous DER settings, modification of active and reactive power commands sent to controllable loads, DoS attacks on the non-isochronous dispatchable DER, and DoS attacks on controllable loads. They use a real-time testing platform based on a 25KV distribution system to demonstrate these attacks. The testing platform consists of two OPAL-RT Digital Real-time Simulators (DRTSs) that communicated using the IEC 61850 GOOSE protocol, with the Ethernet communication links having a star architecture. Based on the results of these experiments, Chlela *et al.* conclude that relying on local control loops can help mitigate cyberattacks impact, and that DoS resilience is increased when the microgrid switches to decentralized control upon detection of communication link loss **[5]**.

Zhong *et al.* **[3]** discuss several security vulnerabilities in the microgrid information network as well as possible solutions to address these vulnerabilities. These vulnerabilities include side channel attacks, DDoS, privacy leakage in the AMI, malware, software flaws, and theft of service. They emphasized that the microgrid is a critical infrastructure, therefore it must be operational during active attacks. Some of the solutions that Zhong *et al.* suggested for defending against cyberattacks include traffic camouflaging via artificially induced dummy packets, DDoS attack detection algorithms, and defensive kernel rootkits. The proposed solutions are however not strictly applicable to the microgrid and may be applied to corporate computing networks as well. Zhong *et al.* conclude by stating that further study in regards to microgrid cybersecurity is needed **[3]**.

Maynard *et al.* **[44]** explore the effectiveness of Man in the Middle (MitM) attacks against SCADA networks using the IEC 60870-5-104 (IEC 104) protocol for telecontrol communications. Maynard *et al.* consider both modification and injection of IEC 104 Application Protocol Data Units (APDUs) as possible means to attack the microgrid through MitM. They designed two experimental test environments. One of them simulates SCADA master and slave device endpoints using QTester and WinPP104, respectively. The other makes use of the testbed built by LINZ

STROM GmbH, which is an electricity Distribution System Operator in Austria, as part of the FP7 PRECYSE project. The testbeds have a SNORT Intrusion Detection System (IDS) installed on the switch that forwards IEC 104 traffic across the network. Maynard *et al.* run experiments where a MitM attack is successful on the tested SCADA network, for example by making use of Address Resolution Protocol (ARP) poisoning. During the experiment, the IEC 104 traffic is intercepted by the attacker positioned within the network and is either replayed back into the network or has its Application Service Data Unit (ASDU) modified before it is transmitted back through the network. They show that replayed IEC 104 packets would appear as normal traffic in the network but would be rejected by the Snort IDS and the TCP/IP stack due to having incorrect sequence numbers. However, it is also shown that modification attacks can be engineered to evade the various network checks while still having potential to cause adverse physical effects, for example changing an "ON" message to "OFF" in a IEC 104 ASDU to hide a ground fault. According to Maynard *et al.*, the IEC 62351 standard has specifications designed to prevent eavesdropping, replay, and spoofing for IEC 104. However, they claim that it is rarely deployed in real systems due to practical issues. In terms of mitigation strategies against these MitM attacks, Maynard *et al.* recommend taking steps to block possible channels that can be used for MitM attacks, such as the blocking of ARP poisoning **[44]**.

Liu *et al.* **[45]** present a risk assessment method for evaluating microgrid cybersecurity that makes use of Markov-based techniques. The risk assessment considers syntactic attacks such as viruses and worms as well as semantic attacks such as message modification. The proposed risk assessment method considers the primary, secondary, and tertiary control layers as attack entry points. The considered attacks include modification of measurements, modification of control parameters, and altering of DG behaviours by targeting information flows. Liu *et al.* use a Markov chain process to find the important microgrid operation states and adopted the Monte Carlo simulation to assess the risk of adverse effects on the microgrid when PV and ESS devices are hacked. The microgrid at Illinois Institute of Technology is chosen by Liu *et al.* as an example microgrid model on which to apply their proposed risk assessment method. This microgrid includes solar, wind, and gas energy sources as well as ESSs. It also makes use of actual ABB inverter products. To perform their experiments on Markov-based techniques, Liu *et al.* use the MATLAB-based Stateflow toolbox

to simulate dynamic cyberattacks and the internal state of the PV and ESS resources. Liu *et al.* acknowledge that microgrids are complex systems to analyze, but nevertheless claim that their proposed risk assessment method can be effective at evaluating cybersecurity risk in the microgrid **[45]**.

3.2.2 Cybersecurity Approaches

This section describes the proposals made in the state of the art on ways in which the cybersecurity of the microgrid, as well as other power grid systems like the electrical substation, can be enhanced to defend against cyberattacks. The approaches employed by the proposed solutions fall within the categories of applying cryptography to protect communications, enhancing network resiliency, detecting intrusions with rule-based, and detecting anomalies using machine learning models. The classification of related proposals, based on their cybersecurity approach, is given in Figure 3.5.

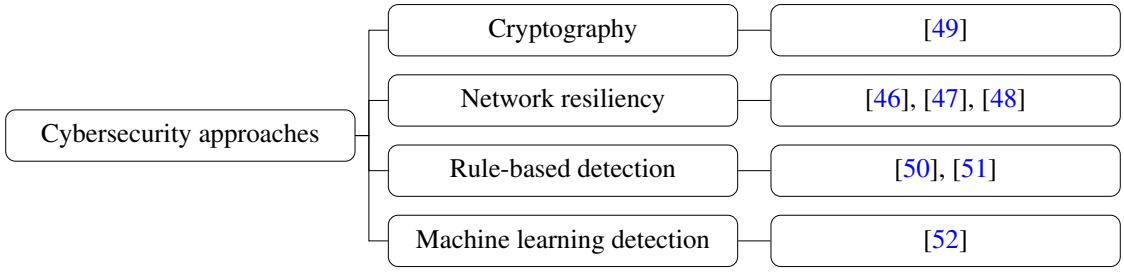

Figure 3.5: Cybersecurity solutions

3.2.2.1 Cryptography

Through the application of cryptography, the effectiveness of certain cyberattacks can be greatly reduced. Cryptography utilizes mathematical constructs to protect the integrity, authenticity, and confidentiality of information. However, it may not be necessary to protect these three things at one. In the microgrid, cryptography may be used to prevent digital messages modified by an attacker from being accepted or to prevent a message forged by an attacker from being considered legitimate.

Kounev *et al.* **[49]** propose a communication architecture designed to support the security of the microgrid transition from islanded mode to grid-connected mode. The proposed secure communication scheme has a hierarchical security structure that meets the real-time requirements of the

microgrid. It is designed to protect sampled data, safety messages, and control messages transmitted over IEC 61850 protocols. Kounev *et al.* claim that the recommendation of the IEC 62351 standard to hash time-critical messages using SHA-256, then sign the hashes with an RSA private key, fails to meet the three-millisecond end-to-end delivery requirement specified by IEC 61850. They claim that, because of the time delivery issue, the recommendation has little industry acceptance. In its place, Kounev *et al.* propose that microgrid control messages be protected with an encrypt-then-MAC scheme that has an authentication tag created from the encrypted message. They recommend the use of the AES-CMAC-96 Message Authentication Code (MAC) algorithm with truncated 96-bit output for protected messages and with the encryption keys shared in advance. Kounev *et al.* assume an attacker model with full access to the microgrid communication network links and with the capability to modify the network traffic in any way. This attacker model motivates Kounev *et al.* to design their secure communication scheme so that it provides full end-to-end security. The proposed scheme is tested on a co-simulation testbed. The results of experiments run on this testbed show that the proposed scheme is able to meet the three-millisecond requirement. However, Kounev *et al.* note that the end-to-end delay increases linearly with the number of multicast receivers **[49]**.

3.2.2.2 Network Resiliency

One strategy that can be utilized to mitigate cybersecurity threats is to adopt a system design that is resilient. A resilient system is defined as one that can recover from a change in part of the system such that it resumes operating as it did before the change. From a cybersecurity perspective, this means the system can, to some extent, perform corrective action or reconfigurations to reverse the impacts of a cyberattack. In the case of the microgrid, such resiliency can be present within the communication network itself or within the power system that may choose to become autonomous.

Jin *et al.* **[46]** propose a novel Software-defined Network (SDN) tool named DSSnet, which can be used as a means to make the microgrid more resilient to both inadvertent and deliberate cyber threats. The proposed software-defined network tool separates network control functions from forwarding functions and delegates the task of configuration management for the network to centralized controllers. DSSnet provides self-healing capabilities for the microgrid communication network through dynamic/programmable SDN configuration, and supported by global visibility of

the network. It allows for isolation of suspicious or malfunctioning devices from the rest of the network through reconfiguration of routes on switches. The global visibility of the network allows the use of Dijkstra's shortest paths algorithm to determine the proper reconfiguration for the network more efficiently than spanning tree protocols. Jin *et al.* use a campus microgrid at Illinois Institute of Technology for running experiments with DSSnet. These experiments demonstrate results that suggest SDN can improve the resilience of the microgrid to cybersecurity threats **[46]**.

Chlela *et al.* **[47]** highlight the threat of DoS attacks against DERs in islanded microgrids relying on information and communication technologies, and propose a rule-based fallback control strategy to mitigate this threat. They explain that DoS attacks against an isochronous ESS, which prevent the IED controlling the ESS from communicating with the central Energy Management System (EMS), can lead to adverse physical effects on the microgrid. Should the ESS IED lose contact with the EMS, the fallback control strategy proposed by Chlela *et al.* makes use of decentralized algorithmic control on the energy delivery and absorption of the ESS such that the frequency of the microgrid is kept within reasonable limits. The remaining DERs in the microgrid have control loops that respond accordingly to the control actions taken to mitigate the attack against the ESS. To demonstrate the effectiveness of the proposed strategy, Chlela *et al.* built a real-time HIL microgrid testbed which simulates an ESS, a wind turbine generator, and a synchronous generator. The attack scenario launched against this testbed has an ESS IED, which communicate with IEC 61850 protocols, becoming infected by malware through a network intrusion similar to the cyber attack launched against the Ukrainian power grid on December 2015. The malware then performs DoS against the infected ESS. According to Chlela *et al.*, the results of their experiments demonstrate that the proposed fallback strategy ensures reliable power supply to the loads during an attack compared to when it is not used **[47]**. However, they do not consider attack scenarios where attacks can inject fabricated control messages into the network.

Chalamasetty *et al.* **[48]** present a SCADA model that uses mobile ad hoc networks as part of an intrusion detection and prevention system for residential microgrid communication networks against black hole attacks. The model also defends against attacks that involve the dropping of message packets. They propose the use of a secure knowledge algorithm, where nodes share information about their recently forwarded packets and neighbouring nodes, to identify black hole nodes in the

network. If the information shared between nodes is not the same, then that is an indication of a black hole being present in the network. Once detected, the network determines new routes to use for network traffic flow that do not pass through the black hole node. Chalamasetty *et al.* determine that finding new routes to avoid detected black holes when there were more than 40 nodes in the network is effective. In small network of only about 10 nodes, it is much harder to find new routes that do not pass through a black hole. The black hole detection method that Chalamasetty *et al.* propose made use of a peer-to-peer algorithm rather than a centralized or local detection approach **[48]**.

3.2.2.3 Rule-based Detection

One strategy for detecting attacks is to define a set of rules that are expected to be followed by system should it be operating when cybersecurity threats are not present. Rule-based detection relies on the elaboration of rules whose violation is a strong indicator that an attack on the system is in progress. Naturally, the use of rule-based detection in the microgrid should make use of rules that are designed for the microgrid.

Yang *et al.* **[50]** propose a stateful IDS for IEC 104 protocol traffic that uses Deep Packet Inspection (DPI) to determine if IEC 104 packets passing through the network contain malicious payload. They highlight the cybersecurity threat posed by IEC 104 messages being sent in clear text without integrity checks in place. Yang *et al.* consider the threat of an attacker that sends a small number of modified and injected IEC 104 packets into the network. The proposed IDS makes use of a whitelist of acceptable behaviour for IEC 104 packets, identifying packets that are not found in the whitelist as being abnormal. The IDS applies the concept of the finite state machine to create a detection state machine specific to the IDS. This detection state machine is built using the Internet Traffic and Content Analysis (ITACA) tool. Yang *et al.* also evaluate the effectiveness of the IDS by mixing normal IEC 104 traffic acquired from real commercial sources with modified and injected packets, then having the combined set of packets read by the IDS. The tested dataset includes a total of 116,469 normal packets and 28 abnormal packets. The experiments performed by Yang *et al.* show that the IDS is able to detect the abnormal packets without having any false positives or false negatives **[50]**. The use of DPI allows the proposed IDS to identify message tampering and protocol misuse, but is less suitable for detecting attacks based on changing the rate of traffic.

Li *et al.* [51] experimented with the use of an active synchronous detection method to detect injection and modification attacks on microgrid inverter controllers in real time. They explain that inverter controllers perform many vital microgrid operations such as voltage regulation. They also describe how false data injection attacks against these controllers can be detrimental to the operation of the microgrid. The active synchronous detection method proposed by Li *et al.* generates small probing signals periodically to different targets across the microgrid and compares the responses to the probing signals by the targets to see if they are within expectations. The probing signals and detection rules are constantly being adjusted, making it harder for attackers to adapt to the signals. Li *et al.* tested the proposed detection method on a microgrid with three PV units, three batteries, and two microturbines. The results of the tests suggest that their proposed active synchronous detection method can distinguish normal traffic from attack traffic, and can detect the type and origin of attacks. Li *et al.* also find that the probing signals and their adjustments do not impede microgrid operations in any significant way, making it compatible with more complex microgrid control systems [51].

3.2.2.4 Machine Learning Detection

Machine learning techniques can be used to model system behaviour under normal conditions and to categorize different attacks. Machine learning models are trained to detect anomalies by being provided with a suitably large sample of data from the target system, then comparing live data to a system mode derived from processing the training data. The digital communications within the microgrid are expected to maintain fairly consistent behaviour, making machine learning models suitable for detecting anomalous behaviours.

Inoue *et al.* [52] investigate the effectiveness of unsupervised machine learning for anomaly detection in a cyber-physical system, specifically the Secure Water Treatment (SWaT) system. According to Inoue *et al.*, one of the main advantages of using machine learning techniques is that it does not require a deep understanding of the targeted cyber-physical system. The SWaT testbed used for experiments by Inoue *et al.* was built at the Singapore University of Technology and Design (SUTD) for cybersecurity research. To perform tests on machine learning anomaly detection in cyber-physical systems, Inoue *et al.* collected log data from the SWaT that spanned over seven

days of continuous normal operation and four days of continuous operation when subject to 36 different network attack scenarios. The attack scenarios involved the interception and modification of data packets travelling to the Programmable Logic Controllers (PLCs), pumps, and valves in the SWaT. These modifications are capable of causing physical damage in the SWaT. Inoue *et al.* subject the log data to a Deep Neural Network (DNN) that uses Long Short-term Memory (LSTM) and to a one-class Single Vector Machine (SVM). Their experimental results show that, while the DNN has fewer false positives, the one-class SVM had fewer false negatives. Both methods have difficulty detecting gradual anomalous change of sensor values or anomalous actuator movements. They however note the large difference in precomputation needed for the two tested machine learning methods, with the DNN requiring training in the order of weeks while the one-class SVM could be trained in around 30 minutes. Inoue *et al.* point to the validity of their results being challenged by having only tested the machine learning methods on the SWaT. They note that their research can be extended by considering controller logic and by extending the comparison of machine learning techniques beyond just DNN and SVM **[52]**.

3.3 Microgrid Testbeds

This section describes existing experimental microgrid testbeds built for use in research towards understanding the effect of microgrid operations on the power system. They have also been used to demonstrate the effectiveness of mitigation strategies against cyberattacks.

3.3.1 Digital Testbeds

The microgrid testbeds discussed in this section are labeled as digital testbeds due to their exclusive use of software tools to model microgrid behaviour. Examples of experimentation where digital testbeds are suitable include the evaluation of different microgrid communication network conditions and the evaluation of microgrid control algorithms.

Islam and Lee **[17]** developed a microgrid simulation testbed in order to evaluate potential microgrid communication networks that map information for microgrid operations onto IEC 61850

protocols. They use OPNET modeller to built a simulation model that consists of multiple networked microgrid agents. The testbed is used to simulate digital traffic between agents across the microgrid communication network. Among the agents are measurement IEDs, circuit breaker IEDs, and P&C IEDs, and the microgrid control centre. The OPNET modeller allows for the simulated network load of each agent to be configured. Islam and Lee identify the network agents as being the largest users of the communication network, with each measurement agent transmitting 500 KB/s while the other agents generate 60 KB/s. They designed an communication network integrating both wired and wireless links. Wired links are used between local agents, with 10 Mbps, 100 Mbps, and 1000 Mbps optical fiber links being available for them. The wireless communication in the simulation is configured to use WiMAX. The testbed built by Islam and Lee in OPNET modeller was able to demonstrate the capability of a microgrid communication network using IEC 61850 protocols to meet the strict timing requirements of the IEC 61850 protocols **[17]**. The testbed used by Islam and Lee does not seem to include any real microgrid monitoring and control hardware devices. Also, the topic of microgrid cybersecurity was not part of their scope. However, there is potential to determine the input required by an attacker to achieve DoS using a similar microgrid simulation model.

Ahamed *et al.* **[53]** use simulation software to study the use of energy management and control of a DC-microgrid composed of batteries and PV arrays. As motivation for studying the DC-microgrid over the AC-microgrid, they state the advantage of DC-microgrids requiring fewer AC-DC interfaces for consumer loads such as laptops and electrical lighting. They highlight the importance of energy management and control for DC-microgrids with renewable energy sources. In particular, energy management and control is relied upon for the control of PV generation, battery charging and discharging, and DC-DC converters. Ahamed *et al.* make use of simulation software to simulate a DC-microgrid to demonstrate the usage of management and control on a DC-microgrid system. They use the PSCAD/EMTDC software to simulate a DC-microgrid operating in islanded mode with a PV array and a battery. While the battery and PV array are simulated by PSCAD/EMTDC, the input provided to the PV array is taken from real measurements of solar radiation during a sunny day between 7:00am and 5:00pm. Ahamed *et al.* studied three scenarios: the battery reaches its maximum charge, an additional load is connected, and the battery reaches its

minimum charge. In the case of the battery reaching its minimum charge, load shedding is required to maintain the appropriate DC-link voltage. Their results demonstrate the proper functionality of the energy management and control designed for the target DC-microgrid. However, the work of Ahamed *et al.* leaves room for expansion through the incorporation of different DG sources such as wind turbines, super capacitors, and diesel engines. In addition, the work does not present the use of digital communications to perform the modelled energy management and control operations. Nevertheless, the simulation capabilities presented by Ahamed *et al.* are suitable for testing a variety of power system scenarios **[53]**.

3.3.2 Hardware in the Loop Testbeds

The microgrid testbeds discussed in this section are referred to as HIL testbeds due to their integration of hardware components, such as real IEDs, when running experimental tests. The software tools used in digital testbeds may also be used in HIL testbeds. The realism of a testbed microgrid model being studied may be enhanced by the integration of IEDs used in the microgrid within the HIL testbed. However, there is an added cost to the construction of the microgrid model when acquiring IEDs and other hardware.

Xiao *et al.* **[54]** describe the HIL microgrid testbed developed for experiments on microgrid operation and control. This microgrid testbed consists of a DRTS for simulation of microgrid power and control systems and deploys a Microgrid Energy Management System (MicroEMS) built in MATLAB. Connected to the DRTS are several physical NI CompactRIO IEDs as well as a relay protection system supported by 351S programmable digital relays. The architecture of the microgrid simulated by Xiao *et al.* in the HIL testbed is based on the Distributed Energy Communications and Controls (DECC) microgrid at Oak Ridge National Laboratory **[56]**. The simulated microgrid has a three-phase AC main bus connecting several simulated energy sources, a load, and a simulated main grid. The simulated energy sources include one PV array, two batteries, and a synchronous machine. A DC/AC bidirectional inverter is used to convert the DC electricity produced from the PV array and batteries into AC. Real hardware is connected to the DRTS to provide the microgrid operation and control functions as well as the relay protection functions. As for digital communication, UDP is used for communication between the DRTS and the real devices in order to perform device level

control. Xiao *et al.* separate the microgrid control responsibilities into three levels: device level, microgrid communication and control level, and grid level. They designed the MicroEMS to work towards optimizing the microgrid power generation while the microgrid is in grid-connected mode and towards grid stability when in islanded mode. The experiments performed by Xiao *et al.* on this testbed relating to microgrid operation and control include testing of controllers in the device level, testing the MicroEMS, and testing the relay protection system. The testbed allows for replacing the microgrid controllers in order to test other control schemes **[54]**. Xiao *et al.* do not discuss the topic of microgrid cybersecurity when describing their microgrid testbed, but the use of real equipment and communications offers the potential to explore the behaviour of the simulated microgrid in the presence of cybersecurity threats.

Liu *et al.* **[55]** describe the experimental platform developed at the Smart Microgrid and Renewable Technology laboratory upon which microgrid HIL simulation testbeds can be built. This experimental platform is intended to be used for both teaching and research purposes, particularly for the study of power electronics. Of particular interest are the challenges of elaborating fast optimization algorithms for energy management and high-performance control algorithms for power electronics. Liu *et al.* believe that addressing these challenges requires multi-disciplinary expertise, which their experimental platform attempts to capture. The experimental platform consists of one ORAL-RT DRTS, two one-bus microgrid testbeds, one modular multilevel converter, one cascaded multilevel converter, and one multi-agent system for microgrid control. Liu *et al.* make use of MATLAB and Simulink to implement modeling and algorithms. One of the one-bus microgrid testbeds can be used to study shipboard power system and renewable microgrids and simulates one PV array, one wind turbine generator, and one energy storage system. The other microgrid testbed is designed to be easier to reconfigure and can simulate 1-phase, 3-phase, and DC microgrids with a connection to a simulated main grid through a static switch. Examples of simulations that can be run on these testbeds according to Liu *et al.* include controller HIL simulations, power HIL simulations, cascaded PV system simulations, and parallel uninterrupted power supply system simulations **[55]**. While not the focus of their work, Liu *et al.* claim that the configuration options of the multi-agent system allow for testing of cybersecurity solutions using the experimental platform

Chlela *et al.* **[47]** built a real-time HIL microgrid testbed in order to demonstrate the effective of

their proposed fallback control strategy against DoS attacks. This testbed uses an OPAL-RT DRTS to model the microgrid, including its DERs and loads. The testbed microgrid itself is configured as a 25 kV microgrid connected to a distribution system. Chlela *et al.* deploy an NI-cRIO digital controller to act as the energy management system for the testbed. The tested microgrid architecture consists of a wind turbine generator, an ESS, and a dispatchable generator which could be configured as being thermal or diesel depending on the desired experimental setup. When using the thermal generator, the microgrid has full inverter interface control for its DERs and loads. The testbed connects real IEDs, which communicate to the central energy management system using IEC 61850 protocols, to the DRTS in order to control the DERs. The wind speed profile is made to be categorized by the Kaimal power spectral density in order to simulate the wind behaviour for the wind turbine generator. Chlela *et al.* use this testbed to validate their proposed fallback control strategy against cybersecurity threats. The use of HIL makes the study of cybersecurity solutions on this testbed particularly interesting.

3.4 Conclusion

In this chapter, a review of related work on the topics of microgrid power networks, communication networks, and cybersecurity is presented. Related work on power networks describe the different architectures that have been used to built real microgrids. They also explain the role and importance of control operations in the power network. Work on communications networks highlight the importance of digital communication in maintaining proper microgrid operation, and discuss the different technologies used to enable these communications.

A review is also presented for related work that studies the impact of cyberattacks against the microgrid. The studies discuss the vulnerability of the microgrid to cybersecurity threats such as DDoS and MitM. In particular, attacks against the integrity of microgrid control communications were found to be very dangerous to the health of the microgrid. Proposed solutions to microgrid cybersecurity issues are presented as well. Different approaches for improving microgrid cybersecurity are discussed. Among them are DPI, network monitoring, and fallback control schemes. In addition, existing microgrid testbeds are also reviewed.

This chapter presented related work on the topic of microgrid systems in order to guide the design of the microgrid model studied in this research. As for the related work on microgrid cybersecurity topics, many of the cyberattacks that the NSM security platform designed in this research aims to detect are also considered in previous research. However, the tools and techniques used by the NSM platform, in particular its adherence to IEC 62351-7, are novel. The details of the proposed NSM platform design is the next important topic to be discussed, along with the steps being followed to evaluate its effectiveness.

Chapter 4

Design of NSM and Attack Scenarios

4.1 Overview

A core element of this research is the design and implementation of an NSM platform that adds network monitoring to the microgrid for security and maintenance purposes. The design and implementation of the proposed NSM platform is part of a joint research with Ms. Chantale Robillard, who proposed the use of NSM to protect IEC 61850 digital substations [57]. The NSM platform aims to add intrusion detection capabilities within the microgrid network as well as detection of performance issues within the network. This is achieved through the deployment of NSM agents across the microgrid network that collect data useful for microgrid NSM and having these agents transmit the collected NSM data to a central NSM manager. The manager makes use of the data it receives from agents for monitoring the health of the network and the detection of cyber-physical threats to the microgrid.

The overall design of the NSM platform uses a centralized architecture, with a central NSM manager requesting and receiving status updates from NSM agents deployed on monitored IEDs, with each IED being monitored by their respective NSM agent. An NSM agent only communicates with the device that it monitors and with the NSM manager to which the agent reports the monitored device data. The centralized architecture is chosen because of its simplicity, and it is compatible with the NSM platform design that does not have the NSM agents communicate among themselves.

The information transmitted to the NSM manager by the agents is structured in the data objects

defined in IEC 62351-7 [34]. The NSM manager aggregates the received data objects and processes the data to determine if it suggests anomalous behaviour in the network. The anomaly detection method used in this research uses a hybrid approach consisting of both rule-based detection and machine learning detection techniques.

This chapter presents relevant concepts related to the core components and tools of the end-to-end design for the proposed NSM platform. These components include the NSM agent, the NSM manager, and the anomaly detection techniques used to label anomalous behaviour in the microgrid network based on the data collected through NSM. This chapter also gives details on the IEC 60870-5-104 (IEC 104) protocol in use within the microgrid system being considered and gives some details on the data being monitored by the NSM platform.

4.2 NSM Agent

NSM agents are responsible for reporting on the health of monitored IEDs in the microgrid network, such as circuit breakers and protective relays. They are also responsible for reporting events that have taken place within the IEDs. The types of IED information reported by NSM agents include performance measures, network traffic statistics, device health, and configuration.

Each NSM agent is associated with one monitored IED whose state is reported to the NSM manager by that agent. To this end, the IED needs to have the relevant information somehow accessible to the NSM agent. How the relevant information is made accessible to the agent depends on how the agent is installed. If the NSM agent functionality is provided by software installed within the monitored IED, then the information to report can be accessed directly by the agent. If the agent is installed on a separate device, then the monitored IED must have a way to make the information to report accessible externally. In this case, the agent is considered to be a proxy device. Ways that the IED can expose needed information to an NSM agent installed on a proxy device include the publishing of logs that are accessible to the agent, allowing the agent to access the IED remotely, or having the traffic flowing into and out of the IED be observable by the agent.

Currently, direct support for IEC 62351-7 NSM data objects within vendor equipment is very minimal. During this research, commercial IEDs did not yet map IEC 62351-7 NSM data objects

to the internal data that they expose. Because of this, custom NSM agents are used to perform this mapping instead. These custom agents are deployed on proxy machines positioned between IEDs and the NSM manager. The custom agents need not be identical. They can use different configurations depending on the data that must be collected from the specific vendor device that the agent monitors and the mechanisms through which the vendor device exposes its internal data.

The NSM agent collects and stores data to be reported to the NSM manager over a digital communication network in near real-time. The main source of delay between when the NSM manager requests data from the NSM agent and when the manager receives the data response is the network delay. Network delay is present in the digital communication network when messages are relayed from the manager to the agent and vice versa. The agent may collect the information to report upon request of that information by the NSM manager. Alternatively, it may constantly update a stored value to report based on the results of a repeating sequence of operations. For example, the agent may periodically record the average amount of data traffic received by the monitored IED, transmitting the most recent average to the manager upon request.

The NSM platform has the NSM manager poll the NSM agents over regular intervals for the data values set by the agent, based on the state of the monitored IED, to be later analyzed by the manager. Alternatively, the agent can notify the manager of a key security event regarding the monitored IED without being polled.

The data collected by the NSM agents in the proposed NSM platform is chosen and structured in accordance with the NSM data objects specified in IEC 62351-7 **[34]**. The data objects used for the NSM platform designed as part of this research are briefly discussed in Section **4.7**.

NSM agents do not report data to other NSM agents in the network. The intent of this design is to keep the NSM agents lightweight while having threat detection logic centralized in one network node. In the case of the proposed NSM platform, the detection logic lies within the manager. There are also no nodes in the network that can switch between acting as an NSM agent and as an NSM manager. The presence of such nodes would facilitate a hierarchical architecture for the NSM platform, but the network on which the NSM platform is tested was not considered to be large enough to warrant the added complexity of having nodes that can act as both an NSM agent and an NSM manager.

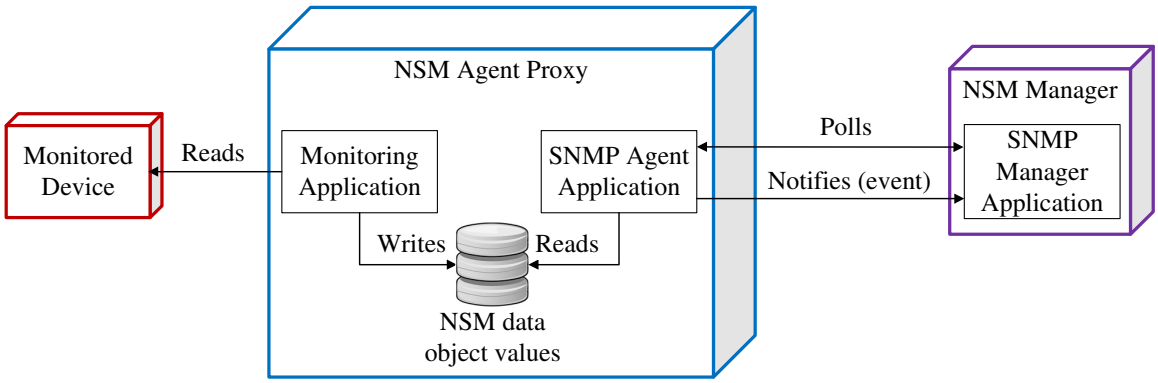

Figure 4.1: Setup of NSM agent proxy

4.3 NSM Manager

The NSM manager is responsible for collecting the raw NSM data object values from the NSM agents distributed across the network and aggregating the data into a representation of the network state as a whole. The manager persists the state of the network at different times so that changes to the network over time can be observed and analyzed.

The NSM manager periodically polls each NSM agent for the set of NSM data object values that the agent can provide. The manager then aggregates the updated data object values into a single snapshot dataset instance that approximates the microgrid state at a single moment in time. The snapshots of aggregate NSM data, sorted by time, are saved and processed by the anomaly detection module to observe the changes to data objects values or sets of values over time, comparing them to expected behaviour. Should an anomaly be found, an alert is generated and saved so that they may be viewed by a human operator. The alerts are made accessible from a web server so that a human operator may view the alerts through a web client over HTTPS.

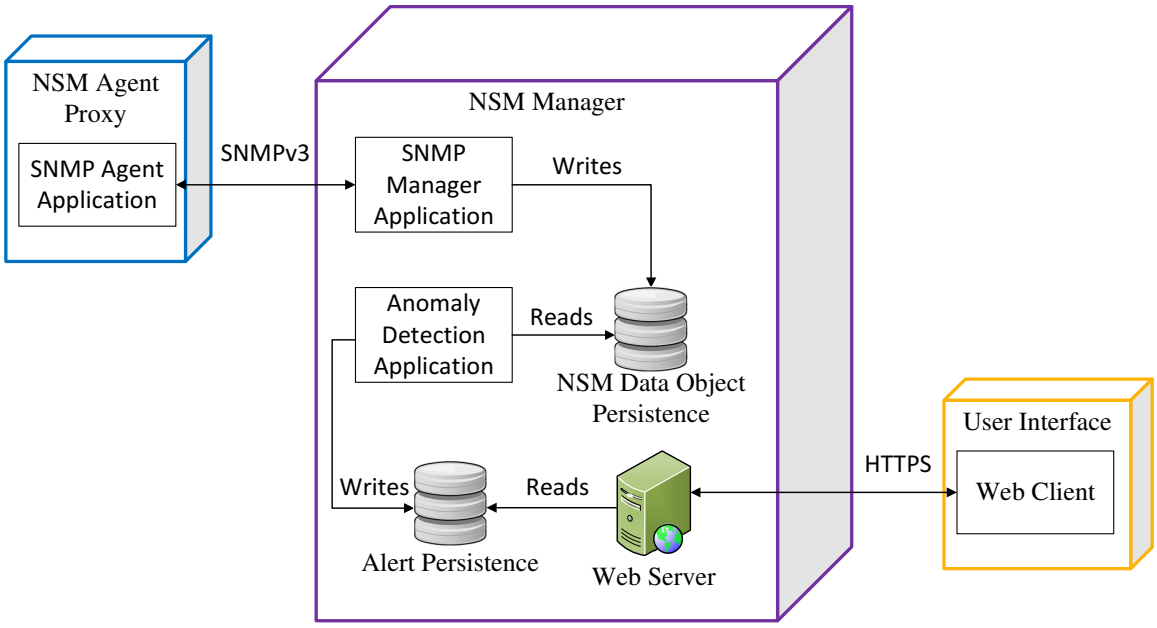

Figure 4.2: Setup of NSM manager

4.4 Communication Network Topology

The NSM manager is located in a network node that is separate from the rest of the microgrid. The NSM manager acts as the centre of the NSM platform, having communication channels to all NSM agents in the network. The NSM platform has a star architecture, where the NSM manager can communicate with all NSM agents without having the communication depend on any other NSM agents relaying messages in between. The role of the NSM manager involves observing the microgrid as a complete system. As such, it was deemed appropriate to deploy the NSM manager at the centre of a star topology so as to minimize the maximum distance between the NSM manager and any one NSM agent. The manager is expected to be manually kept up to date in regards to the agents currently installed in the network in order to access them. The network of monitored IEDs in the microgrid is expected to be relatively static, so updating the manager with a new topology of the microgrid network is not expected to be required very often.

4.5 Anomaly Detection Module

The anomaly detection module consists of an application that combines rule-based detection with machine learning to detect anomalies within the snapshots of the microgrid network state aggregated by the NSM manager. The rule-based detection component sets certain conditions relating to the NSM data objects that generate an alert when met. For example, rules can be set to generate an alert if an NSM data object relating to errors in network packets indicates that an error packet has been received. The machine learning component uses Long Short-term Memory (LSTM) **[58]** to build a prediction model by observing the values of the NSM data objects under normal microgrid operation. The LSTM-based component of the anomaly detection compares the NSM data object values being collected by the NSM manager to what is expected based on the prediction model. The module generates an alert if there is a discrepancy that crosses a set threshold.

The anomaly detection module is part of a joint work and was build through collaboration with Dr. Rachid Hadjidj, Mr. Abdullah Albarakati, and Ms. Chantale Robillard.

4.6 Details on IEC 60870-5-104 protocol

The primary digital communication protocol in the microgrid that is being studied as part of this research is the IEC 104 telecontrol protocol. It is therefore important that the usage and behaviour of this protocol is well-understood.

The IEC 60870-5-104 (IEC 104) protocol is used for sending telecontrol messages over TCP between a master station and an outstation. In this context, "telecontrol" is described as the remote transmission of supervisory actions and data acquisition requests using electrical signals in order to control the power transmission grid **[24]**. The master station acts as a central control station responsible for the monitoring and control of one or more outstations.

The IEC 60870-5-104 protocol uses the telecontrol communication profile defined in the IEC 60870-5-101 companion standard for communications between master stations and outstations, but extends it to have IEC 60870-5-101 messages transmitted using TCP/IP profiles for such communications. The telecontrol profile described in IEC 60870-5-101 is itself founded on top of the IEC

60870-5 standard protocol stack. The IEC 60870-5 protocol stack is based on a reference model known as the Enhanced Performance Architecture. This architecture consists of an application layer, data-link layer, and a physical layer that correspond to layers 7, 2, and 1 of the ISO Open System Interconnection (OSI) model respectively **[24]**.

The monitoring and control messages sent over IEC 104 are structured as APDUs. Each APDU has an Application Protocol Control Information (APCI), and also has an ASDU if the APDU contains a data payload or a control command. The data payload in the ASDU contains one or more information objects. These information objects hold data elements that each correspond to a particular value being monitored.

The APCI is generally six 8-bit bytes in size. It contains the IEC 104 protocol header byte (`0x68`), followed by the length of the APDU in bytes and then four control field bytes. The ASDU has a six byte data unit identifier that includes the following:

- The type of data contained in the ASDU
- The number of data elements
- The number of information objects in the ASDU alongside a flag that specifies the format of the information object addressing in the ASDU
- The Cause of Transmission (COT) field that provides a reason for why the APDU was transmitted
- The address fields for the master and outstation, and
- The flag that indicates if the APDU was only sent for test purposes.

The rest of the ASDU contains a list of information objects, with each information object having an Information Object Address (IOA) and a data element holding a value. All information object data elements within the same ASDU must have the same data type. A single TCP segment may carry more than one APDU. This can occur when IEC 104 messages carrying different data types or have different COT are being sent at around the same time. Figure 4.3 depicts the structure of the ASDU that is sent over TCP for communications using the IEC 104 protocol.

According to Part 5 of IEC 62351, the IEC 104 APDU that directly cause output at the destination, such as APDU which are intended to cause parameter changes at the destination, are considered to be "critical" APDUs [22]. The COT field can be used to help distinguish critical APDUs from non-critical ones. For example, the `ACT` value of the COT field is an indication that the APDU is meant to elicit an action at the destination.

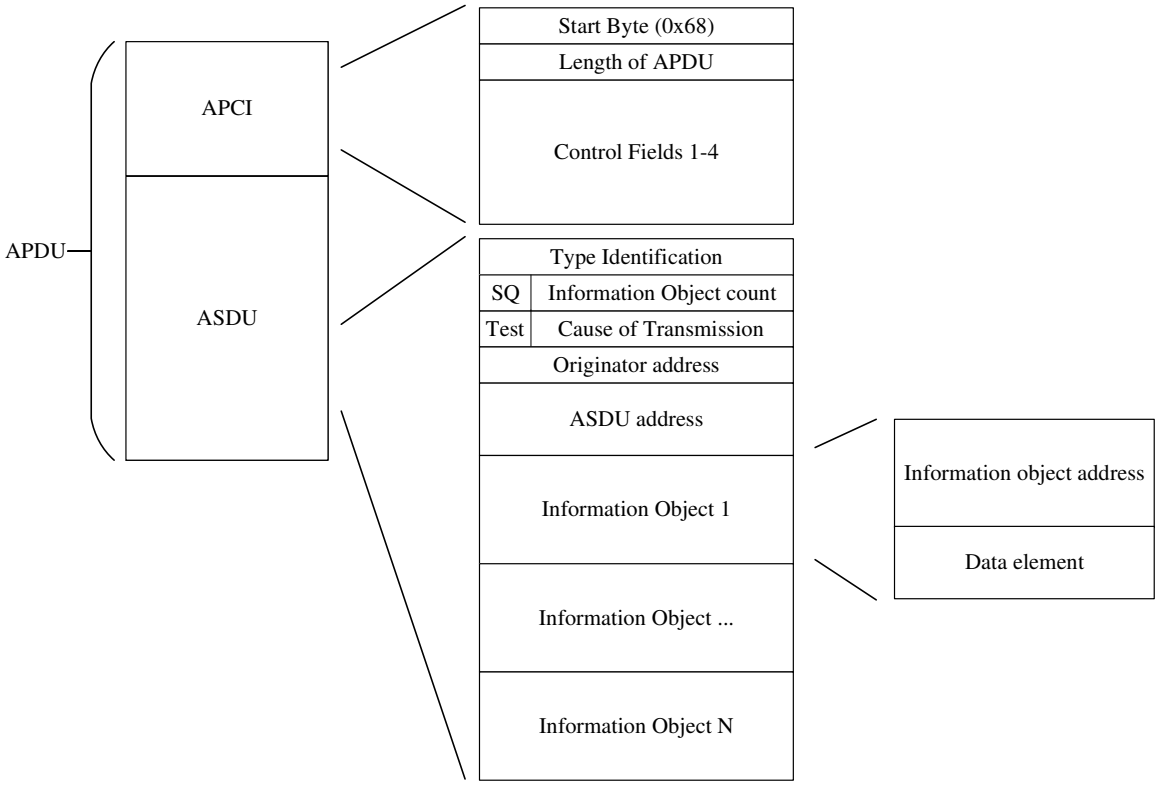

Figure 4.3: Structure of IEC 60870-5-104 APDU

The APCI has three different formats: the I-format, the S-format, and the U-format. The I-format APCIs are used for the transfer of monitoring or control information between the master station and the outstation. The I-format uses the four control field bytes for sequence numbers, with separate sequence numbers being maintained for outgoing messages and for incoming messages. The I-format is the only frame format that includes an ASDU. The S-format is used for

the acknowledgment of longer APDU chains. The S-format uses the control fields to send a sequence number that acts as an acknowledgment that the sender of the S-format frame received all messages with sequence numbers lower than the number given in the S-format frame. The sending of these S-format messages is necessary when communications are only taking place in one direction for an extended period of time. IEC 104 devices may have a timeout or maximum number of unacknowledged I-format messages configured that prevent the devices from sending additional I-format messages if the timeout or maximum permitted number is exceeded before receiving an S-format APCI confirmation message. The U-format APCI has a fixed length and does not have a corresponding ASDU. It is used for sending command messages that are concerned solely with the IEC 104 connection between the communicating parties.

The APCI control fields are used for different purposes depending on the format of the APCI. For the I-format frame, the control fields hold sequence numbers assigned to each ASDU. Both the master station and the outstation maintain two independent sequence numbers. One sequence number, Rx, is incremented every time the station receives an ASDU from the station with which the IEC 104 connection was made. The other sequence number, Tx, is incremented every time the station transmits an ASDU to the station that is part of the IEC 104 connection. Each I-format APDU frame includes both the Rx and Tx sequence numbers of the station that transmitted it. The Rx and Tx sequence numbers are reset at the start of every new IEC 104 connection. The S-format APDU frame uses to APCI control fields to transmit the value of just the Rx sequence number of the station transmitting the S-format frame. This Rx value is used to confirm the number of messages that the sender has read from the receiver. The Rx value in the S-format frame will be equal to the Tx value that the receiver will provide in the next I-format frame it transmits if all previous ASDUs it transmitted were received by the sender of the S-format frame. For the U-format frame, the control fields are used to identify the command given by the U-format frame. The U-format control fields can have the value representing the Test Frame (`TESTFR`), Start Data Transfer (`STARTDT`), or Stop Data Transfer (`STOPDT`) commands. The U-format frame can also carry a `STARTDT_con` message to confirm a `STARTDT` command.

An I-format APDUs will have an `Act` cause of transmission if the message in the APDU is intended to enact a change of settings at the destination station. The station receiving the Act APDU

responds with a `ActCon` I-format APDU with the same information object values to confirm that the station received the `Act` APDU and took appropriate actions based on its contents.

4.7 Applicable Network and System Management Data Objects

The IEC 62351-7 standard defines NSM data objects that are grouped across several packages as described in Section 2.5.4. Several of the packages defined in IEC 62351-7 contain objects that can be monitored by the proposed NSM platform developed for this research. The choice of NSM data objects to monitor is based on their potential in helping identify anomalies and intrusions as well as the practicality of monitoring the system element that corresponds to the object.

4.7.1 Monitored IEC 62351-7:2017 Data Objects

A summary of the subset of NSM data objects defined in IEC 62351-7 that can be monitored by the proposed NSM platform on each monitored device is given below.

- **Monitoring of Environment Data Objects**

  The NSM platform monitors the Environment data objects that indicate when direct access to an IEDs has occurred.

- **Monitoring of IED Data Objects**

  The NSM platform monitors IED data objects that are related to the physical health of the IED. This includes the device's memory usage, total available memory, maximum and remaining storage, current CPU usage, number of detected warm starts that were initiated, and number of watchdog timer interventions. The NSM platform also monitors IED data objects related to security issues in the IED. This includes the number of expired and nearly expired local certificates, the number of detected service privilege violations, the number of missed events, the current RBAC database version, the current configuration version, and the current firmware version.

- **Monitoring of Interfaces Data Objects**

The NSM platform monitors the Interfaces data objects that provide a count for the number of active, installed, and failing Ethernet interfaces on an IED.

- **Monitoring of IEEE 1815 and IEC 60870-5-104 Data Objects**

  The NSM platform monitors the data objects that pertain to the statistics of transmitted and received network traffic for the IEEE 1815 DNP3 and IEC 104 protocols. The monitored statistics concern the number of different kinds of PDUs observed. The statistics consider the count of PDUs transmitted, retransmitted, and received. They also consider the count of critical PDUs, the count of PDUs in error, and the count of PDUs having the wrong size. Additionally, the DNP3 protocol distinguishes PDU as being either solicited or unsolicited, with the count of each being monitored by NSM. The IEC 104 protocol however does not distinguish between solicited and unsolicited traffic. The PDU round trip time and the time between two consecutive PDUs that have been received are also monitored.

- **Monitoring of IEC 61850 Data Objects**

  The NSM platform monitors data objects that are tied to the subscribers and publishers of the IEC 61850 GOOSE and SV protocols. For GOOSE, the rate of transmitted PDUs per second and of received PDUs per second are monitored. In addition, the number of occurrences for several unusual events is counted. This includes the number of PDUs with an incorrect configuration revision number, PDUs indicating that the subscriber needs commissioning, PDUs with a Time Allowed to Live (TAL) that has expired, and PDUs that were received in error. For SV, the rate of transmitted PDUs and received PDUs are monitored.

- **Monitoring of Clock Data Objects**

  The NSM platform monitors data objects that report on the clock synchronization method being used by the clock and that report whether the clock is receiving a signal from a recognized standard time source.

4.7.2 Monitored TCP and UDP Data Objects

The data objects defined in IEC 62351-7 are not the only network elements monitored by the NSM platform. Statistics related to TCP and UDP network traffic are also collected. For TCP, the monitored statistics include the number of received TCP segments, the number of transmitted TCP segments, the number of TCP retransmissions, the number of TCP resets, the number of TCP segments received in error, and the number of opened TCP connections. For UDP, the monitored statistics include the number of received UDP datagrams, the number of transmitted datagrams, the number of received UDP datagrams with no application at the destination port, and the number of UDP datagrams received in error. There are also data objects that expose the available TCP and UDP ports on each device.

4.8 Comparison of Collected Data Objects with Required NSM Data Objects

The IEC 62351-7 standard defines many data objects to be used for supporting the intrusion detection capabilities of NSM. The defined data objects are designed to meet the security requirements specified by IEC 62351-7 for the detection of intrusions. The data object requirements given by the standard are summarized in Section 2.5.3.

The NSM platform designed in this research does not implement every NSM data objects defined in IEC 62351-7. The data objects that were not implemented are either not applicable to the scenarios considered for experiments in this research or are not practical to implement. These included data objects corresponding to physical access to real devices and data objects corresponding to usage of cryptographic keys shared between communication nodes. Neither of these are used for this research. This results in some gaps between what data objects are required to be available to NSM according to IEC 62351-7 and the data objects available to the NSM platform developed as part of this research.

Below is a review of the requirements for supporting intrusion detection defined in IEC 62351-7 that are met by the proposed NSM platform through monitoring of the NSM data objects described

in Section 4.7.

- **Detection of Unauthorized Access**

  The capability of the NSM system to detect attempts at unauthorized connections and transmissions depends on authorization keys being installed on devices. The current set of implemented data objects does not cover invalid key use, but can provide indication of machine access times and changes in configuration.

- **Detection of Resource Exhaustion**

  The IED data objects used as part of the proposed NSM platform provide a means for NSM to monitor memory and CPU exhaustion in an IED. There are also data objects that give information on the number of TCP connections that have been opened. The exact number of active connections open at the same time in a monitored device might not be directly exposed, making it difficult to determine if the maximum number of connections on a device has been exceeded. However, when compared to the maximum number of TCP connections available to the monitored device, the rate of increase in the number of opened TCP connections can act as an indicator that available TCP connections are being exhausted.

- **Detection of Invalid Buffer Access**

  The capability to detect invalid buffer access, specifically buffer overflows and buffer underflows, in the monitored devices requires that the monitored device has some way to inform an NSM agent when the device has experienced an overflow or underflow. This is expected to be a simpler task when the NSM agent is integrated inside the monitored device compared to the NSM agent being installed on some proxy device.

  The monitored devices used in this research do not expose when they experience a buffer overflow or underflow to other external devices. This prevents the proposed NSM platform from being able to detect invalid buffer access.

- **Detection of Malformed Packets**

  The monitored IEC 61850 data objects for the GOOSE protocol can indicate when malformed network packets or packets in error have been received. The same is true for the TCP and UDP

data objects. However, detecting packets that have been deliberately tampered, in the absence of integrity checks, likely requires either DPI or a IDS making use of contextual clues from other parts of the microgrid.

- **Detection of Physical Access**

  The monitored Environment data objects provide the capability of detecting when a monitored device has been directly accessed. In addition, the monitored Interfaces data objects can detect changes in the number of used interface ports. However, a direct means of detecting when a monitored device has been powered off is not provided to the proposed NSM platform. The NSM manager can however determine that a particular device is not responding to polling requests and can infer that the device may have been disconnected from the network or may have been shut down.

- **Detection of Invalid Network Access**

  The monitored data objects for TCP, UDP, IEC 61850, and IEC 104 (along with its derivatives) give information on the frequency and rate of traffic involving monitored devices as well as a count on the number of malformed network packets detected in the network. When taken together, this information can help to identify network misuse through a network intrusion.

- **Detection of Coordinated Attacks**

  In terms of detecting coordinated attacks, all of the monitored data objects may be considered to support this goal. The SCADA can attempt to detect similar patterns of abnormal behaviour across different power systems by one or more NSM managers. In particular, the data objects for protocols can give indication of communication failures and DoS attacks across different systems, while the IED data objects can help detect device failures across different systems.

4.9 Attack Scenario Formulation

In order to assess the effectiveness of the proposed NSM solution at detecting cyber-physical attacks launched against the microgrid, attack scenarios that are representative of potential attacks in real system need to be formulated and launched on the microgrid testbed. The set of attack

scenarios considered for validation of the proposed NSM solution are meant to cover a wide range of possible actions that an attacker can take to negatively impact the operation of the microgrid. Both the network elements targeted by the attacks and the means through which these attacks are accomplished should be carefully considered so as to reach this coverage.

As part of this research, a methodology for designing attack scenarios to be launched against the microgrid testbed is elaborated. The goal of this methodology is to provide a set of steps that can be followed to systematically generate microgrid attack scenarios. The methodology accepts a set of system constraints as input in order to generate these attack scenarios.

The set of input constraints used in this methodology consists of a list of invariants. If an invariant is violated, then an abnormal condition is created, and negative impacts on the operation of the microgrid may occur. Examples of negative impacts include power losses, system instability, loss of system visibility, and theft of information. Through this methodology, the different kinds of attacks that can be launched against the microgrid to break the constraints, along with the variations of these attacks, can be exposed. From these attacks, a set of practical attack scenarios to simulate for evaluating the effectiveness of the NSM solution can be chosen.

For this research, the attacker model restricts attackers to only have direct access to the communication network. Attackers are assumed to have access to the digital communication channels, allowing attackers to both read and modify the traffic flowing between communication nodes.

4.9.1 General Methodology

The methodology for designing attack scenarios against the microgrid is adapted from one that is applicable to any ICS system. In short, the methodology involves the identification of undesirable system conditions, the determination of system variables relevant to each undesirable condition, and an assessment of what means are available to attackers within the system for influencing those system variables.

This research focuses on the impact of potential cyberattacks on physical systems. As such, the attacker capabilities considered are restricted to the digital communication network. Attack scenarios can be broken down into a series of basic actions that can be performed by an attacker. The basic actions considered here are inspired by the cyberthreats outlined in the Sandia Laboratories report

described in Section 2.2. Together, they compromise the availability, integrity, and confidentiality of microgrid communications.

An attacker is assumed to have the capability of eavesdropping on network traffic, injecting traffic, and using a MitM attack to modify message contents or impact message transmission. With these capabilities in mind, six basic cyberattack actions are available to an attacker in the network when considering potential attack scenarios. These actions are the following:

- Reading messages
- Replaying messages
- Injecting messages
- Modifying messages
- Delaying messages, and
- Dropping messages

The generic methodology for formulating attack scenarios against an ICS is composed of five steps. These steps are described as follows:

(1) **Define the invariants of the system**

An invariant is a condition that, if violated, moves the system to a state of operation that can result in undesired impacts on the system output or system resources. Security measures should aim to prevent these invariants from being violated.

(2) **Determine the variables related to the invariants**

An invariant being violated depends on a set of elements of the system that can change during operation. These variable elements must be identified as well as what state these variables must be in to violate the given invariant.

(3) **Identify the basic actions that alter the related variables**

Attackers launching a cyberattack have a specific set of actions they can perform against communication networks depending on the capabilities that the attacker is assumed to have.

The subset of these actions which have an impact on the variables related to the invariants must be identified.

(4) **Find attack step sequences that cause the invariant to be violated**

Once the variables and the actions that can alter these variables are determined for a given invariant, the specific actions that an attacker must take to violate each invariant must be determined. The values, timing, and parameters that an attacker needs to use as inputs must be taken into account.

(5) **Assess the impact of the attack sequences**

After describing the cyberattack that an attacker can launch to violate the given invariant, an assessment of the impacts the attack would have on the system is made. This assessment influences the choice of relevant attack scenarios to be used for experimental evaluation.

4.9.2 Methodology Applied to IEC 60870-5-104

In the microgrid testbed, the microgrid simulation relies on digital communications to enable the exchange of information between the microgrid power system devices and the their central control. The IEC 104 protocol, running over TCP, is used for telecontrol communication in the simulated microgrid. The tasks performed using telecontrol include frequency regulation, load shedding, power shedding, and setting operation mode of microgrid DERs. The IEC 104 protocol is susceptible to cyberattacks, and the relative importance of the control tasks performed using this communication protocol make it necessary to study the security issues related to the use of this protocol.

4.9.2.1 Invariants of Microgrid Communication Network

Based on the characteristics and behaviour of the IEC 104 protocol described in Section 4.6, a set of invariants can be derived for the microgrid communication network using the protocol. The violation of these invariants can result in adverse effects such as microgrid power instability, loss of efficiency, and damage of equipment. The invariants considered here are all limited to the specifications of the IEC 104 protocol itself and does not consider implementations of the protocol from particular vendors.

The violations for invariants related to IEC 104 communications in the microgrid can be broken down into three categories: APDU rejection, false APDU data, and disconnecting an established IEC 104 connection. The invariants for IEC 104 communications and the categories their violations fall under are listed in Table 4.1.

#	Violation Name	Violation Category	Invariant Being Violate
1	Invalid header byte	APDU rejection	$apduStartByte = 0x68$
2	Incorrect APDU length	APDU rejection	$len(apdu) = apduLen + 2$
3	Incorrect information object count	APDU rejection	$informationObjectCount(apdu) = apduNumIx$
4	Wrong sequence number	APDU rejection	$lastRxS\_frameSeqRx \geq lastTxI\_frameSeqTx + 1$
5	Wrong type	APDU rejection	$typeOf(informationObject) = apduTypeId$
6	Test flag is set	APDU rejection	$test = false$
7	Incorrect ASDU address	False data	$senderAddr(apdu) = asduAddr$
8	Incorrect cause of transmission	False data	$senderCauseTx(apdu) = apduCauseTx$
9	Incorrect object address	False data	$ioAddr(informationObject) = ioa$
10	Incorrect object value	False data	$senderValue(informationObject) = value$
11	Unconfirmed connection	Connection drop	$\exists apdu \in RxU\_frame, apdu.UType = STARTDTcon \vee unconTimeout = false$
12	Unacknowledged message chain	Connection drop	$bufferOverflow = false \wedge respRxTimeout = false \wedge maxUnconTxI\_Format = false$

Table 4.1: List of invariants for IEC 60870-5-104

4.9.2.2 Variables Related to Invariants

The variables considered for the invariants described in Section 4.9.2.1 relate to several aspects of IEC 104 communications. These aspects include the value of the IEC 104 APDU fields in the IP packets transmitted across the network, the actual information and characteristics of the IP

packets containing IEC 104 APDUs, the data intended to be delivered through the APDUs, the sequence numbers maintained by the stations communicating over IEC 104, and the state of timeouts and buffers.

The variables are classified as being APDU field data contained within IEC 104 packets, being data that a station transmitted and intended to be received by the destination, or being related to an internal state of a station. The variables within these categories are listed in Table 4.2, Table 4.3, and Table 4.4, respectively.

Variable Name	**Related Invariant Violation**	**Description**
$apdu$	Invalid header byte	IEC 104 payload unit consisting of a APCI/ASDU pair
$apduStartByte$	Invalid header byte	The first byte of the APDU, which identifies it as a IEC 104 packet
$apduLen$	Incorrect APDU length	The length of the APDU as stated by the APDU length field
$apduNumIx$	Incorrect information object count	The number of information objects in the APDU as stated by the information object count field
$lastRxS\_frameSeqRx$	Wrong sequence number	The value of the Rx sequence control field in the APCI of the last S-format APDU frame received
$apduTypeId$	Wrong type	The data type of the information object values in the APDU as stated by the type identification field
$test$	Test flag is set	The test flag field that, if true, indicates that the APDU is meant for testing and should not generate a response
$asduAddr$	Incorrect ASDU address	The ASDU address as stated by the ASDU address field
$apduCauseTx$	Incorrect cause of transmission	The CoT of the ASDU as stated by the CauseTx field
ioa	Incorrect object address	The IOA of the information object as stated by the IOA field
$value$	Incorrect object value	The value of the information object as stated by the value field
$apdu.UType$	Unconfirmed connection	The type of the U-format APDU frame (STARTDT_con, STOPDT_con, or TESTFR)

Table 4.2: Invariant variables corresponding to APDU fields

4.9.2.3 Identification of Cyberattack Actions

The IEC 104 APDU are transmitted over TCP in plaintext without any checks on message authenticity or integrity. The lack of message authentication and integrity checks allows an attacker

Variable Name	Related Invariant Violation	Description
$senderAddr(apdu)$	Incorrect ASDU address	The original ASDU address of the sender of the APDU
$senderCauseTx(apdu)$	Incorrect cause of transmission	The original Cause of Transmission (CoT) of the ASDU
$ioAddr(InformationObject)$	Incorrect object address	The original Information Object Address (IOA) of the APDU information object
$senderValue(informationObject)$	Incorrect object value	The original value of the information object in the ASDU

Table 4.3: Invariant condition variables corresponding to incorrect data

Variable Name	Related Invariant Violation	Description
$lastTxI\_frameSeqTx$	Wrong sequence number	The value of the Tx sequence control field in the APCI of the last I-format APDU frame transmitted
RxU_frame	Unconfirmed connection	The last U-format ASDU frame received
$bufferOverflow$	Unacknowledged message chain	Is set to true when the buffer space used to hold ASDUs before transmission has been exceeded
$unconTimeout$	Unacknowledged message chain	Is set to true when the time interval where connection establishment response is expected is exceeded
$respRxTimeout$	Unacknowledged message chain	Is set to true when time the interval where ASDUs can be sent without confirmation S-format frame is exceeded
$maxUnconTxIFormat$	Unacknowledged message chain	Is set to true when the maximum number of ASDUs that can be sent without a confirmation S-format frame is exceeded

Table 4.4: Invariant variables corresponding to internal state

who has compromised the communication link with a MitM attack to freely modify packets that they intercept. In addition, the attacker is capable of injecting, delaying, or dropping packets while acting as a MitM. For the purpose of elaborating attack scenarios, the attacker is assumed to be able to perform any number of actions from a section of basic cyberattacks. The set of basic cyberattacks consists of reading, injecting, replaying, modifying, delaying, and dropping IEC 104 packets. The attacker can make use of these actions to modify the variables in IEC 104 communication in order to violate an invariant. The list of which basic cyberattack actions can change the state of each relevant variable is described in Table 4.5.

Being a protocol that uses TCP connections, the IEC 104 protocol is also susceptible to DoS attacks that are effective against TCP such as SYN flood attacks. While these attacks are relevant threats to the operation of the microgrid, they are out of the scope of this research.

Name	Invariant #	Replay/Inject	Modify	Delay/Drop
$apduStartByte$	1		✓	
$len(apdu)$	2		✓	
$apduLen$	2		✓	
$informationObjectCount(apdu)$	3		✓	
$apduNumIx$	3		✓	
$lastRxS\_frameSeqRx$	4	✓	✓	✓
$lastTxI\_frameSeqTx$	4			
$typeOf(informationObject)$	5		✓	
$apduTypeId$	5		✓	
$test$	6		✓	
$senderAddr(apdu)$	7			
$asduAddr$	7	✓	✓	
$senderCauseTx(apdu)$	8			
$apduCauseTx$	8	✓	✓	
$ioAddr(InformationObject)$	9			
ioa	9	✓	✓	
$senderValue(informationObject)$	10			
$value$	10	✓	✓	
RxU_frame	11	✓	✓	✓
$apdu.UType$	11		✓	
$bufferOverflow$	12		✓	✓
$unconTimeout$	12		✓	✓
$respRxTimeout$	12		✓	✓
$maxUnconTxIFormat$	12		✓	✓

Table 4.5: Susceptibility of variables to basic cyberattacks

4.9.2.4 Attack Step Sequences that Violate Invariants

With consideration of the basic cyberattacks that can impact the communication variables, a sequence of actions that an attacker can take to violate each invariant can be described. Below are attack step sequences that can cause the IEC 104 invariants to be violated.

- Invalid header byte

  1) Intercept an IP packet with IEC 104 APDU
  2) Modify the header byte so that it no longer matches the IEC 104 header byte (`0x68`) e.g., by setting it to `0x00`
  3) Forward the modified packet to the original destination

  Result: an error is raised on the APDU and the connection must be reset.

- Incorrect APDU length

  1) Intercept an IP packet with IEC 104 APDU
  2a) Modify the APDU length field to a value that does not match the APDU size
  2b) Append or truncate bytes from the APDU
  3) Forward the modified packet to the original destination

  Result: an error is raised on the APDU and the connection must be reset.

- Incorrect information object count

  1) Intercept an IP packet with IEC 104 APDU
  2) Modify the information object count field of the intercepted packet to a value that is lower than the number of information objects
  3) Forward the modified packet to the original destination

  Result: an error is raised on the APDU and the information objects beyond the modified information object count field value are not parsed.

- Wrong sequence number

  1a) Read Tx sequence number of an I-format APDU sent from an outstation
  2a) Fabricate an I-format APDU with a Tx sequence number that is one greater than the read APDU

3a) Send the fabricated packet to the master station that received the read APDU

1b) Intercept an IP packet with a S-format APDU sent from the master station

2b) Modify the Rx sequence number of the intercepted packet to a value that is less than the original APDU Rx sequence number

3b) Forward the modified packet to the original destination

Result: the master station considers the APDU sent by the outstation to be out of sequence.

- Wrong type

1) Intercept an IP packet with IEC 104 APDU

2a) Modify the type field to a type with a different expected data value byte size than the original type

2a) Modify the type field to a type with the same expected data value byte as the original type

3) Forward the modified packet to the original destination

Result: The APDU is not parsed properly, and a parsing error is raised if the expected data value byte size differs from the original.

- Test flag is set

1) Intercept IP packet with a I-format APDU

2) Modify the test flag field to have it set to $true$ (1)

3) Forward the modified packet to the original destination

Result: the APDU is considered a test packet and no further action is taken based on the APDU data.

- Incorrect ASDU address

1) Identify two I-format APDU packet streams with the same information object address and type identification from two different outstations having different ASDU addresses

2) Intercept IP packet with a I-format APDU from one of the streams

3) Change the ASDU address field to the ASDU field value of the other stream

4) Forward the modified packet to the original destination

Result: the APDU is considered to have come from an outstation that is not the original sender.

- Incorrect cause of transmission

1) Intercept IP packet with a I-format APDU

2) Modify the cause of transmission field to a different value

3) Forward the modified packet to the original destination

Result: the APDU is attributed to a cause of transmission that differs from the original cause of transmission.

- Incorrect object address

1) Identify two I-format APDU packet streams with the same type identification field value but different information object address field values

2) Intercept IP packet with a I-format APDU from one of the streams

3) Modify the information object address field to the information object address value of the other stream

4) Forward the modified packet to the original destination

Result: the value of the information object in the APDU is attributed to the state of a different monitored element than was intended.

- Incorrect object value

1a) Read information object values of an I-format APDU

1b) Intercept IP packet with a I-format APDU from one of the streams

2a) Fabricate an I-format APDU with false values for that information object

2b) Modify the value field of an information object to another value that is parsed with the same type identification

3a) Send the fabricated packet to the station that received the original read APDU

3b) Forward the modified packet to the original destination

4a) Drop any confirm APDU that might be sent by the station receiving the fabricated packet

4b) Revert the modifications to the information object value for any $ActCon$ response APDU that is sent by the original destination

Result: A value for the information object is assumed that differs from the intended value of the original APDU.

- Unconfirmed connection

1) Intercept IP packet with a STARTDT_con U-format APDU

2a) Modify the packet to remove the STARTDT_con field value

2b) Drop or significantly delay the intercepted packet

3) Forward the modified packet to the original destination

Result: The IEC 104 connection is not confirmed and becomes closed, preventing further IEC 104 communication.

- Unacknowledged message chain

1) Intercept IP packet with a S-format APDU used for message chain confirmation

2a) Modify the packet to change it to a U-format frame

2b) Drop or significantly delay the intercepted packet

3) Forward the modified packet to the original destination

Result: The destination station closes IEC 104 connection due to the maximum allowable time or transmitted APDUs without confirmation being exceeded.

4.9.2.5 Impact of Attack Sequences

By bringing about invariant violations and disrupt communication, an attacker can impact the secondary control level operations that rely on IEC 104 communications. This disruption can involve the prevention of needed information from being successfully transmitted or even injecting false data that becomes interpreted as legitimate secondary control data. The adverse effects that attacks against the control communications will have on the microgrid include loss of reliability, loss of stability, and loss of efficiency. Specific communications to target in order to produce these losses include messages that change operation parameters and messages that carry data being utilized for feedback control processes such as frequency regulation.

4.10 Conclusion

In this chapter, the design of the NSM platform used to address the problem of microgrid security monitoring is described in detail. As part of the design, multiple NSM agents are used to collect NSM data directly from the microgrid system elements. A central NSM manager periodically polls each of the NSM agents for the NSM data collected, then aggregates the data by time. The aggregated data is sorted by time and given as input to an anomaly detection module that uses rule-based and machine learning techniques to detect anomalies in the data. Should an anomaly be detected, an alert is generated to signal the presence of a potential cybersecurity threat.

Also discussed in this chapter is the methodology used to design the attack scenarios chosen for evaluating the NSM platform. The application of the methodology begins by identifying the invariants that, if violated, set the microgrid to an undesirable state. The variables tied to the invariants are determined, along with the vulnerability of each variable to different types of cyberattacks targeting the availability, integrity, and confidentiality. Attack steps to violate the invariants by attacking these variables are elaborated, and their impact on the microgrid system is assessed.

Having explained the design of the NSM security monitoring platform, what follows is a description of its implementation details, along with details on the microgrid system on which the platform is tested. In addition, the set of tests performed for NSM evaluation are described. The results of these tests are provided and discussed.

Chapter 5

Microgrid Testbed and Experimental Evaluation

5.1 Overview

In order to carry out research on the effectiveness of the proposed NSM design for the microgrid against cyber-physical attacks, an NSM platform is implemented and deployed on a smart grid co-simulation testbed that is leveraged for microgrid simulation.

The smart grid co-simulation testbed is used to perform experiments relevant to cyber-physical security. The testbed combines a DRTS with real IEDs connected to the simulation as HIL. The DRTS and real hardware devices are interconnected through a local IP network. The testbed is able to simulate attacks scenarios on the simulated power system that combine physical failures in the simulation with cyberattacks in the digital network. For this research, the DRTS is used to simulate a microgrid power system.

The NSM manager and agents are realized as software installed on Virtual Machines (VMs) deployed in the network. To address the limitation of monitored devices not allowing custom code providing added functionality to be installed on them, the NSM agent software is installed on VMs acting as proxies for the monitored devices, collecting information about the monitored device and the digital traffic flowing through it to be served to the NSM manager.

In this chapter, the smart grid co-simulation testbed is described, which includes a description of

the simulated microgrid power model and the IP network that connects the power model simulation with real and virtual devices. This chapter also gives details on the implementation of the NSM agent and NSM manager, as well as details on how they are deployed in the microgrid testbed. Moreover, details on the attack scenarios launched on the testbed are given in this chapter, as well as details on the anomaly detection tools used in the testbed.

5.2 Smart Grid Co-simulation Testbed Setup

The smart grid co-simulation testbed used in this research is extended from the work of Albarakati *et al.* **[59]**. It consists of a real-time electrical power model simulator, an IP network that connects to the power model simulator, physical IEDs, and VMs that are placed within the IP network.

The simulated microgrid features simulated power equipment that makes use of digital communication for monitoring and control. The simulated equipment can both send and receive digital messages through the network that connects the real IEDs and VMs. In this way, the equipment simulated in the power simulator is capable of communicating with devices deployed in the IP network. Figure 5.1 gives a high-level view of the smart grid co-simulation testbed. Additional details can be found in the work of Albarakati *et al.* **[59]**.

5.2.1 Power System Simulator

This research makes use of HYPERSIM DRTS developed by OPAL-RT Technologies. The HYPERSIM DRTS is able to integrate HIL and digital communication protocols into a real-time simulation of power system applications. HYPERSIM is capable of running simulations with time steps under 100 microseconds (μs) and capable of HIL integration. HIL integration allows real IEDs to interact with HYPERSIM so as to take part in the power simulation **[60]**.

HYPERSIM offers the capability to construct an electrical power system model using modular components. The components can be categorized as follows:

- Simulated power generation sources e.g., electrical power generators
- Simulated line equipment e.g., circuit breakers

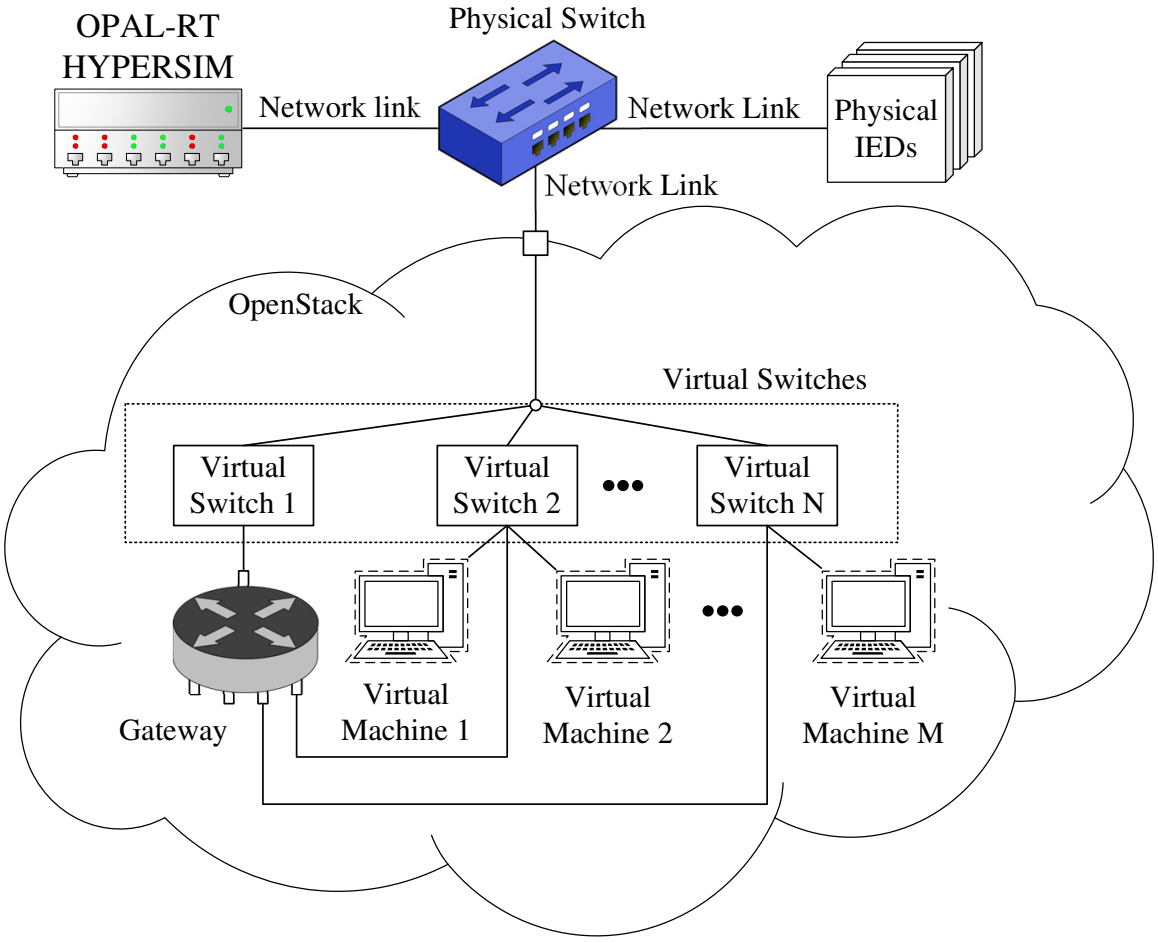

Figure 5.1: Configuration of smart grid co-simulation testbed

- Control functions e.g., overcurrent protection
- Control signals e.g,. pulse waves, and
- Input and output nodes for interfacing with real devices connected to HYPERSIM.

The features provided by HYPERSIM allow one to test the operation of electrical power systems under normal conditions and under fault conditions. HYPERSIM allows monitoring of the simulated real-time power system measurements such as line voltage and current. HYPERSIM also supports the triggering of electrical faults in the power grid, whose impact can be determined by observing voltage and current measurements across the simulated power network.

In regards to networking, HYPERSIM allows the power system it simulates to send and receive

message traffic using ICS digital communications protocols. These capabilities allow real IEDs to receive appropriate signals from HYPERSIM simulations to act upon as well as having traffic from IEDs impact the simulation.

For this research, HYPERSIM is used to construct a microgrid power system to be simulated in real-time. The set of modular components available in HYPERSIM together with its real-time simulation capabilities makes it appropriate and relatively simple to use for demonstrating the effectiveness of NSM in the face of cyber-physical threats against the microgrid. Details on the microgrid model built for use in the co-simulation testbed are provided in Section 5.3.

5.2.2 Testbed Communication Network

A communication network is implemented on the testbed in order to enable the transmission of digital message within the microgrid simulation. The communication network is realized as a local IP network with configurable routing. This research studies the effect of attacks compromising the digital communications between devices in the microgrid, therefore having an isolated and controllable network on which to run cyberattack experiments is an important aspect of the testbed.

This research makes use of a server with an IP communication network to interconnect VMs with the OPAL-RT DRTS. Virtual machines are created within the network, while the ORAL-RT DRTS has network interfaces allowing it to be connected to the network. The IP network and OPAL-RT DRTS are connected to a shared physical switch through which they can communicate.

The IP communication network used for this research is built using OpenStack **[61]**. OpenStack is a software that is used to create and manage public or private IP cloud networks. OpenStack can configure connections between routers, switches, and computer machines to integrate them into the managed network. It can also create VMs for the managed network. OpenStack allows for the creation of virtual network switches. These virtual switches are capable of separating the OpenStack VMs into different subnets, whose access to other subnets is controlled by firewall and routing rules.

For this research, OpenStack is chosen to create the communication network due to its ability to integrate the HYPERSIM DRTS into the network, deploy VMs on which to install custom code, and configure virtual switches for subnetting. The communication network uses several virtual switches to separate the deployed VMs based on their function, and a gateway manages the firewall

and routing rules for the IP network. The integration of HYPERSIM into the network is necessary to generate the digital communications of the microgrid simulation in the presence of NSM and microgrid control applications. The installation of custom code is needed for the deployment of the NSM manager, NSM agents, and the application performing the microgrid central control logic. The OpenStack virtual switches are used to facilitate the monitoring of traffic flowing into and out of the the HYPERSIM DRTS. To perform traffic monitoring, the virtual switch connecting the HYPERSIM subnet to the rest of the network duplicates data packets passing through the HYPERSIM subnet, then forwards the packet duplicates to other VMs in the subnet that analyze the packets. This traffic monitoring mechanism is used to allow the deployed NSM agents to analyze microgrid network traffic.

5.3 Simulated Microgrid Benchmark

In order to simulate the effect of attacks on the microgrid, a simulation model that is representative of a real microgrid has to be built. As part of this research, a microgrid system is elaborated in HYPERSIM for simulation in the OPAL-RT DRTS connected to a co-simulation testbed. The microgrid simulation model is treated as a benchmark, with the performance and behaviour of the simulated microgrid being evaluated when subjected to different attacks. While the simulation is running, NSM agent proxies deployed in the co-simulation testbed report on the state and actions of the components in the microgrid to the deployed NSM manager.

The microgrid benchmark simultaneously models the microgrid power system and the microgrid digital communications. The power and communication system components in the benchmark can be coupled to HIL devices installed in the testbed and connected to the testbed IP network. This allows the simulation to better capture the real behaviour of any connected HIL devices and their communications in response to microgrid system inputs. The benchmark also includes components that are purely simulated within OPAL-RT. These nodes simulate the behaviour of the real component to which they correspond, both in regards to the impact they have on the power system and the digital communications they may transmit and receive. Digital communications from the simulated

components are transmitted through the testbed IP network to reach the VMs in the OpenStack network, as well as any HIL devices. Similarly, network components simulated in the benchmark can receive digital communications from HIL devices and the OpenStack network that is directed to the benchmark components.

The power model of the microgrid benchmark consists of DERs, loads, a power source simulating the main grid, and a PCC connection to the simulated main grid. In addition, it includes power lines interconnecting these power system components as well as power equipment such as circuit breakers, measurement units, and transformers. In addition, the power model includes local control loops for the DERs to help regulate the frequency of the microgrid, where the target frequency is 60 hertz (Hz).

Microgrid control operations fall into a hierarchy of three levels: the primary control level, the secondary control level, and the tertiary control level **[13]**. The primary control level involves operations local to each DER and load, with controls to such microgrid elements being based solely on information available from within that element. The secondary control level involves operations that control the microgrid based on consideration of the state of the microgrid as a whole. The tertiary control level involves operations that take into account the smart grid at large when exerting control on the microgrid with the intention to coordinate between multiple power subsystems such as microgrids. The simulated microgrid only includes primary and secondary control level operations. Primary control functions are performed within each DER, while secondary control functions are performed by a Microgrid Central Controller (MGCC) that monitors the entire microgrid.

5.3.1 Topology of Microgrid Benchmark

The microgrid benchmark simulation has the following DERs: One PV array, one Combined Heat and Power (CHP) synchronous generator, a wind farm with three WTs, and three battery Energy Storage Systems (ESSs). The PV array can deliver up to 1.5 MW of electric power to the microgrid. The PV array produces DC power, which is converted to AC power by a converter before reaching the microgrid. A high level view of the microgrid benchmark topology and its various components is given in Figure 5.2.

The CHP synchronous generator can deliver up to 10 MW of AC power under normal conditions

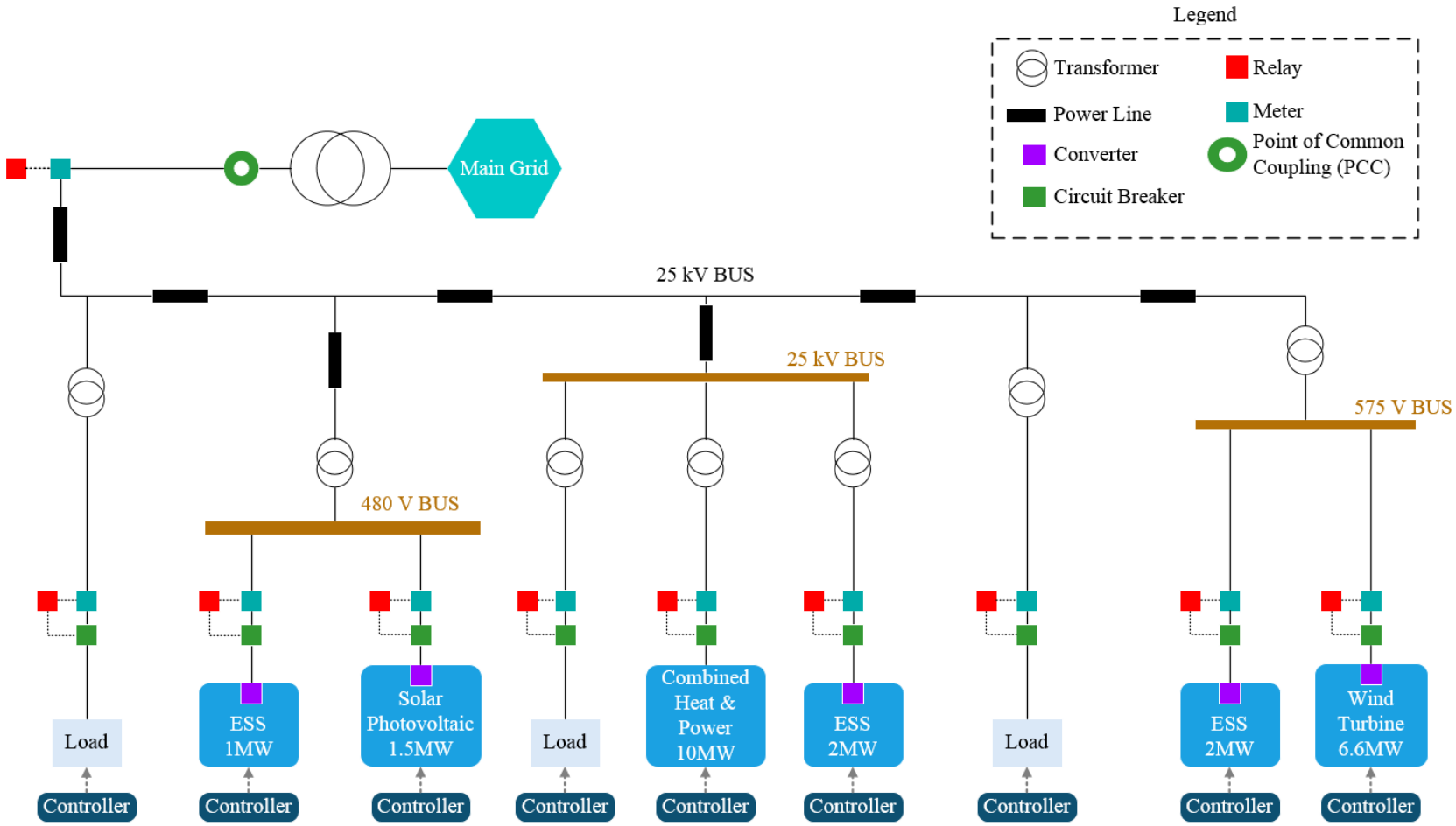

Figure 5.2: Microgrid benchmark simulated in co-simulation testbed

while the microgrid is in grid-connected mode. The CHP generator is the largest source of power entering the microgrid among the DERs. Due to being asynchronous machine with large power supply capacity, the CHP generator acts as the "slack bus" when the microgrid is in islanded mode, and the phase angle of the CHP generator is used as the reference phase angle that is set to the zero value when performing power flow analysis for the islanded microgrid. The power delivered by the CHP generator is set to adjust in real time while the microgrid is in islanded mode to help regulate the frequency of the microgrid as a whole. The three WTs in the wind farm can each deliver up to 2.2 MW, delivering a total of 6.6 MW. The WTs provide AC voltage, but a converter is needed to set the frequency of the WT power to the 60 Hz target frequency of the microgrid. Of the three ESS batteries, two of them can absorb or deliver up to 2 MW of electric power and have a capacity of 9600 ampere hour (Ah), while the third battery can only absorb or deliver up to 1 MW of power and has a capacity of 4800 Ah. The ESS batteries deliver and absorb power through DC, and a converter is needed to convert the DC voltage of the batteries to the AC voltage of the microgrid. The PV array also provides DC voltage, and requires a converter in order to provide AC voltage.

The DERs power lines connect to a shared common bus in the microgrid benchmark. The common bus is also connected to the microgrid loads and the PCC acting as the interface to the main grid. The common bus of the microgrid benchmark is 25 kV (root mean square). The DERs operate at a much lower voltage, and a transformer steps up the voltage from the DERs to the 25 kV voltage of the common microgrid bus. The 1 MW ESS batteries is placed in the same low-voltage level as the PV array. This low-voltage level is 0.48 kV. The CHP generator is in a 2.4 kV voltage level, and a transformer steps up its voltage to 25 kV. One of the 2 MW batteries is placed in its own voltage level of 0.48 kV. The other 2 MW battery lies within the same 0.575 kV voltage level bus as the wind farm, with the bus being connected to the common microgrid bus through a transformer that steps up the voltage to 25 kV.

The benchmark has three dynamic loads, whose power demand can be adjusted while the simulation is running. The power demand set for the three loads is 1 MW each under normal conditions, reaching a combined total of 3 MW. The loads are configured to operate at 0.24 kV and at 60 Hz. Transformers are needed to step down the 25 kV voltage coming from the common microgrid bus to 0.24 kV.

In the microgrid benchmark, the common microgrid bus is connected to a high-voltage 60 Hz AC power source, which represents the expected input voltage coming from the main grid between which power would be exchanged with the microgrid. The high-voltage line that connects the microgrid to the main grid operates at 120 kV. Between the power source and the common microgrid bus is the PCC. A transformer steps down the high-voltage of the main-grid line from 120 kV to 25 kV after passing through the PCC.

Circuit breakers are used throughout the microgrid benchmark, placed between the common microgrid bus and the DERs as well as the loads on the power lines connecting them. There is also a circuit breaker between the transformer that steps down the voltage from the main grid and the common microgrid bus. The line voltage and current of the microgrid and its DERs are measured at the location of the circuit breakers in the simulation benchmark. Through measuring the voltage and current, the active and reactive power can also be determined at these locations in real time.

5.3.2 Protection and Control Systems of Microgrid Benchmark

The power distribution of the microgrid is subject to protection and control systems. An essential part of the protection system is line fault protection, which prevents electrical line faults from destabilizing a large portion of the microgrid. Among of the functions of the control system is frequency control, which ensures that the microgrid frequency remains within safe levels.

5.3.2.1 Line Fault Protection

In order to ensure the smooth operation of the microgrid against faults, adequate protection measures must be in place. The microgrid benchmark allows for line-to-ground faults to be triggered during the microgrid simulation. A line-to-ground fault on a line describes the event when a direct path between the line and a ground is inadvertently formed [62]. It is important that these faults are detected quickly and that the system is able to rapidly recover from these faults in order to maintain the stability of the microgrid. Fault protection can be realized through the use of protection relays. Measurement units read electrical system measurements, such as current and voltage, which are transmitted to protection relays. In the event of an electrical line fault, the protection relays send trip signals to circuit breakers. The trip signals cause the circuit breakers to open in an attempt to

isolate the fault and prevent damage from propagating across the microgrid from the fault location. By isolating the fault, only a small portion of the microgrid may be brought offline as a result of the fault.

Several challenges unique to the microgrid complicate the task of providing protection for microgrid operations. These include the existence of bidirectional power flows, DERs with output dependent on weather conditions, uncertain load demand, and the capability for the microgrid to switch between grid-connected mode and islanded mode [13]. In regard to the operation mode of the microgrid, what constitutes acceptable levels for electric power characteristics like voltage and current can differ depending on whether the microgrid is in grid-connected mode or in islanded mode. This means relays need to be aware of the operating state of the microgrid, and requires that relays be connected to communication links that can transmit the operation mode of the microgrid to the relays.

The microgrid benchmark relies on protection relays to detect faults that arise in the microgrid and send commands to the appropriate circuit breakers so that those circuit breakers open in order to isolate the fault. The commands sent to circuit breakers to trigger the opening of the circuit breaker are known as trip commands. The protection relays detect faults by receiving local current and voltage measurements, then comparing the received measurements to configured fault thresholds. If a measurement threshold for a relay is exceeded, a trip command is sent by the relay to circuit breakers such that the fault becomes isolated from the rest of the microgrid as a result of the circuit breakers being opened.

The microgrid benchmark makes use of three kinds of protection relays: overvoltage relays, undervoltage relays, and overcurrent relays. Overvoltage relays detect when the line voltage reaches voltage levels that are significantly higher than the expected, or nominal, voltage. when an overvoltage is detected, the overvoltage relay sends a trip command to circuit breakers that can isolate the line experiencing overvoltage. Similarly, the undervoltage relays detect when the line voltage dips too much from the nominal voltage, sending trip commands to circuit breakers when undervoltage is detected. The overcurrent relay detects when the amount of current exceeds a configured threshold, sending trip commands to circuit breakers when an overcurrent is detected. The benchmark uses overcurrent relays to protect the microgrid system from electrical faults. At the same time, it also

uses overvoltage and undervoltage relays to protect the DERs.

The thresholds that the protection relays must use when the microgrid is in islanded mode is different from the ones they must use when the microgrid is in grid-connected mode. In islanded mode, the relays should widen the range of acceptable power quality values to account for the less stable operating conditions expected for the microgrid. The protection relays in the benchmark microgrid can toggle between operating in grid-connected islanded modes by receiving a digital input signal indicating that the microgrid has switched operation mode.

5.3.2.2 Frequency Control

In the microgrid benchmark, various DERs delivering power to and absorbing power from the microgrid simultaneously in differing amounts can cause fluctuations in the frequency across the microgrid. In addition, the amount of power absorbed by the loads can change over time, contributing to frequency fluctuations. These fluctuations are the result of imbalances between the amount of power delivered by the DERs and the amount of power absorbed by the loads. Should the amount of power being delivered to the microgrid exceed the power being absorbed from the microgrid, the frequency of the microgrid will exceed the target frequency, in this case 60 Hz. Similarly, should the amount of power being absorbed from the microgrid exceed the power being delivered to the microgrid, the frequency of the microgrid will drop below the target frequency.

In grid-connected mode, the main grid is capable of both absorbing excess power from the microgrid and supply power to fill any power deficits in the microgrid. However, in islanded mode the lack of connection to the main grid makes it more difficult to balance the power sources and consumers. The IEEE 1547 standard specifies the maximum allowed deviation of the microgrid frequency from the target frequency in grid-connected mode and in islanded mode [14]. IEEE 1547 specifies that in grid-connected mode, the maximum allowable deviation from nominal frequency, with 60 Hz being the nominal frequency for the microgrid benchmark, is 2.5%. In islanded mode, the maximum allowable deviation is 5%. Should the frequency deviation exceed these limits, corrective action must be taken to bring the frequency within the acceptable range of deviation. If the corrective actions are not sufficient to stabilize the frequency and bring it within acceptable range, the microgrid is shut down, causing all loads and DERs to be shut down.

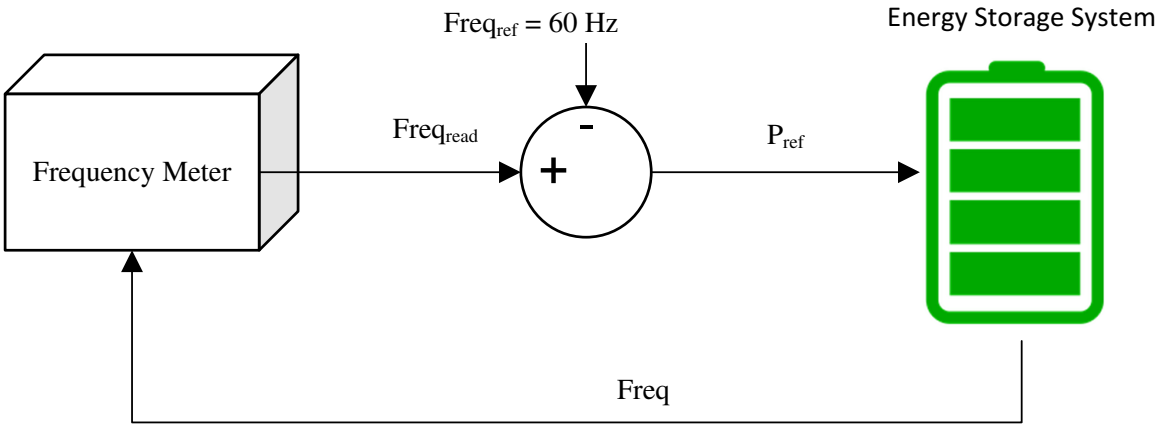

Figure 5.3: Local frequency control loop of ESS

The DERs offering the most control over the amount of power they deliver or absorb are the ESS batteries. The ESS batteries can be reconfigured during operation to absorb energy instead of deliver energy and vice versa. Changing the active power of the ESSs allows for frequency control of the microgrid that aims to maintain a microgrid frequency of around 60 Hz. Underfrequency can be corrected by increasing the power output of the ESSs, while overfrequency can be corrected by decreasing it.

The ESS units simulated in the microgrid benchmark each accept an input from a controller that sets their power output, with both the direction and magnitude of the voltage being determined by the input value. To regulate the frequency at each ESS, the local feedback loop depicted in Figure 5.3 is used. As part of the local feedback loop, the frequency of the ESS is measured. The difference between the measured frequency and the nominal frequency of 60 Hz is passed as an input to the ESS voltage control by the ESS controller.

5.3.3 Communication Network of Microgrid Benchmark

The simulated power equipment used across the microgrid benchmark is connected to a digital communication network that spans the entire microgrid and provides a means of exchanging digital messages with the MGCC.

5.3.3.1 Topology of Microgrid Communication Network

The communication network of the microgrid benchmark is composed of IEDs, with each IED controlling a set of local devices and acting as an outstation to engage in digital communications with a master station. An IED is deployed near the PCC and at each of the DERs and loads. Specifically, each ESS and load has a corresponding IED, as does the CHP generator and the wind farm. The MGCC is deployed in a station that is separated from the rest of the microgrid. It engages in digital communication with the IEDs in the microgrid. While the MGCC is able to directly communicate with the IEDs, the IEDs do not directly communicate with each other. The IEDs execute control commands received from the MGCC commands. They also read data from measurement meters and send commands to relays for which they are responsible. The IED near the PCC also informs the MGCC whether the PCC breaker is open or closed. The communication network can thus be described as having a star topology, with the MGCC at the centre of the network. The placement of the IEDs within the benchmark is shown in Figure 5.4

5.3.3.2 Microgrid Communication Network Protocols

Communications between the IEDs and the MGCC use the IEC 60870-5-104 (IEC 104) telecontrol protocol that runs over TCP/IP. The IEDs act as outstations while the MGCC acts as the master station. The MGCC, acting as the master station, initiates IEC 104 connections with the IEDs and sends commands to them while receiving responses and spontaneous event messages from the IEDs. The protection relays use the IEC 61850 GOOSE Ethernet protocol to send trip commands to circuit breakers. There is less overhead involved in GOOSE communication compared to IEC 104 communication, with GOOSE communications not requiring connection establishment protocols or having messages be acknowledged. This results in GOOSE trip commands being read by circuit breakers sooner than they would be if IEC 104 was used.

5.3.3.3 Microgrid Protection and Control

The MGCC performs several protection and control functions that fall within the secondary control level of the microgrid benchmark. These functions include frequency control, load shedding,

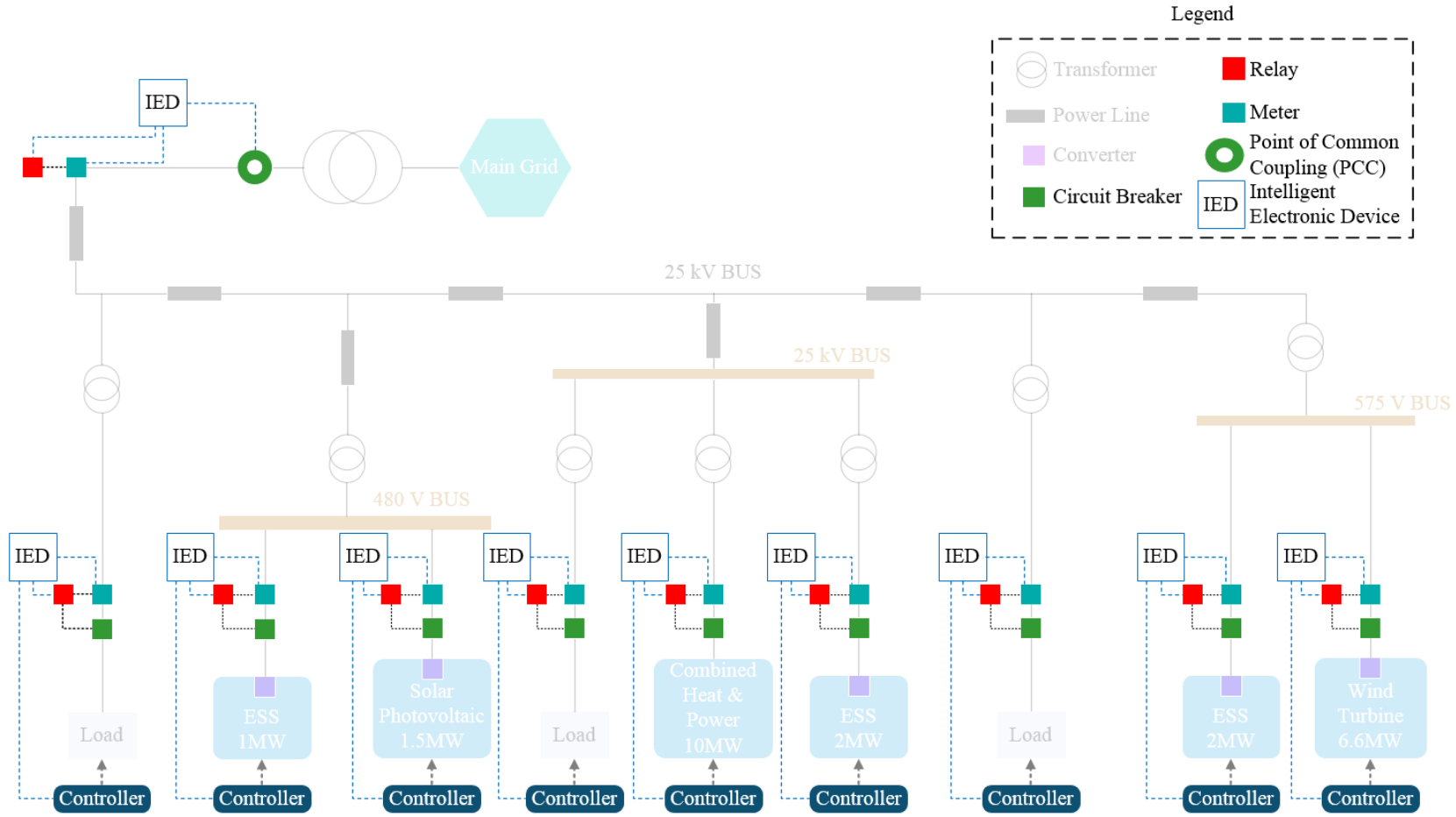

Figure 5.4: Placement of IEDs in microgrid benchmark

power shedding, and switching the operation mode setting for the microgrid devices. The various protection and control communications occurring in the benchmark are shown in Figure 5.5.

The MGCC sends power control reference value inputs to the ESSs in order to help stabilize the frequency of the shared microgrid bus at 60 Hz while the microgrid is in islanded mode. The frequency control performed by the MGCC is depicted in Figure 5.6. In order to perform frequency control, the microgrid frequency is transmitted to the MGCC periodically by the IED located near the PCC using IEC 104. When the frequency measurement is received, the MGCC determines the amount of deviation of the frequency from 60 Hz and provides the deviation to a Proportional Integral (PI) controller as input. The goal of the PI controller is to bring the system output, in this case the microgrid frequency, to a constant value. To achieve this, the PI controller maintains a numeral state, and updates its state based on inputs passed to it according to a $1/s$ integrator transfer function. In short, the current state of PI controller is equal to its previous state plus the product of the last frequency deviation input and the time elapsed since the last input was received. The state of the PI controller is then transmitted as output to the ESS controllers by the MGCC using IEC 104. The ESS controllers use this state as an input to the power control of the ESS alongside the input from the local feedback loop that reads the frequency deviation of the local power line for the ESS. The frequency control exerted by the MGCC described here is not used when the microgrid is in grid-connected mode, as the frequency in grid-connected mode is led by the main grid and the impact of the ESS power delivery on the microgrid frequency is minimal.

When the microgrid is in islanded mode, the MGCC performs load shedding as a protection measure when, despite the three ESS units delivering power at near-maximum capacity, the frequency of the microgrid drops too far below 60 Hz. Load shedding is done by having the setting for the amount of power consumed by the loads reduced dynamically through a signal sent by the MGCC. For the purposes of load shedding, the MGCC receives periodic frequency measurements of the shared bus by the IED near the PCC and periodic power output measurements from the IEDs tied to the ESSs. These measurements are transmitted using IEC 104 APDUs. While in islanded mode, If for over one second the microgrid frequency falls below 60 Hz by more than 5% and the ESS units are delivering over 90% of their maximum power delivery, then the MGCC sends a IEC 104 set command to each of the three loads to reduce their power consumption. The load

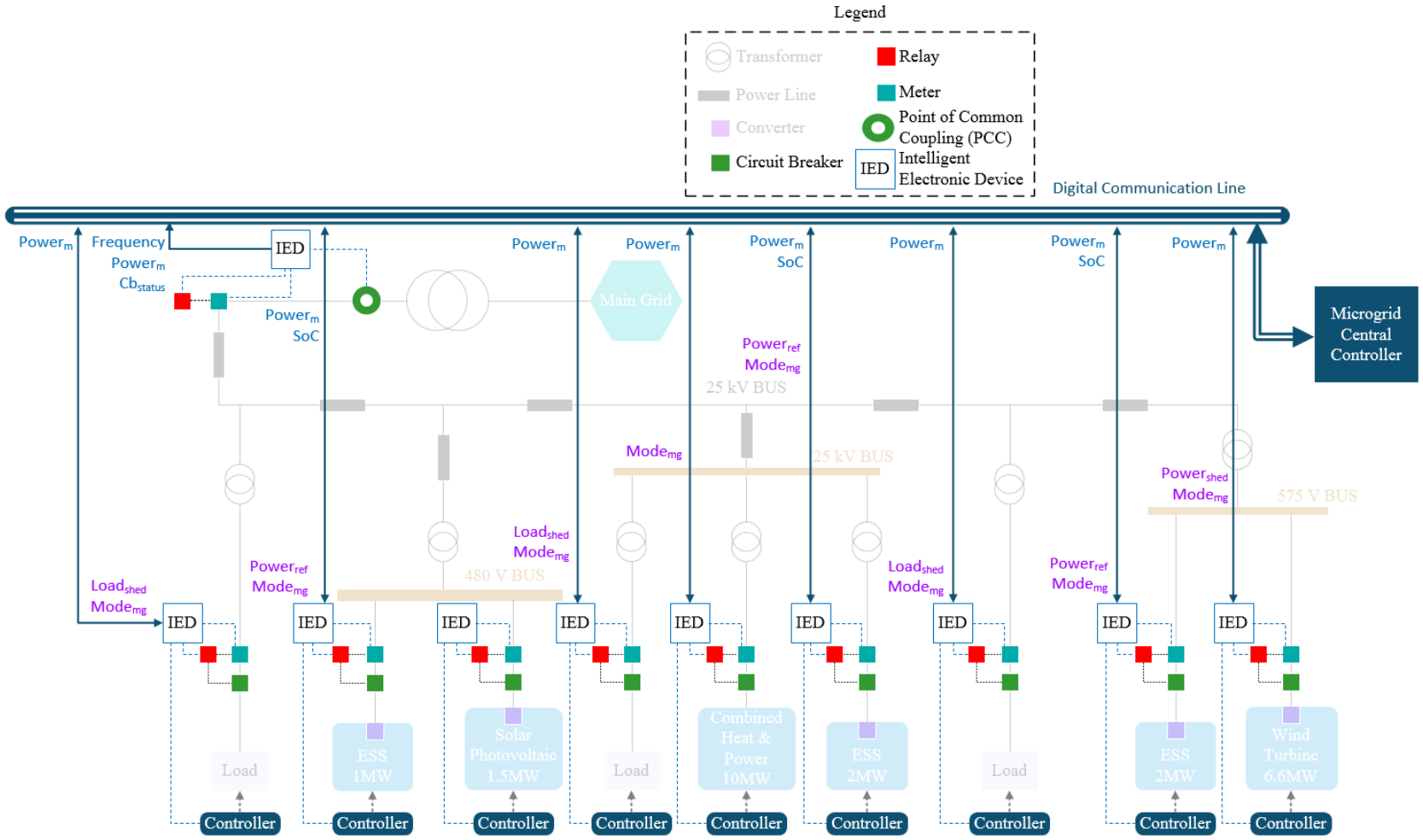

Figure 5.5: Protection and control communications between IEDs and MGCC

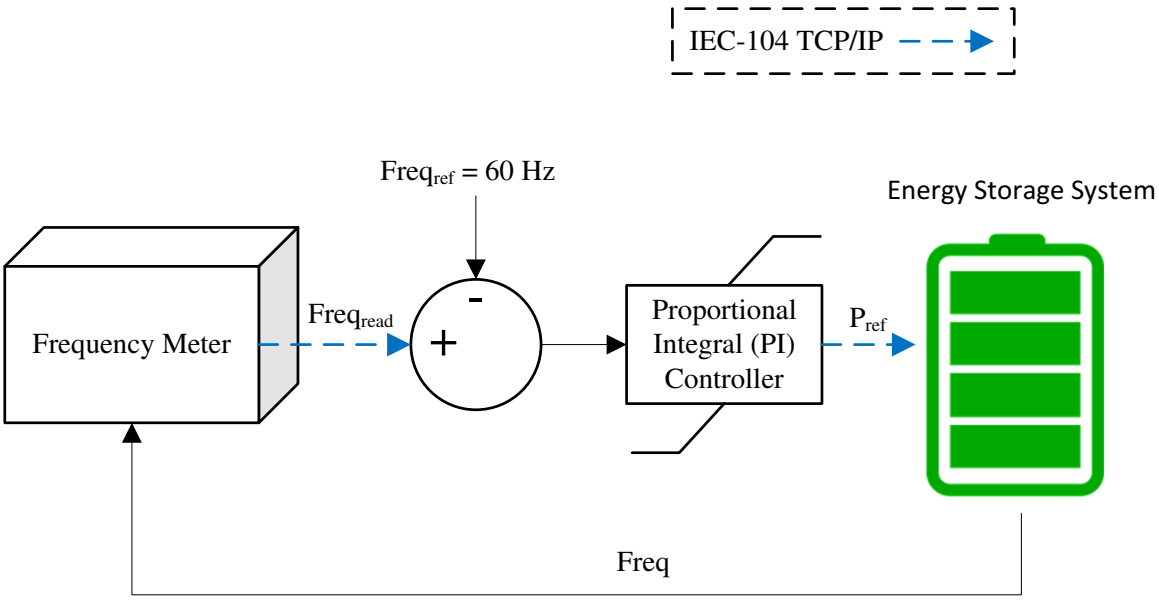

Figure 5.6: Frequency control performed by MGCC

shedding is done in incremental steps. If, after one second of sending a load shed command, the frequency is still too far below 60 Hz, then another load shed command is sent by the MGCC to reduce the load power consumption further. This is repeated until the frequency rises enough to pass the acceptable lower bound frequency of 5% below the nominal 60 Hz.

The strategy used for the power shedding protection function of the MGCC is similar to that of load shedding. The frequency measured by the IED near the PCC is once again used for determining the current frequency of the microgrid shared bus. The power output measurements of the IEDs at each ESS is used again as well. However, the condition that triggers power shedding differs from the one that triggers load shedding. If, while in islanded mode, the frequency of the shared bus deviates from 60 Hz by over 5% for over one second while the ESS units are required to absorb power despite being full, then the MGCC sends a trip command to open the circuit breaker connecting one of the three WTs to the microgrid. This essentially cuts down the power being delivered to the microgrid from the wind farm by one third. The trip command is transmitted to the IED stationed at the wind farm over IEC 104, which in turn takes the necessary action to forward the trip command to the circuit breaker of the WT to be disconnected.

The DERs and protection relays deployed across the microgrid generally do not have a direct

means of knowing when the microgrid has moved from grid-connected mode to islanded mode or vice-versa. Any change in the state of the PCC and hence the operation mode of the microgrid is reported to the MGCC by the IED monitoring the PCC, and it is through the MGCC that the rest of the microgrid receives the signal to change operation mode. When the state of the PCC changes, a IEC 104 APDU is transmitted to the MGCC containing a binary value representing the current state of the PCC. The MGCC in turn informs the rest of the microgrid if the new microgrid operation mode by sending an IEC 104 single point command APDU containing the binary value representing the new operation state to all the other IEDs. Upon receiving the update on the microgrid state, the IEDs switch the mode of the protection relays and DERs as appropriate. In particular, the CHP generator must be set to operate as the swing bus in islanded mode, where it becomes responsible for stabilizing the microgrid frequency through adjustment of its power output.

In grid-connected mode, the CHP generator moves to PV mode, where it generates constant active power and maintains a constant voltage magnitude. The amount of electric power passing through the PCC is also measured by the IED monitoring the PCC and reported to the MGCC. This measurement is relevant for potential peak shaving operations while the microgrid is in grid-connected mode to determine if an excessive amount of power is being delivered to or absorbed from the main grid. Should an excess be detected, the MGCC adjusts the power output references at the ESSs, lowering the power output if excess power is being delivered to the main grid and increasing the power output if an excess is absorbed from the main grid.

5.3.4 Implementation of IEC 60870-5-104 Outstation and Master Station

The IEC 104 outstations are simulated within the OPAL-RT Digital Real-time Simulator (DRTS) as IEC 104 slave devices. The OPAL-RT Digital Real-time Simulator (DRTS) comes with a driver for simulating IEC 104 slave devices. This driver allows for the creation of multiple IEC 104 slave devices capable of being simultaneously simulated. The inputs and outputs of the slave devices are mapped to inputs and outputs within the microgrid benchmark. For example, each slave device that manages a ESS has an information object address used as a power setpoint input from the master station. This input is fed into the ESS power control. A separate information object address is used as an output that passes the power currently being delivered or absorbed by the ESS to the

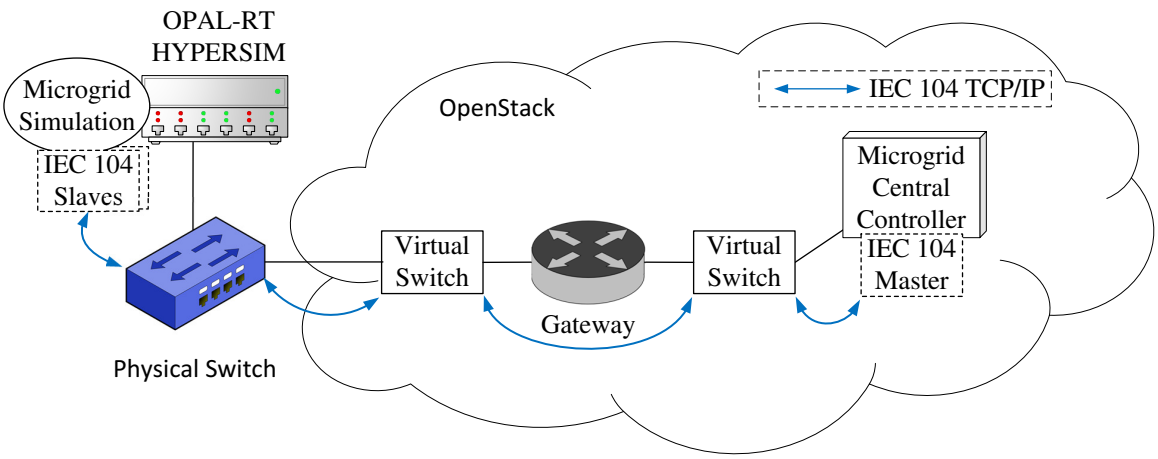

Figure 5.7: Deployment of microgrid simulation in co-simulation testbed

master station.

The master station is located in a separate VM within the OpenStack network. The VM runs an application that acts as the MGCC. The MGCC application is a custom application written in the C programming language for the purposes of this research and uses the open source lib68070 library. This library provides the functionality needed to open IEC 104 connections, send IEC 104 APDUs to outstations, and receive IEC 104 APDUs from outstations. The logic used to perform the microgrid secondary control level functions is written into the MGCC application, and is used to determine the appropriate messages to send to outstations in response to readings received from APDUs sent by the outstations simulated within the OPAL-RT DRTS. The arrangement of the IEC 104 slaves and MGCC when integrated in the co-simulation testbed is given in Figure 5.7.

5.4 Implementation of NSM Agent and NSM Manager

For this research, NSM agents are installed on proxy machines and must be able to report on the state and network traffic statistics of the devices they are assigned to monitor to a central NSM manager. This requires that the NSM agents are installed in such a way as to have visibility of the monitored device and have a network connection to the NSM manager. The NSM manager must be able to receive NSM data from multiple NSM agents simultaneously. The NSM agent

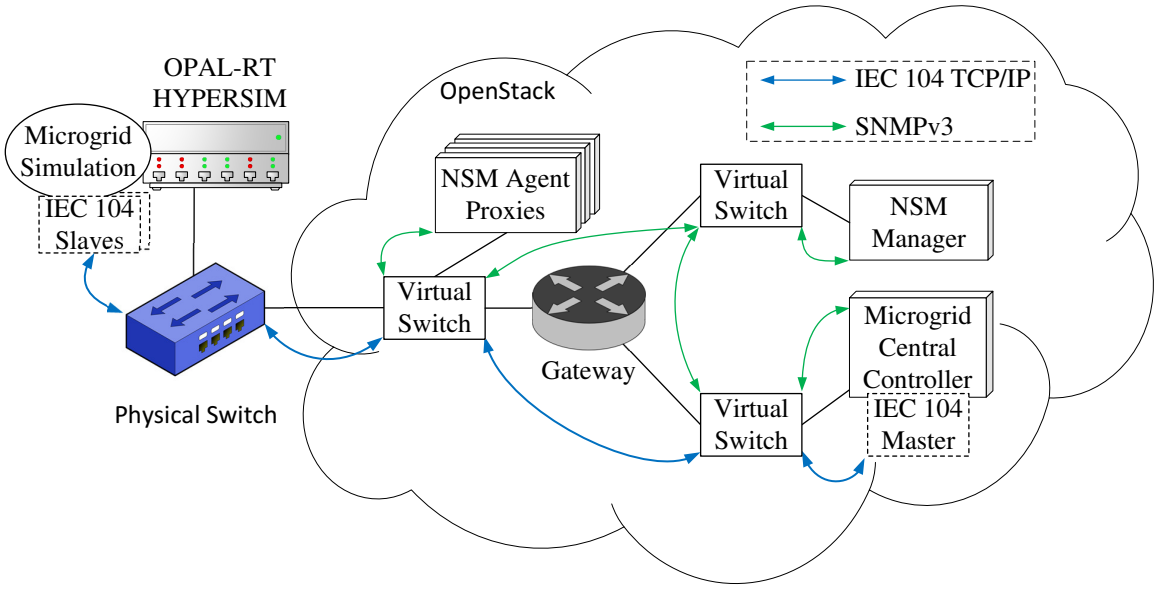

Figure 5.8: Deployment of NSM platform in microgrid testbed

proxy machines must have visibility of the network traffic travelling into and out of the DRTS simulating the microgrid and its communication network. A high-level view of the NSM platform when integrated into the microgrid testbed is presented in Figure 5.8.

5.4.1 NSM Agent

The NSM agent is deployed on an Ubuntu 16.04.4 Linux VMs within the OpenStack network. It uses SNMPv3 for the transmission of NSM data objects to the NSM manager deployed on OpenStack, with the NSM data objects being related to the monitored devices. The specific data objects communicated between the NSM agent and master are described in Section 4.7. The NSM agent responds to the periodic polling of the data objects by the NSM manager. In addition, the NSM agent can transmit unsolicited SNMPv3 *TRAP* messages containing a set of data objects to the NSM manager. The data objects are mapped to the corresponding MIB objects that are also defined in IEC 62351-7 and which are directly compatible with SNMP.

5.4.1.1 NSM Agent SNMP Application

The NSM agent has custom software designed to respond to the SNMP `GET` requests the agent receives from the master. This custom software is implemented as an extension of the NetSNMP software suite **[63]**. The version of NetSNMP used in this research is written in the C programming language and is deployable in Ubuntu Linux. The installation of NetSNMP allows the Linux machine to receive SNMP requests and respond with a SNMP response containing the requested information within a MIB object, or an error when appropriate.

NetSNMP supports SNMP, SNMPv2, and SNMPv3. The NSM agents are expected to only use SNMPv3 for communication with the NSM manager in order to protect against attacks on the integrity, authenticity, and confidentiality of transmitted SNMP messages. NetSNMP allows the use of MD5 or SHA to authenticate SNMPv3 messages and DES or AES for encryption of SNMPv3 messages. A shared key for authentication and one for encryption must be shared between the NSM agent and master in order for SNMPv3 messages to be transmitted between them and for them to be understood while making use of the SNMPv3 authentication and encryption features.

For this research, the SHA-256 hash function is used for SNMPv3 authentication and AES256 is used for SNMPv3 encryption. The NSM agents are initialized with a default user having a default SHA and AES password that the NSM manager uses to access the SNMP functions of the agent in order to create a new SNMPv3 user on the NSM agent with a unique authentication and encryption password known only by the agent and the manager. The default user is then deleted by the manager.

Upon initial installation, the NetSNMP software package by default supports the reporting of MIB objects from various SNMP MIB objects packaged with NetSNMP that are listed in the NetSNMP documentation **[64]**. This includes the execution of whatever functions are needed to retrieve the appropriate data requested over SNMP. The set of standard SNMP MIBs however does not include the MIBs defined in IEC 62351-7. Part of this research involved the writing of C language code that provides functionality to serve the required information for objects defined in the IEC 62351-7 MIBs for NSM. The custom code adding this functionality is compiled together with the NetSNMP software. The custom code is used to execute user defined actions upon receiving a

SNMP request for the IEC 62351-7 MIB objects that would be considered undefined and subsequently rejected by an unmodified NetSNMP. Specifically, this requires the defining of new handler functions to be executed upon receiving SNMP requests for IEC 62351-7 MIB objects.

Several MIB objects from the TCP and UDP MIBs packaged with NetSNMP were also considered relevant for the purposes of research on NSM data collection in microgrids. The default handler functions executed by NetSNMP upon receiving a request for these MIB objects was overwritten so that an NSM agent proxy machine installed with the modified NetSNMP application reports on the TCP and UDP statistics of its respective monitored device rather that the statistics related to its own communications. A brief description of the TCP and UDP MIB objects that are collected by the proposed NSM platform and whose respective NetSNMP response was modified is given in Section 4.7.2.

The custom SNMP software reads the value requested by a SNMP *GET* request from a source of data persistence on the proxy machine on which the software is installed and send those values as a SNMP response. The values saved to persistence for MIB object value reporting are determined through other applications and scripts running on the NSM agent proxy machine, with the values periodically being updated to reflect the current state of the monitored device.

The network traffic flowing into and out of the monitored device is made visible to the NSM agent proxy by having the proxy connected to the network switch used to reach the monitored device, with the traffic involving the monitored device being duplicated and forwarded to the proxy. The proxy being able to observe the traffic involving the monitored device enables the NSM agent on the proxy to report on several MIB objects involving statistics on network communication protocol usage such as TCP protocol messages and the IEC 104 protocol messages.

5.4.1.2 NSM Agent Data Persistence

The NSM agents require that the NSM data to report is persisted such that the data is not lost if the SNMP application is closed and re-opened. For this research, the Ubuntu Linux version of the SQLite database technology is used **[65]**. SQLite has the advantage of being a lightweight application compared to other database technologies, with the entire SQLite database being stored within a single file on disk. The MIB object values being saved to persistence are generally small in

size, and the NSM agent does not need to keep record of previous MIB object values. This means it is viable for the same database rows to simply be updated with the newest values, and thus the size of the database does not grow over time. The constant database size and low complexity of the data relationships makes the compact SQLite suitable for the purposes of data persistence in the NSM agent.

5.4.2 NSM Manager

Like the NSM agent, the NSM manager is deployed on a Ubuntu 16.04.4 Linux VMs within OpenStack. The NSM manager communicates with the NSM agents across the OpenStack network using SNMP, whose IP addresses are manually made known to the NSM manager in advance. The manager polls each agent for NSM data object information every 10 seconds, with the data object information being transmitted as MIB object values over SNMP. Specifically, the polling of NSM agents is done using SNMPv3, with the manager having set up a shared SNMPv3 authentication and encryption password with each agent. The authentication and encryption passwords are unique for each agent and are randomly generated as a 32 character string mixing uppercase, lowercase, and numerical digits.

5.4.2.1 NSM Manager SNMP Application

Unlike the NSM agent, the NSM manager does not require the installation of NetSNMP to fulfil its role in SNMP communication. The manager makes use of the *snmp* package available on Ubuntu Linux. This package allows the manager to make SNMP *GET* and *SET* requests over SNMPv3 as well as other SNMP requests like *GETNEXT*. The manager primarily uses these commands to create users with unique SNMPv3 authentication and encryption passwords on each agent.

For the purpose of polling the NSM agents periodically, the NSM manager makes use of the *pysnmp* Python library. The manager runs a Python script that periodically polls the agents for MIB object values over SNMPv3, with the polling rate being set at ten seconds. Once received, the MIB object values are saved to persistence in order to be later aggregated and analyzed for anomalies and intrusions.

The NSM manager is also capable of receiving SNMPv3 `TRAP` messages from NSM agents.

These are received through use of the *snmptrapd* package available on Ubuntu Linux. A separate Perl application called SNMP Trap Translator (SNMPTT) is used to register a handler function for received SNMP `TRAP` messages that fall within a specified filter **[66]**. Upon the manager receiving an SNMP `TRAP` message, the handler function whose filter recognizes the message is executed. In this research, the SNMPTT handler functions are responsible for persisting the MIB object data received from SNMPv3 traps into the manager's persistence for later analysis.

5.4.2.2 NSM Manager Data Persistence

The NSM manager uses Elasticsearch **[67]** to persist the collected NSM data objects transmitted by the NSM agents over SNMP as MIB object values. Elasticsearch is a search engine capable of generating a wide variety of statistics and searches on sets of data entered into it. It was chosen as a persistence technology due to its ability to provide adequate scalability for the volume of NSM data collected by the NSM manager while providing convenient search and data presentation features. Each agent is given its own Elasticsearch index in which MIB object values reported by the agent. The collected NSM data objects are then grouped within timestamped documents according to when they are received by the manager. These timestamped documents are considered as snapshots representing the full state of the monitored microgrid system within a short interval of time. The snapshots are pushed to Elasticsearch under an index that is separate from the NSM agents. The alerts generated by the anomaly detection module are also pushed to Elasticsearch, with a separate Elasticsearch index being used to store the alerts. The time between each snapshot creation is ten seconds, matches the MIB object polling rate.

The SNMPv3 authentication and encryption passwords used by the NSM manager to communicate with the NSM agents over SNMPv3 are also stored in persistence. These passwords are accessed every time the NSM manager sends a SNMPv3 request to an NSM agent as part of its NSM polling. MongoDB **[68]** is the persistence technology currently used to store these passwords. However, the storage size of the passwords is very small, therefore the constraints on alternate persistence technology that could have been chosen for storing these passwords are very minimal.

5.4.2.3 NSM Manager Data Analysis Application

The NSM manager has access to the Elasticsearch server deployed within the OpenStack network. NSM data object values collected from the NSM agents are inserted into Elasticsearch upon being received by the NSM manager.

Elasticsearch is capable of displaying data stored within its indexes through a data visualization tool called Kibana **[69]**. Kibana offers a customizable dashboard that allows data within Elasticsearch to be cleanly visualized, providing options for data filters and the toggling of visible fields. Because of these features, Kibana can act as a means for a human operator to have a clear view on the current state of the microgrid as well as a way to make security alerts concerning the microgrid readily visible. This research makes use of a customized Kibana dashboard to read the alerts generated through analysis of the collected NSM data. Figure 5.9 and Figure 5.10 give an example of how a Kibana dashboard can present alert information based on data collected during an attack against the microgrid, with both figures presenting the same set of alerts. Figure 5.9 shows the distribution of alerts across each monitored microgrid device and gives the number of alerts generated for each particular MIB object. Figure 5.10 shows the histogram of all alerts generated within a given time period, with the red bars indicating the absolute number of each alert and the pink bars indicating the number of unique MIB objects that have generated an alert. Note that the set of alerts presented in these figures is not associated with any particular attack and was generated purely to demonstrate the dashboard.

5.4.3 Implementation of Anomaly Detection Module

The anomaly detection module is composed of a prediction model for the microgrid NSM data object values, a custom learning application to build the prediction model, and a custom prediction application that uses LSTM to compare the real-time MIB object values within the snapshots saved in Elasticsearch to predictions based on the prediction model. The learning and prediction application have specified features which are to be observed to determine if an alert should be generated. These features include rules that result in an alert being generated if broken and relations between MIB object values, for example the difference between two MIB object values, that result in an alert

being generated if it deviates significantly from the predicted value based on the prediction model. The alerts are pushed to Elasticsearch so that they can be viewed in Kibana.

The learning and prediction applications are written through a joint effort by Dr. Rachid Hadjidj, Mr. Abdullah Albarakati, and Ms. Chantale Robillard.

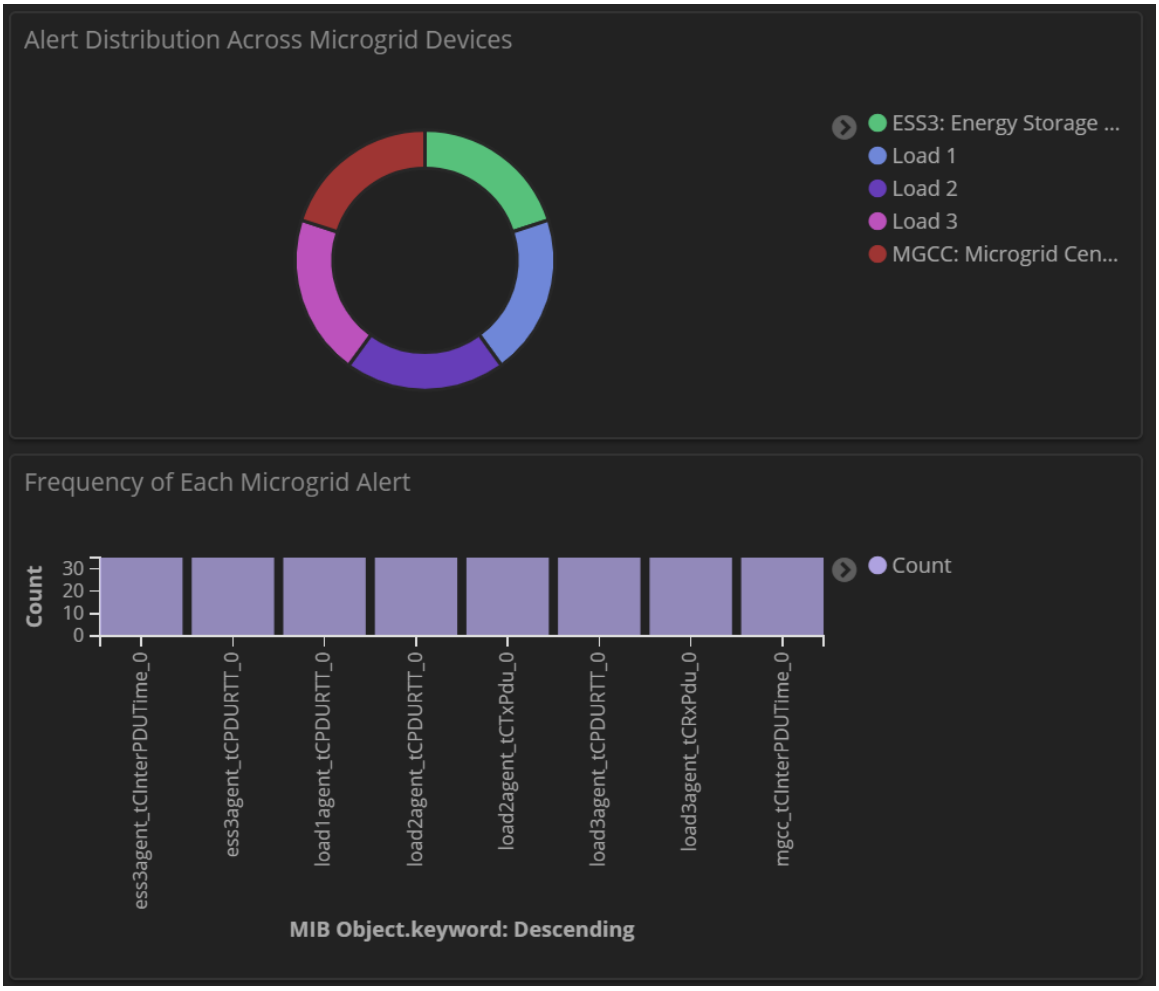

Figure 5.9: Example of attack alerts

5.5 Attack Scenarios

From the attack scenarios described in 4.9.2 that result in invariant violations, a subset of the attack scenarios are chosen for launching on the microgrid testbed. The attack scenarios are launched

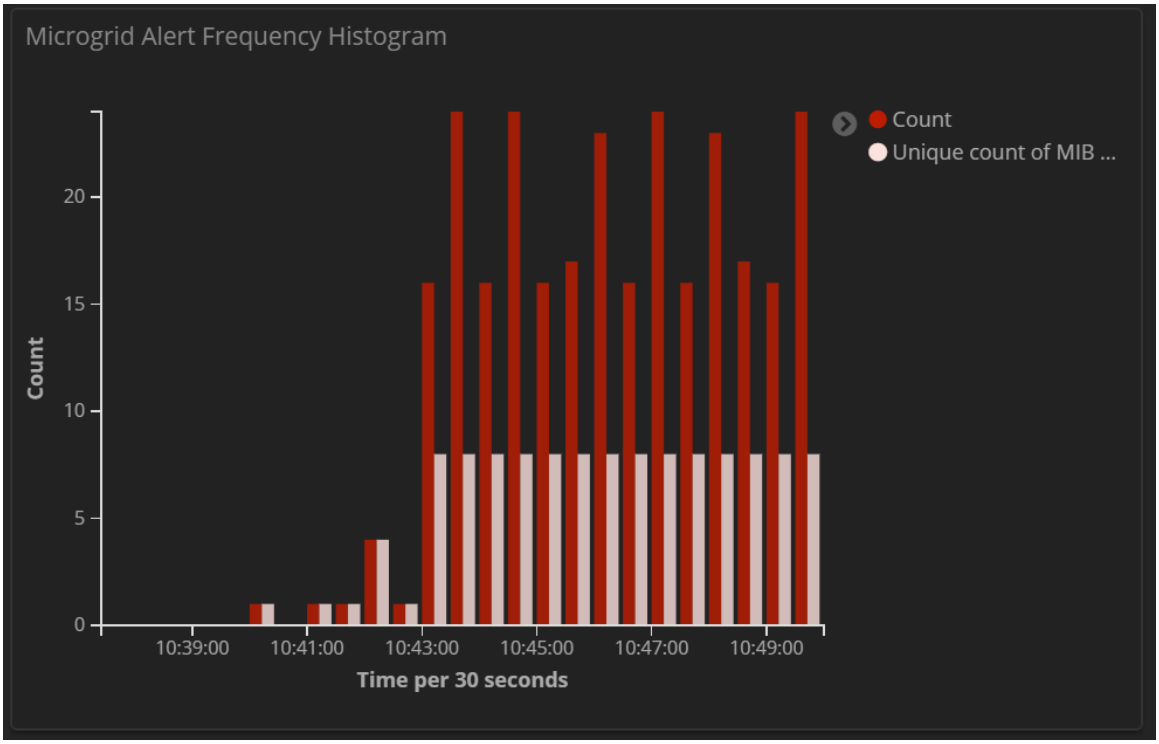

Figure 5.10: Time series of attack alerts

in order to evaluate the effectiveness of the attack and the effectiveness of the NSM platform at detecting the attack. The violation of certain invariants was not pursued for practical reasons. In particular, the invariants related to incorrect cause of transmission and the test flag are excluded, as the effect this has on the IEC 104 application received the affected APDU depends on the implementation details of the application. In addition, invariants related to changing of ASDU address are excluded because in the testbed each ASDU address is mapped to a unique IP address and so an effective version of this attack would also spoof the associated IP. IP address spoofing is a relevant security concern as well but is currently out of scope for the experimental evaluation considered.

Some of the the messages involving the simulated microgrid that are most likely to lead to losses in reliability, stability, and efficiency if attacked include the following: 1) reference value set commands for ESS power output 2) the status of the PCC breaker indicating whether it is open or closed 3) frequency and power measurement values from the PCC outstation. These messages are attractive targets for an attacker who wishes to disrupt microgrid operations and who has compromised

the communication network.

Some invariant violations are separated into multiple attack scenarios that target different kinds of information carried within the targeted APDU. There may also be different basic actions that can be used to violate the same invariant. Each of the chosen attacks scenarios are limited to targeting only one IEC 104 connection, but the attacked connection can differ between scenarios. The list of attack scenarios launched on the testbed for evaluation is described in Table 5.1.

Attack #	**Targeted Invariant Violation**	**Targeted Information**	**Basic Cyberattack**
1a	Invalid header byte	Reference values	Modify
1b	Invalid header byte	Circuit breaker status	Modify
2	Invalid APDU length	Circuit breaker status	Modify
3	Invalid information object count	Frequency and power measurement values	Modify
4	Wrong sequence number	Frequency measurement values	Modify
5a	Wrong type	Circuit breaker status	Modify
5b	Wrong type	Frequency measurement values	Modify
6	Incorrect object address	Frequency and power measurement values	Modify
7a	Incorrect object value	Circuit breaker status	Modify
7b	Incorrect object value	Circuit breaker status	Inject
7c	Incorrect object value	Frequency measurement values	Modify
8	Unconfirmed connection	Reference and measurement values	Drop
9	Unacknowledged message chain	Reference and measurement values	Drop

Table 5.1: List of attack scenarios

5.5.1 Attack Impacts

Instead of communicating directly through the OpenStack network, the MGCC connects to the microgrid slave devices simulated in OPAL-RT through an intermediary VM in the network that forwards the TCP traffic sent by the MGCC to the slaves and vice versa. It is on this intermediary VM forwarder that the application responsible for launching attacks is deployed. The attack application on this forwarder acts as a MitM, forwarding traffic to its intended destination but having the capability to modify, delay, or drop packets it receives instead of forwarding them normally while also being able to fabricate packets to send to the master station or outstations. The deployment of the forwarder within the co-simulation testbed that runs the attack application is shown in Figure 5.11. Should a IEC 104 connection be lost or fail to be established, the MGCC will make another attempt to establish a IEC 104 connection with the disconnected outstation four seconds after the connection fails.

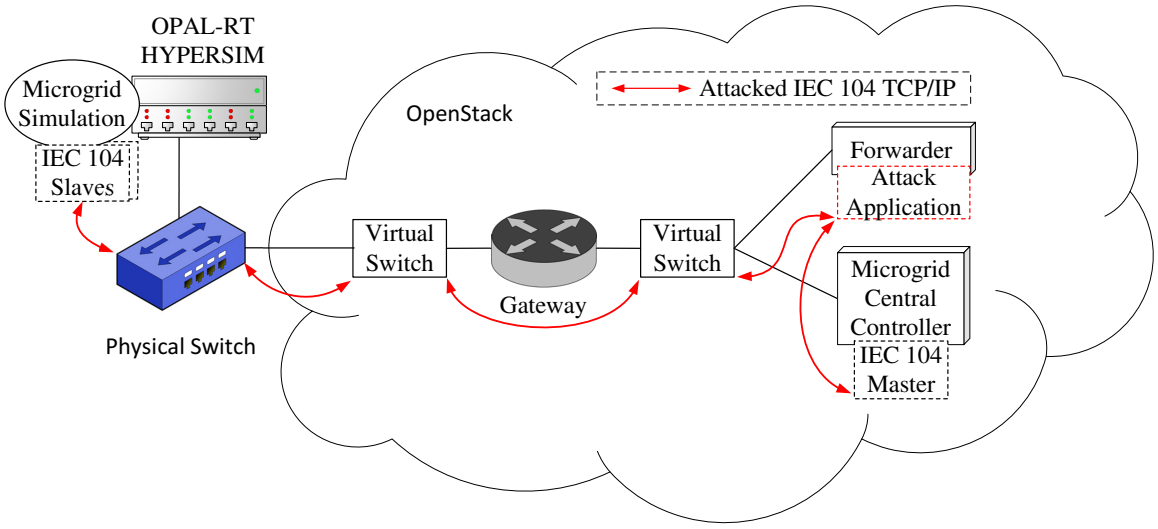

Figure 5.11: Setup of attacker component in microgrid testbed

The attack application is controlled through a web interface that is linked to back-end scripts. The scripts are written in Python, and are responsible for managing the MitM connection between the MGCC and the outstations as well as performing the appropriate packet manipulations depending on the attack chosen through the web interface. The web interface is shown in Figure 5.12.

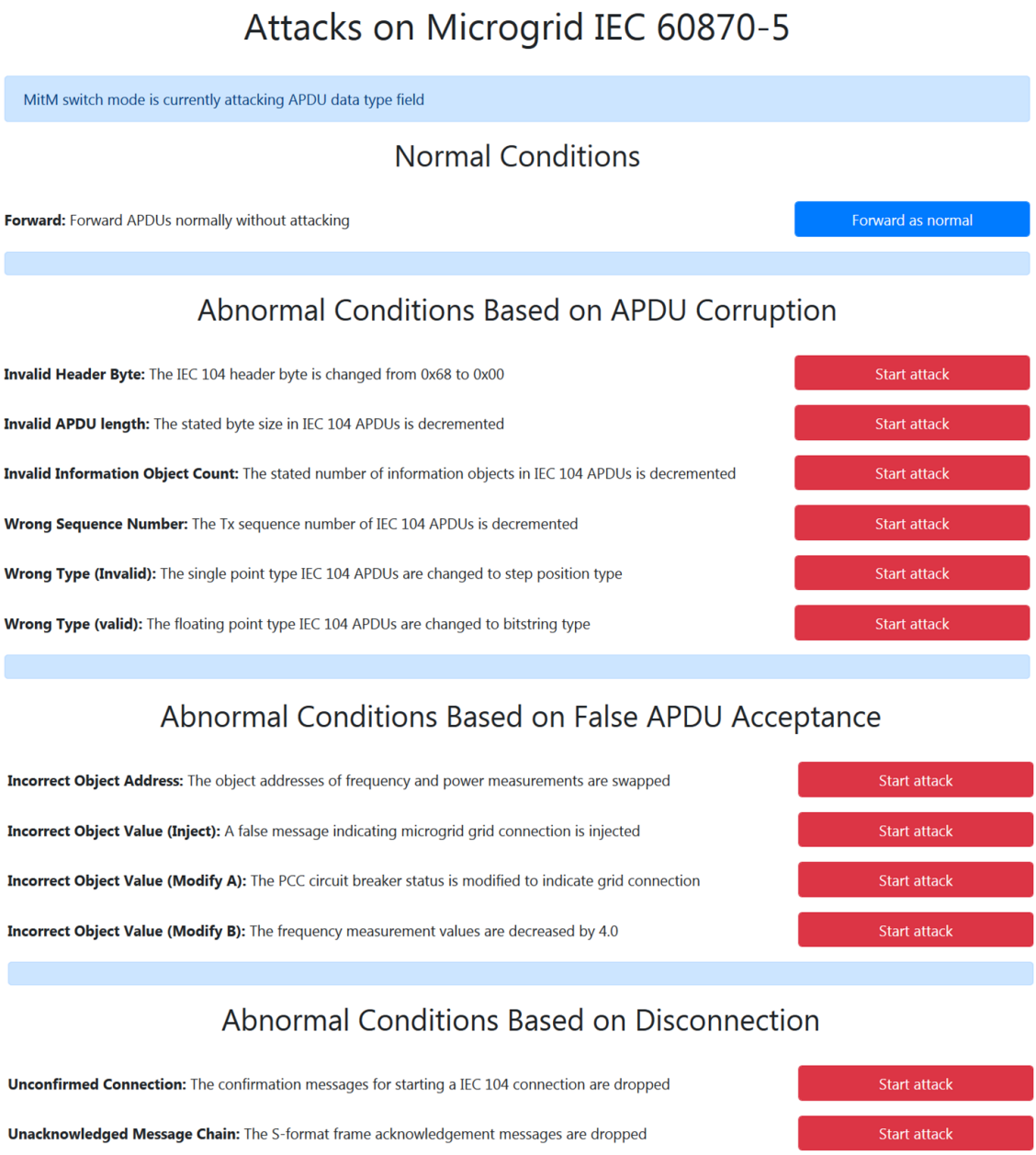

Figure 5.12: The web interface used to launch attacks

The scope of the experiments are limited in that they are all launched against an initial microgrid state where the microgrid has stabilized in islanded mode. Additionally, the MGCC sends an interrogation command to all outstations to be updated on the current state of all information objects every 20 seconds while the microgrid has stabilized. Creating a model of normal behaviour for the microgrid that transitions between grid-connected mode and islanded mode is complex because the behaviour of the microgrid network traffic changes depending on the microgrid operation mode and the transition period between the two modes also exhibits its own traffic behaviour. By only considering the operation of the microgrid in islanded mode, a much more consistent model of normal behaviour for the microgrid is established for comparison with the behaviour of the system while under attack.

When in islanded mode, the normal operation of the simulated microgrid results in a stable state where the loads absorbing a roughly constant amount of power. As for the DERs, the wind farm generates a nearly constant amount of power, while the power generated by the ESSs and the CHP changes gradually. However, the net power generated by the ESSs and CHP under normal conditions tends towards a constant value. The power balance and frequency of the simulated microgrid when in islanded mode and under normal conditions are shown in Figures 5.13 (a) and (b), respectively.

The attacks scenarios are all launched after the simulated microgrid reaches the stable state shown in Figure 5.13. Below are details on the steps used to launch the chosen attack scenarios against the microgrid testbed as well as their impact on the microgrid simulation.

1a) **Invalid header byte (reference values modification)**

In this attack, the transmission of the power output reference values sent to one of the ESSs by the MGCC for frequency control is disrupted by periodically modifying the first byte of a transmitted APDU from `0x68` to `0x00`.

Upon receiving the incorrect header byte for a APDU, the IEC 104 station recognizes the APDU as an error packet. This results in the IEC 104 connection used to transmit the reference values needing to be reset, even though the APDU can still be parsed otherwise. Once the connection is re-established, the transmission of reference values can resume as normal. If the attack is performed continuously, the downtime until the connection is reset

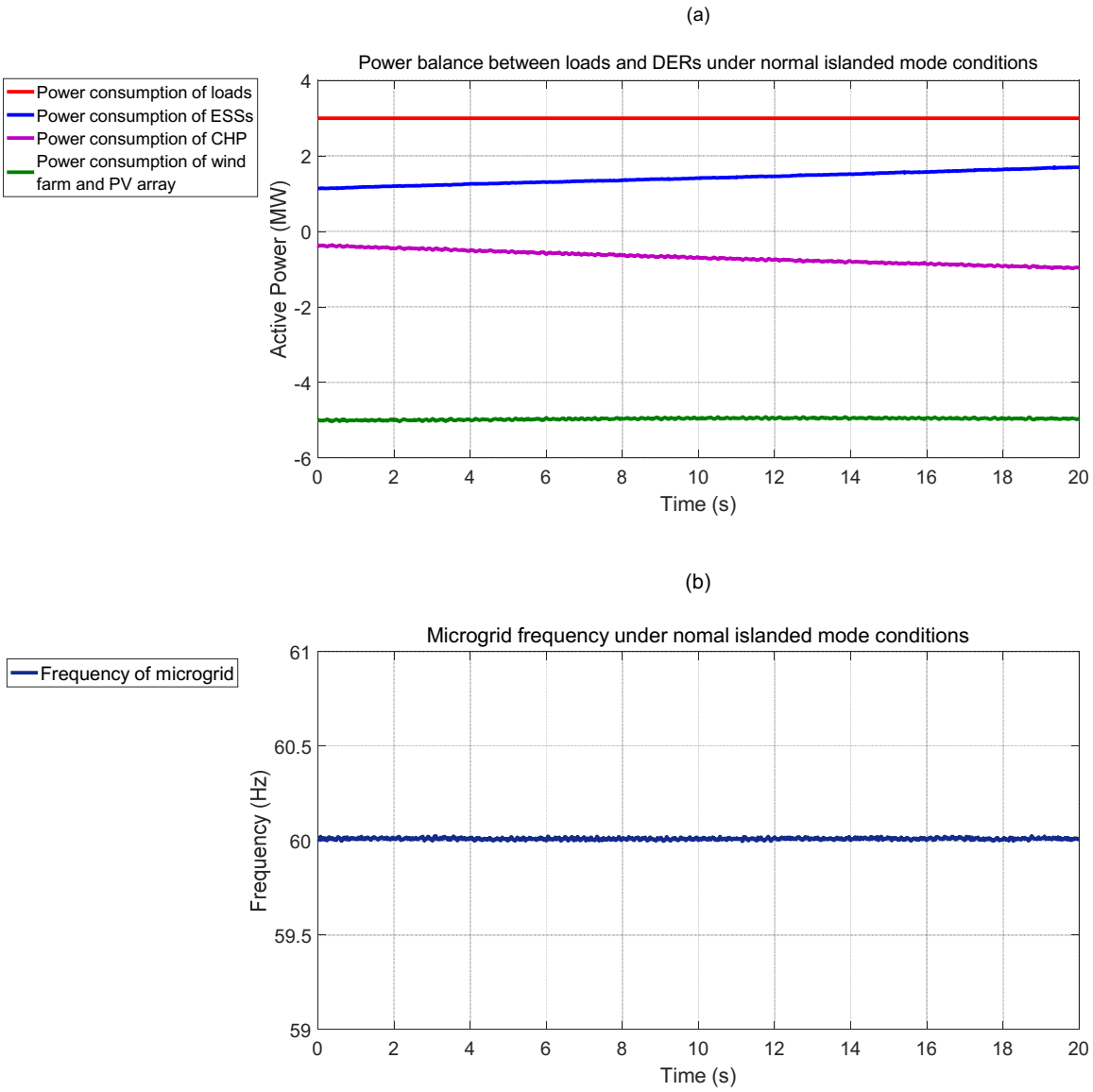

Figure 5.13: Microgrid power balance and frequency under normal conditions

will prevent the ESS from properly being controlled through reference values and the attack results in DoS against the MGCC frequency control.

1b) **Invalid header byte (circuit breaker status modification)**

In this attack, the state of the PCC circuit breaker, which connects the microgrid to the main grid, being reported to the MGCC is disrupted by modifying the first byte of the circuit breaker

status APDU from `0x68` to `0x00`.

Upon receiving the incorrect header byte for a APDU, the IEC 104 station recognizes the APDU as an error packet. This results in the IEC 104 connection used to transmit the circuit breaker status and frequency needing to be reset. If the attack is performed continuously, the downtime until the connection is reset will prevent the MGCC from reading the circuit breaker status and the microgrid frequency, both of which are sent by the same outstation. This disables the control of the ESSs power reference values from the MGCC and the attack results in DoS against the MGCC frequency control.

2 **Invalid APDU length (circuit breaker status modification)**

In this attack, the value of the APDU length field in a PCC circuit breaker status APDU is decremented through packet modification so that it no longer matches the true length of the APDU.

Upon receiving the circuit breaker APDU with the incorrect length, the MGCC recognizes the APDU as an error packet. As in Attack 1b, this results in the IEC 104 connection used to transmit the circuit breaker status and frequency needing to be reset in order to read those measurements and perform frequency control.

3 **Invalid information object count (measurement values modification)**

In this attack, the value of the information object count field in a APDU sent from the PCC outstation reporting on circuit breaker status and microgrid frequency is decremented through packet modification. This is only done when the breaker status and frequency are reported in the same packet resulting in an APDU with at least two information objects.

Upon receiving the APDU with the incorrect information object count, the MGCC recognizes the APDU as an error packet, however the IEC 104 connection remains open. The information objects beyond the number stated in the attacked packet are not parsed. In the simulated microgrid, the interrogation command sent to the outstation responsible for the circuit breaker and measurement devices near the PCC produces a response APDU from the outstation that includes information objects for both the circuit breaker state and the amount

of power passing through the PCC. The attack on the information object count field causes the MGCC to not parse the power measurement sent as a response to the interrogation commands.

4 **Wrong sequence number (measurement values modification)**

In this attack, the Tx sequence number of a frequency measurement value APDU is decremented by one through packet modification, matching the Tx sequence number of a previously received I-format APDU.

Upon receiving the APDU with an already used Tx number, the MGCC does not parse any information object values in the APDU. As in Attack 1b, the IEC 104 connection must be reset in order to resume reading the circuit breaker status and the frequency measurements used to perform frequency control.

5a **Wrong Type (circuit breaker status modification)**

In this attack, the Type ID field in the ASDU of a PCC circuit breaker status APDU is modified from the single point information type (`M_SP_NA_1`: 1) to the step position information type (`M_ST_NA_1`: 5), which has a different expected size for the information object values.

Due to the expected size of the single point type values differing from the step position type values, the MGCC recognizes the modified APDU as an error packet and fails to parse the circuit breaker status. As in Attack 1b, the IEC 104 connection must be reset in order to resume reading the circuit breaker status and the frequency measurements used to perform frequency control.

5b **Wrong Type (measurement values modification)**

In this attack, the Type ID field in the ASDU of a frequency measurement value APDU is modified from the (timestamped) short floating point type (`M_ME_TF_1`: 36) to the 32-bit (timestamped) string type (`M_BO_TA_1`: 8). Unlike in Attack 5a, the new data type has the same expected size for the information object values as the original type.

Because the expected size of the short floating point type values is the same as the size of the bitstring (32 bits) type values, the MGCC does not recognize the modified APDU as an error packet and parses the frequency measurement value as a bit string instead of a

floating point. This does not result in the connection being reset. The collection of frequency measurements resumes as normal unless the attack is repeated continuously, in which case frequency control will cease because the frequency measurements required to perform such control will never be parsed by the MGCC.

6 **Incorrect object address (measurement values / modification)**

In this attack, the packets sent by the outstation near the PCC that contain information objects for both the frequency of the microgrid and the power delivery through the PCC, in kW, within the same APDU are modified so that the IOA field values for those two information objects are swapped. The power measurement, being near zero while the microgrid is in islanded mode, is interpreted as the frequency measurement in Hz and vice versa. This attack, once started, is performed continuously to modify every such packet. This attack is possible because both the frequency measurement and the power measurement share the same type of short floating point, and so end up being reported within the same APDU by the outstation.

This attack results in the MGCC believing that the frequency of the microgrid is near zero. This causes the MGCC to send power output reference values to the ESSs that increase their power output. As the frequency is consistently reported as being near zero due to the IOA field value swapping, the ESSs are eventually set to their maximum output, which is perceived by the MGCC through the power measurements sent to the MGCC by the outstations responsible for the ESSs. The MGCC, believing that the microgrid system is still experiencing underfrequency even when the ESSs are delivering the maximum amount of power, performs load shedding operations to reduce the total power consumption of the loads. At the same time, the increased power output of the ESSs causes power imbalance resulting in an elevated microgrid frequency and microgrid instability. The impact of this attack on the power balance between the loads and DERs is shown in Figure 5.14 (a), while the impact on the microgrid frequency is shown in Figure 5.14 (b).

7a **Incorrect object value (circuit breaker status / modification)**

In this attack, the value of the information object in the PCC circuit breaker status APDUs that represent the status of the circuit breaker connecting the microgrid to the main grid is modified

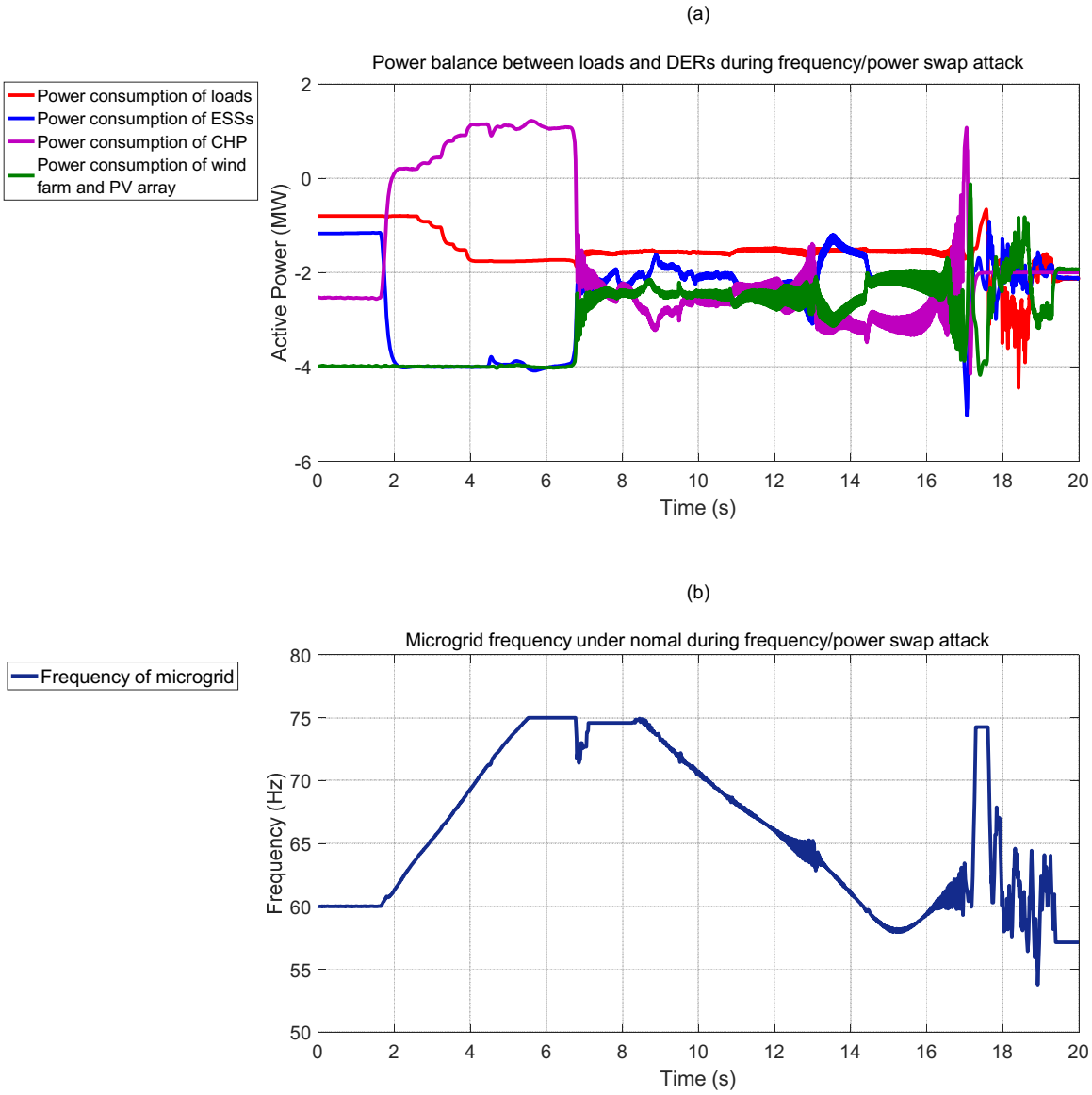

Figure 5.14: Impact of Attack #6 on microgrid power balance and frequency

to the value that indicates the circuit breaker is closed and hence that the microgrid should be operating in grid-connected mode. This attack, once started, is performed continuously to modify every such packet, including the ones sent as a response to interrogation commands from the MGCC. To make it more convincing in a real scenario, the attack can be paired with modifications to the power measurements at the PCC so that the measurements are more typical of grid-connected mode operations, but this step was omitted for simplicity.

This attack results in the MGCC believing that the microgrid is currently connected to the main grid and therefore should operate in grid-connected mode. Frequency control through the sending of power output reference values to the ESSs is not meant to be performed in grid-connected mode, and so frequency control from the MGCC is disabled even though the microgrid is in fact in islanded mode.

7b **Incorrect object value (circuit breaker status / injection)**

In this attack, the APDUs sent to the MGCC from the outstation responsible for frequency measurement and PCC circuit breaker status reporting are read to keep track of the most recent Tx sequence number. During operations, a PCC circuit breaker statusAPDU is fabricated and sent to the MGCC which indicates that the PCC circuit breaker is open and which has the proper Tx sequence number to be accepted by the MGCC. It should be noted that this attack does not require a MitM setup to be launched, and only requires an attacker who can read the network traffic and inject packets into the network.

This attack results in the MGCC believing that the microgrid is currently connected to the main grid and therefore should operate in grid-connected mode upon initially receiving the fabricated APDU. However, the next APDU to arrive will contain the Tx sequence number matching that of the fabricated packet, causing the IEC 104 connection to close similar to Attack 4. Once the connection is re-established, the transmissions from the PCC outstation can resume as normal and the proper circuit breaker status read to have the MGCC return to islanded mode operation. If the injection attack is performed continuously, the downtime until the connection is reset will result in DoS against the MGCC frequency control.

7c **Incorrect object value (measurement values / modification)**

In this attack, the values of the information object in the microgrid frequency APDU that corresponds to the frequency of the shared microgrid bus is modified before it reaches the MGCC so that it is equal to the original value minus 4.0. This attack, once started, is performed continuously to modify every such packet.

This attack causes the MGCC believing the microgrid frequency is 4 Hz lower than it actually is, resulting in the power output reference values sent to the ESSs pushing the microgrid to stabilize at a frequency of 64 Hz rather than 60 Hz. The MGCC will not be able to detect the overfrequency of the microgrid due to the ongoing attack, and therefore will not trigger load shedding in the microgrid even though the frequency has exceeded to allowable 5% deviation from 60 Hz in islanded mode. The impact of this attack on the microgrid frequency is shown in Figure 5.15 (b). Its impact on the power balance is shown in Figure 5.15 (a).

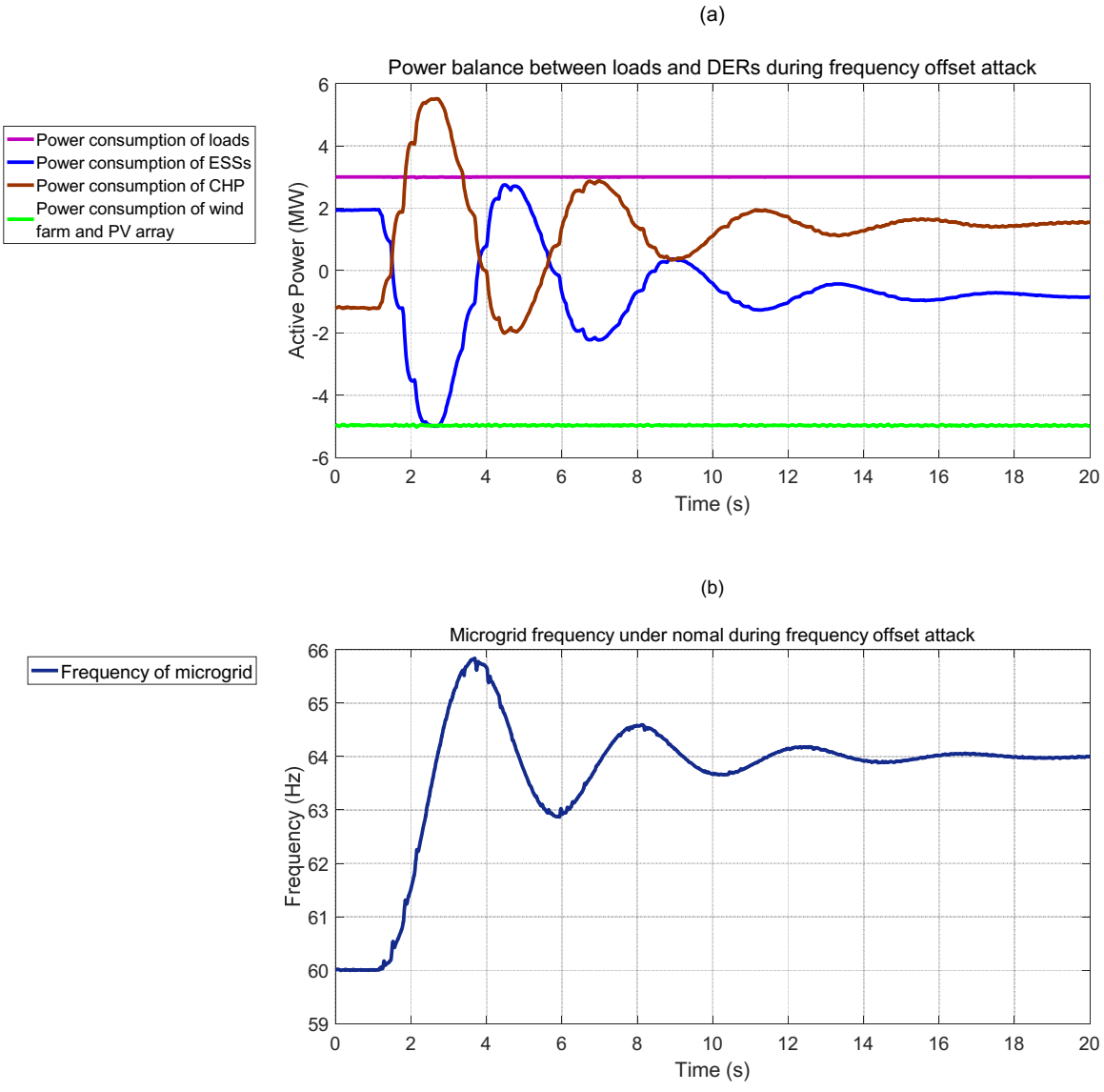

Figure 5.15: Impact of Attack #7c on microgrid power balance and frequency

8 **Unconfirmed Connection (measurement and reference values / drop)**

In this attack, the `STARTDT_con` messages sent by the outstation responsible for one of the ESSs to confirm the establishment of a IEC 104 connection with the master station are dropped. This attack, once started, is performed continuously to drop every subsequent `STARTDT_con` message sent by the targeted outstation.

This attack prevents the MGCC from ever accepting or responding to IEC 104 APDUs sent by the targeted ESS outstation. The MGCC will constantly reattempt to establish a IEC 104 connection with the outstation every four seconds. However, the attack prevents the connection attempt from ever being successful and communication with the ESS is lost. This results in DoS against the MGCC frequency control.

9 **Unacknowledged message chain (measurement and reference values / drop)**

In this attack, the S-format frame APDUs sent between the MGCC and the outstation responsible for one of the ESSs to acknowledge extended message chains are dropped. This attack, once started, is run continuously to drop every subsequent S-format frame APDU sent between the targeted outstation and the MGCC.

Contrary to expectation, the prevention of S-format APDUs from ever being received did not stop the MGCC or the outstations from operating as normal. The outstations and MGCC continued to transmit and respond to IEC 104 APDUs even without acknowledgment from S-format frame APDU.

5.6 Monitored MIB Objects for Detecting Attacks

The attack scenarios discussed in Section 5.5 rely on taking control over the communication link between the master station MGCC and the outstations responsible for the various microgrid elements in order to impact the IEC 104 messages transmitted over TCP. While attacks are being launched against the simulated microgrid, IEC 62351-7 NSM data object information is transmitted over SNMPv3 to the NSM manager using the MIB objects defined by IEC 62351-7. The collected MIB object values corresponding to IEC 62351-7 NSM data objects are listed in Table 5.2 are

transmitted to the NSM manager over SNMPv3 as MIB objects. Some MIB objects for TCP communication that are standard to SNMPv3 are also relevant to the attack scenarios given that IEC 104 makes use of TCP. The relevant TCP MIBs objects monitored by the NSM manager are described in Table 5.3. The MIB objects corresponding to IEC 62351-7 NSM data objects and TCP traffic statistics are used for intrusion detection through a combination of specifying constraints that must be upheld and by including some of the data in a prediction model for the LSTM detection tool. The prediction model is also able to capture relations between the MIB object values. The prediction model used in this research also includes the difference between the IEC 104 packets transmitted by the MGCC and the packets received collectively by the outstations and vice versa.

NSM data object	**Description**	Detection strategy
tCInErrCnt	Number of IEC 104 packets received in error	Rule-based
tCInterPDUTime	Average time between received APDU	LSTM
tCOutErr	Number of IEC 104 transmitted in error	Rule-based
tCPDURTT	Average IEC 104 packet round trip time	LSTM
tCPDUSizeFail	Number of IEC 104 packets with wrong length	Rule-based
tCRtxCnt	Number of retransmitted IEC 104 packets	LSTM
tCRxPdu	Number of IEC 104 packets received	LSTM
tCRxCritical	Number of critical IEC 104 packets received	LSTM
tCRxUnsolicitedReq	Number of unsolicited IEC 104 packets received	LSTM
tCTxPdu	Number of IEC 104 packets transmitted	LSTM
tCTxCritical	Number of critical IEC 104 packets transmitted	LSTM
tCTxUnsolicitedReq	Number of unsolicited IEC 104 packets transmitted	LSTM

Table 5.2: Monitored IEC 62351-7:2017 NSM data objects

5.7 Experimental Results

The chosen attacks described in Section 5.5 were launched against the simulated microgrid while the NSM platform was operational. The average time taken for the NSM platform to generate an alert based on the collected MIB object data, as well as the MIB objects generating the alerts, are

TCP MIB object	**Description**	Detection strategy
tcpInSegs	Number of TCP segments received	LSTM
tcpOutSegs	Number of TCP segments transmitted	LSTM
tcpRetransSegs	Number of retransmitted TCP segments	LSTM
tcpOutRsts	Number of TCP segments with the RST (reset) flag set to 1	Rule-based
tcpInErrs	Number of TCP segments received in error	Rule-based
tcpActiveOpens	Number of TCP connections opened from the closed state	LSTM

Table 5.3: Monitored TCP MIB objects

given in Table 5.4.

The attacks that cause packet errors (Attack #1, #2, #3, #5a) can be detection consistently with the InErrCnt NSM data object that counts IEC 104 packet errors. This is because any changes to that value are rare enough under normal scenarios that the number of false positives if alerts are generated on any change would be relatively small. Attacks that cause a IEC 104 TCP connection to be closed (Attack #1, #2, #3, #5a, #7b, #8) tend to generate a TCP reset packet, which can be detected by the tcpOutRsts data object. This does not appear to be a reliable method of detecting connection drops, as Attack #4 and Attack #7b were sometimes able to close the connection without a TCP reset packet being detected through NSM. However, a connection being brought down repeatedly would likely trigger an alert based on the packet rate for IEC 104 or TCP packets even if TCP reset packets are not generated. This is seen with Attack #8, where the connection is down for an extended period of time. It is also worth noting that monitoring of packet rates does not help detect the injection of a single packet in Attack #7b, likely due to the LSTM not being able to distinguish the injection of a single packet from noise present in the packet transmission rate.

Attack #5b does not cause alerts to be generated by the NSM platform and is therefore not detected. This is because the attack is not launched continuously to the point where indirect impact on the microgrid network communications can be observed. Were the attack performed continuously, the lack of reference value transmissions would be detected by NSM. The NSM platform does not monitor application errors or exceptions in regards to the parsing or processing of APDUs by the

Attack #	Attacked Data	Attacks Detected	Average Alert Time	MIB Object Generating Alert
1a	Reference values	10/10	24.688s	MGCC:tCInErrCnt MGCC:tCInterPDUTime
1b	Circuit breaker status	10/10	29.667s	MGCC:tCInErrCnt
2	Circuit breaker status	10/10	31.600s	MGCC:tCInErrCnt MGCC:tCPDUSizeFail ESS1:tCInterPDUTime
3	Frequency and power measurement values	10/10	24.138s	MGCC:tCInErrCnt
4	Frequency measurement values	6/10	24.676s	MGCC:tcpOutRsts
5a	Circuit breaker status	10/10	25.763s	MGCC:tcpOutRsts
5b	Frequency measurement values	0/10	N/A	N/A
6	Frequency and power measurement values	5/5	32.979s	Load1:tCRxPdu Load2:tCRxPdu Load3:tCRxPdu
7a	Circuit breaker status	5/5	28.390s	ESS1:tCInterPDUTime ESS2:tCInterPDUTime ESS3:tCInterPDUTime MGCC:tCInterPDUTime
7b	Circuit breaker status	8/10	29.584s	MGCC:tcpOutRsts
7c	Frequency and power measurement values	0/10	N/A	N/A
8	Reference and measurement values	10/10	27.414s	MGCC:tcpOutRsts MGCC:tCInterPDUTime ESS1: tcpOutRsts ESS1:tCInterPDUTime
9	Reference and measurement values	0/5	N/A	N/A

Table 5.4: Detection results against tested attack scenarios using NSM

MGCC or the IEC 104 slaves in the microgrid.

Contrast to Attack #5b, the modification of packets in Attack #6 is repeated continuously to the point where the MGCC sends messages to the loads to perform load shedding. The NSM platform generates alerts related to the rise in IEC 104 communications between the MGCC and the loads during the load shedding operation. The LSTM prediction model is built based on the behaviour of the microgrid when the microgrid is stable and not communicating frequently with the loads. Load shedding commands are not transmitted when the microgrid is stable, which is why an anomalous transmission rate is detection when load shedding commands are transmitted during microgrid simulation. While load shedding is an expected operation within the microgrid, it was not included in the LSTM training model because it is a rare enough event to be considered an exceptional event. It also takes place over a very short time, making the load shedding operation difficult to incorporate into the learning model without compromising its effectiveness at detecting anomalies in more regular operations. This means that the NSM platform will likely generate a false positive in the event of legitimate load shedding. Ideally, additional contextual information can be used to distinguish legitimate load shedding from load shedding caused by a malicious intruder. Similar to Attack #6, Attack #7 is detectable by frequency control traffic no longer being transmitted to the ESSs when the MGCC starts to operate in grid-connected mode while the microgrid itself is still in islanded mode.

Attack #7c is not detected by NSM due to the attack being able to mislead the MGCC into basing its frequency control on an incorrect frequency without making the frequency error so extreme that it resulted in load shedding or power shedding. The NSM platform currently does not make use of a prediction model based on power quality characteristics such as frequency and power output.

Similar to Attack #5b, Attack #9 is not detected due to having a very minimal impact on packet rates while not causing observable application errors. The LSTM prediction model struggles to distinguish single packet drops and single packet injections from noise in the packet transmission rate present in the microgrid system. The specific implementations of IEC 104 for the simulation outstations and the master station does not require S-format frame acknowledgement to continue transmitting IEC 104 messages. Because of this, DoS does not result from S-format frame acknowledgement messages being dropped. Even though Attack #9 drops every S-format frame that

was transmitted, the S-format frames are transmitted so infrequently that the effectively amounts to a random packet drop of non-critical information. In consideration of other potential systems, this result highlights a need to identify any critical information that is transmitted very infrequently, as this information can be dropped or injected with a much lower chance of being detected by NSM.

The recorded detection time through NSM is in the order of tens of seconds due to a combination of the NSM manager only polling the NSM agents every 10 seconds to update the NSM data object values and the anomaly detection module requiring time to analyze the incoming data. The anomaly detection potentially requires an adequate amount of past data points to detect discrepancies between predicted and actual values using LSTM.

5.8 Recommendations

There is room to expand the efficiency and detection effectiveness of the NSM platform, as well as the potential to include complementary tools to detect and mitigate attacks on the microgrid.

5.8.1 Potential for Improving NSM

With the amount of agents that need to be monitored, scalability concerns arise with the deployment of NSM. As the number of monitored agents rises, more network resources are consumed by the NSM manager to poll each agent and subsequently process the received data for anomalies. Splitting the role of NSM manager across multiple separate stations may allow each NSM agent monitor to poll agents more frequently. At the same time, the managers would each analyze smaller volumes of data for anomalies, further improving detection time.

In regards to the tampering of operation values transmitted through the microgrid communication network such as power quality measurements, it may be possible to extend the set of collected data with MIB objects representing some of these values on which prediction models to compare them to can be built. Outside of NSM, detection of packet tampering can be handled by a separate system using a different intrusion detection strategy such as Deep Packet Inspection (DPI). Such detection systems can even be equipped with NSM agents in order to inform the NSM manager of packet tampering.

When considering the microgrid system, the current NSM platform is incomplete. It has yet to build a predictive model for microgrid behaviour while the microgrid is in grid-connected mode. The platform would then switch between prediction models depending on the current operation mode of the microgrid.

5.8.2 Application of IEC 62351-5:2013

The NSM system prescribed in IEC 62351-7:2017 is largely designed to detect issues with the health and traffic flow of the system. It is meant to be used in tandem with the security measures prescribed in other parts of IEC 62351. In particular, the IEC 62351-5:2013 standard provides details on the security measures to be applied to IEC 104 and its derivatives, such as DNP3 [22]. The IEC 62351-5:2013 standard supports end-to-end security for power systems by enforcing a cryptographic challenge-response mechanism to critical IEC 104 messages secured by a shared key authentication scheme. The challenge response mechanism prevents IEC 104 packets from being modified, injected, or replayed without detection unless the secret authentication session key in use at the time is known, even if a MitM attack is successfully performed. However, a MitM attacker can still delay or drop IEC 104 packets to harm the operation of the microgrid without immediate suspicion of malicious intrusion by the microgrid security system.

When assessing the effectiveness of the attack scenarios used for experimental evaluation in this experiment, attacks 1 through 7, due to not being able to pass the challenge-response step, would fail to achieve the intended result if IEC 62351-5:2013 security measures are applied to all transmitted IEC 104 messages. However, attacks on the circuit breaker status reporting and measurement values would still be possible if such messages are considered non-critical by the microgrid system deploying IEC 62351-5:2013 and choosing not to protect those messages with the challenge-response mechanism. Even with the IEC 62351-5:2013 security mechanisms in place, it is still possible for a MitM attacker to drop and delay packets, allowing the attacker to launch Attack #8 and Attack #9 due to those attacks. The use of NSM as described by IEC 62351-7:2017 is more appropriate for detecting these two attacks.

5.9 Conclusion

In this chapter, the microgrid simulation testbed used to evaluate the microgrid NSM platform is described in detail. The testbed consists of a power system simulator on which a microgrid model is simulation. The simulator is connected to a local IP network through which the microgrid simulation can connect to software applications on the network, including NSM. The microgrid simulation model consists of a power system, a protection system, a control system, and a communication network. It is in the communication network where the focus is placed on cyberattacks, and the role of NSM in detecting them.

This chapter also gives details on what techniques were used to implement NSM. The NSM agents are realized as software applications in the local IP network that monitor the digital communications of the DERs and loads that are part of the microgrid. The NSM manager is also realized as a customized software application in the IP network, relying on SNMP to collect NSM data from the agents.

This chapter lists the attack scenarios that are used to evaluate the scalability and effectiveness of NSM in detecting cyberattacks against the microgrid. These attack scenarios are performed on the microgrid testbed, and the experimental results pertaining to the detection of the attacks by NSM are recorded. Through these results, the effectiveness of the NSM platform in detecting attacks impacting microgrid communication traffic is demonstrated. However, the experiments expose some gaps in detection of attacks against the integrity of network messages. They also provide insight on how quickly the proposed NSM platform might detect attacks in a real system. In light of these results, some recommendations for improving the NSM platform are given, along with the security features offered by IEC 62351-5:2013 being discussed.

Having studied the suitability of IEC 62351-7 NSM in providing microgrid security monitoring, implemented a microgrid monitoring platform based on the studied NSM specifications, and evaluated the platform on a co-simulation testbed simulating a representative microgrid model, conclusions regarding the research objectives and contributions stated in this thesis can be made. This research also leaves room for future work on the topic of microgrid security.

Chapter 6

Conclusion

The usage of digital technologies within the microgrid has raised concerns regarding the vulnerability of microgrid to cybersecurity threats. With microgrid systems being part of the critical power infrastructure, the impact of cyberattacks against the microgrid can have potentially severe impacts, including blackouts. These concerns have inspired the undertaking of this research aiming to enhance the cyberattack detection capabilities within the microgrid.

The problem addressed by this research was the design and implementation of a NSM platform for the purpose of microgrid security monitoring. In addition, the concerns regarding the effectiveness and suitability of the platform against cyberattacks were studied through experimental evaluation of the platform on a microgrid simulation testbed against simulated attack scenarios.

The contributions of this research were the investigation of IEC 62351-7:2017 NSM for use in microgrids, the design and implementation of an NSM platform to enhance cybersecurity in the microgrid, the creation of an anomaly detection module analyzing collected NSM data for threat detection, the elaboration of a microgrid co-simulation testbed, and experimental results regarding the effectiveness of the NSM platform at detecting attacks on the co-simulation testbed.

The security specifications given in IEC 62351-7:2017 defines NSM data objects to monitor through NSM, and these NSM data objects were studied to assess their potential to enhance cybersecurity in the power system. The data objects, which can be realized as SNMP MIB objects, were found to enhance the visibility of the health, access statistics, and network usage statistics of the power system network, and many are applicable to the microgrid. However, these data objects are

meant to act as a complement to attack mitigation mechanisms specified in other parts of IEC 62351.

The implemented NSM platform uses NSM agents deployed across the monitored network to monitor NSM data object information. The agents transmit the information to a central NSM manager as MIB object values over SNMP. The manager combines the collected MIB object values into data sets that each represent a snapshot of the microgrid state at a single moment in time. An anomaly detection module within the manager analyzes the collected MIB object snapshots as they are created, comparing them to previous snapshots. By reading this data, The module detects anomalies representing potential microgrid threats using both rule-based detection and machine learning techniques.

In order to evaluate the intrusion detection capabilities of the NSM platform, a microgrid simulation model was constructed within HYPERSIM for simulation on an OPAL-RT DRTS. Included in the microgrid model are power, protection, and control systems The simulated microgrid power system includes ESSs, a PV array, a wind farm, and a CHP generator. These DERs are used to provide power to several loads. A PCC between the microgrid and a simulated main grid energy source is also included in the model, with the simulated microgrid being capable of connecting and disconnecting from the main grid during operation. The simulated communication model consists of IEC 104 messages being exchanged between communication nodes at each DER and a MGCC over TCP. The microgrid simulation was connected to an IP network through which the microgrid is monitored and controlled by the MGCC while the network is monitored by the implemented NSM platform.

Within the network connecting the microgrid simulation to the NSM platform, attack scenarios were launched to negatively impact the operations of the microgrid simulation by targeting the message exchanges between the DERs and the MGCC. The launched attacks were chosen from a set of attack scenarios designed through the application of a methodology elaborated in this research. Through experimental evaluation, it was found that many of the attacks launched on the microgrid produced anomalies within the NSM data object readings. These anomalies were detected by the NSM platform, which responded by generating corresponding alerts to expose the attacks.

The NSM platform was shown to be effective at detecting attacks which alter the expected traffic behaviour within the microgrid system. However, some attacks were able to evade the NSM

detection. Specifically, attacks that modify values within digital communication packets without producing parsing errors and that do not result in traffic flow changes could not be detected. Attacks that only impacted traffic flow rates very slightly, such as by dropping or injecting only a single packet, were also able to evade detection. These gaps in detection highlight the need for additional cybersecurity measures to be in place within the microgrid alongside NSM.

Comparing the impacts of the studied attack scenarios, the attacks with the most damaging effect on the microgrid were the attacks against message integrity. The time needed for these attacks to create negative impacts was also very short. Even if NSM could detect all instances of such attacks, the response time for NSM may not be quick enough to detect them before the damage has already been done. What allowed these attacks to be so effective was the large extent of control that the MGCC had on the stability of the microgrid. This control over microgrid stability was the result of a large proportion of the total microgrid power being provided by the ESSs, whose power outputs were controllable by the MGCC. One insight to be gleaned by this is that the more critical parts of the control system may have detection speed requirements that are stricter than can be met consistently through NSM. In regards to the microgrid, the IEC 62351-5:2013 standard is intended to solve the issues of message integrity and authenticity for the IEC 104. By implementing IEC 62351-5:2013, some of the more severe attacks studied in this research are mitigated. However, detecting attacks that drop or delay packets without modifying their contents is not within the scope of IEC 62351-5:2013, but within IEC 62351-7:2017. It is recommended to have both of these standards be applied to enhance microgrid security.

The IEC 62351-7:2017 security standard provides the data model to be used for NSM within a power utility system. However, the data model is only one aspect of the NSM design. The design of a full NSM implementation also includes the architecture used for the data collection network as well as a security component making use of the collected data to generate alerts when appropriate. The scope of data collected for NSM can be shifted and expanded to suit the needs of different systems. However It must be stated that the target domain of this research was the smart grid, specifically the microgrid, which is why the focus was on the data model specified in IEC 62351-7:2017, a standard for power system security. The study on the IEC 62351-7:2017 data objects is relevant to other systems in the smart grid, such as the substation. Even within the

smart grid domain, the various systems within the smart grid each present their own challenges. The extendibility of its data model allows NSM to provide solutions for problems specific to the targeted system.

Regarding future work, there is room to enhance the realism of the microgrid system on which the NSM platform is evaluated. Real IEDs that are used in microgrid systems can be integrated into the microgrid simulation as HIL. Having real equipment integrated into the microgrid would enhance the realism of the microgrid control and digital communications within the simulation. It would also allow for impacts of attacks on a microgrid system making use of real IEDs to be assessed, while also allowing the NSM platform to be evaluated with the NSM data objects that are applicable to real IEDs. Aside from adding real equipment, the secondary control layer operations of the microgrid can be expanded, energy management operations can be introduced, and different priority levels for loads (residential, critical, etc.) can be implemented. The intrusion detection capabilities of NSM within the grid-connected microgrid is also yet to be assessed. The deployment of intrusion detection mechanisms in the microgrid system that operate in conjunction with NSM can also be explored. One such mechanism is Deep Packet Inspection, which analyzes the payload data transmitted across the network in order to detect anomalies and misuse. At the same time, the set of data objects monitored through NSM can be expanded to include other MIB bases, such as MIBs supported by commercial equipment and MIBs related to power quality.

Bibliography

[1] S. Safdar, B. Hamdaoui, *et al.*, "A survey on communication infrastructure for micro-grids", in *2013 9th international wireless communications and mobile computing conference (IWCMC)*, Jul. 2013, pp. 545–550. DOI: 10.1109/IWCMC.2013.6583616.

[2] Q. Fu, A. Nasiri, *et al.*, "Microgrids: Architectures, controls, protection, and demonstration", *Electric power components and systems*, vol. 43, no. 12, pp. 1453–1465, Jul. 2015, ISSN: 1532-5008. DOI: 10.1080/15325008.2015.1039098.

[3] X. Zhong, L. Yu, *et al.*, "Cyber security in smart dc microgrid operations", in *2015 IEEE first international conference on dc microgrids (ICDCM)*, Jun. 2015, pp. 86–91. DOI: 10.1109/ICDCM.2015.7152015.

[4] A. Aram, *Global innovation report: Microgrid market in the USA*, 2017, Available: https://www.hitachi.com/rev/archive/2017/r2017_05/Global/index.html.

[5] M. Chlela, G. Joos, and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation", in *Proceedings of the workshop on communications, computation and control for resilient smart energy systems*, ser. RSES '16, Waterloo, Ontario, Canada: ACM, Jun. 2016, 1:1–1:5, ISBN: 978-1-4503-4418-0. DOI: 10.1145/2939940.2939943.

[6] Electricity Information Sharing and Analysis Center, "Analysis of the cyber attack on the ukrainian power grid: Defense use case", SANS Industrial Control Systems, Mar. 2016.

[7] A. Ruiz-Álvarez, A. Colet-Subirachs, *et al.*, "Design, management and comissioning of a utility connected microgrid based on IEC 61850", in *2010 IEEE PES innovative smart grid technologies conference europe (ISGT Europe)*, Oct. 2010, pp. 1–7. DOI: 10.1109/ISGTEUROPE.2010.5638857.

[8] J. M. Guerrero, M. Chandorkar, *et al.*, "Advanced control architectures for intelligent microgrids - part i: Decentralized and hierarchical control", *IEEE transactions on industrial electronics*, vol. 60, no. 4, pp. 1254–1262, Apr. 2013, ISSN: 0278-0046. DOI: 10.1109/TIE.2012.2194969.

[9] L. Mariam, M. Basu, and M. F. Conlon, "A review of existing microgrid architectures", *Journal of engineering*, vol. 2013, 2013. DOI: http://dx.doi.org/10.1155/2013/937614. [Online]. Available: https://www.hindawi.com/journals/je/2013/937614/.

[10] I. Patrao, E. Figueres, *et al.*, "Microgrid architectures for low voltage distributed generation", *Renewable and sustainable energy reviews*, vol. 43, pp. 415–424, Mar. 2015, ISSN: 1364-0321. DOI: https://doi.org/10.1016/j.rser.2014.11.054. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032114009939.

[11] J. Gu, M. Yang, *et al.*, "A group setting of IED in microgrid protection management system", *International journal of information and communication engineering*, vol. 9, no. 8, pp. 764–769, 2015. [Online]. Available: http://www.waset.org/publications/10002424.

[12] C. K. Veitch, J. M. Henry, *et al.*, "Microgrid cyber security reference architecture", Sandia National Laboratories, Tech. Rep., Jul. 2013, version 1.0.

[13] D. E. Olivares, A. Mehrizi-Sani, *et al.*, "Trends in microgrid control", *IEEE transactions on smart grid*, vol. 5, no. 4, pp. 1905–1919, Jul. 2014, ISSN: 1949-3053. DOI: 10.1109/TSG.2013.2295514.

[14] IEEE Standards Coordinating Committee 21, *IEEE std 1547-2018:IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces*, Feb. 2018.

[15] S. W. Blume, *Electric power system basics for the nonelectrical professional*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2007, pp. 61–100, ISBN: 978-0-470-12987-6.

[16] A. Gupta, S. Jain, *et al.*, "Phasor measurement unit", *International journal of engineering and management research*, vol. 6, no. 2, pp. 221–224, Mar. 2016, ISSN: 2250-0758.

[17] M. Islam and H. H. Lee, "Microgrid communication network with combined technology", in *2016 5th international conference on informatics, electronics and vision (ICIEV)*, May 2016, pp. 423–427. DOI: 10.1109/ICIEV.2016.7760039.

[18] D. M. Bui, K.-Y. Lien, *et al.*, "Standards commonly used for microgrids — a research project to develop an industry microgrid standard in Taiwan", *Electric power components and systems*, vol. 44, no. 19, 2143–2160, Oct. 2016, ISSN: 1532-5008. DOI: 10.1080/15325008.2016.1216203. [Online]. Available: https://doi.org/10.1080/15325008.2016.1216203.

[19] A. Bani-Ahmed, L. Weber, *et al.*, "Microgrid communications: State of the art and future trends", in *2014 international conference on renewable energy research and application (ICRERA)*, Oct. 2014, pp. 780–785. DOI: 10.1109/ICRERA.2014.7016491.

[20] Modbus Organization, *Modbus*, 2019, Available: http://www.modbus.org/.

[21] IEC Technical Committee 57, *Telecontrol equipment and systems – part 5-104: Transmission protocols – network access for IEC 60870-5-101 using standard transport profiles*, Jun. 2006.

[22] ——, *Power systems management and associated information exchange - data and communications security — part 5: Security for IEC 60870-5 and derivatives*, Apr. 2013.

[23] ——, *Telecontrol equipment and systems – part 5-104: Transmission protocols – companion standard for basic telecontrol tasks*, Feb. 2003.

[24] P. Matoušek, "Description and analysis of IEC 104 protocol", Faculty of Information Technology, Brno University of Technology, Technical Report, Dec. 2017.

[25] P. WG, *IEEE standard for electric power systems communications — distributed network protocol (DNP3)*, Oct. 2012.

[26] IEC Technical Committee 57, *Communication networks and systems for power utility automation – part 1: Introduction and overview*, Mar. 2013.

[27] ——, *Communication networks and systems for power utility automation – part 8-1: Specific communication service mapping (scsm) – mappings to mms (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, Jun. 2011.

[28] ——, *Communication networks and systems for power utility automation – part 7-2: Basic information and communication structure – abstract communication service interface (ACSI)*, Aug. 2010.

[29] ——, *Communication networks and systems for power utility automation – part 9-2: Specific communication service mapping (scsm) – sampled values over ISO/IEC 8802-3*, Sep. 2011.

[30] Z. Zhang, X. Huang, *et al.*, "Modeling and simulation of data flow for vlan-based communication in substations", *IEEE systems journal*, vol. 11, no. 4, pp. 2467–2478, Dec. 2017, ISSN: 1932-8184. DOI: 10.1109/JSYST.2015.2428058.

[31] IEC Technical Committee 57, *Communication networks and systems for power utility automation – part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE c37.118*, May 2012.

[32] "Ieee standard for synchrophasors for power systems", *Ieee std c37.118-2005 (revision of ieee std 1344-1995)*, pp. 1–65, Mar. 2006. DOI: 10.1109/IEEESTD.2006.99376.

[33] I. Friedberg, D. Laverty, *et al.*, "A cyber-physical security analysis of synchronous-islanded microgrid operation", in *Proceedings of the 3rd international symposium for ICS & SCADA cyber security research*, ser. ICS-CSR '15, Ingolstadt, Germany: BCS Learning & Development Ltd., Sep. 2015, pp. 52–62, ISBN: 978-1-78017-317-7. DOI: 10.14236/ewic/ICS2015.6. [Online]. Available: https://doi.org/10.14236/ewic/ICS2015.6.

[34] IEC Technical Committee 57, *Power systems management and associated information exchange - data and communications security — part 7: Network and system management (NSM) data object models*, Sep. 2017.

[35] W. Stallings, *SNMP, SNMPV2, SNMPv3, and RMON 1 and 2*, 3rd. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1998, pp. 1–14, 55–83, 163–172, ISBN: 0201485346.

[36] J. Case, M. Fedor, *et al.*, *RFC-1157: A simple network management protocol (SNMP)*, May 1990.

[37] K. McCloghrie and M. Rose, *RFC-1156:structure and identification of management information for TCP/IP-based internets*, May 1990.

[38] J. Case, K. McCloghrie, *et al.*, *RFC-3418: Management information base (mib) for the simple network management protocol (SNMP)*, Dec. 2002.

[39] IEC Technical Committee 57, *Power systems management and associated information exchange - data and communications security — part 1: Communication network and system security - introduction to security issues*, May 2007.

[40] L. Mariam, M. Basu, and M. F. Conlon, "Microgrid: Architecture, policy and future trends", *Renewable and sustainable energy reviews*, vol. 64, pp. 477–489, Oct. 2016. DOI: https://doi.org/10.1016/j.rser.2016.06.037. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032116302635.

[41] M. J. Davison, T. J. Summers, and C. Townsend, "A review of the distributed generation landscape, key limitations of traditional microgrid concept & possible solution using an enhanced microgrid architecture", *2017 IEEE southern power electronics conference (SPEC)*, pp. 1–6, Dec. 2017. DOI: 10.1109/SPEC.2017.8333563.

[42] A. Ruiz-Alvarez, A. Colet-Subirachs, *et al.*, "Operation of a utility connected microgrid using an IEC 61850-based multi-level management system", *IEEE transactions on smart grid*, vol. 3, no. 2, pp. 858–865, 2012, ISSN: 1949-3053. DOI: 10.1109/TSG.2012.2187222.

[43] W. Deng, W. Pei, *et al.*, "Adaptive micro-grid operation based on IEC 61850", *Energies*, vol. 8, no. 5, pp. 4455–4475, May 2015, ISSN: 1996-1073. DOI: 10.3390/en8054455.

[44] P. Maynard, K. McLaughlin, and B. Haberler, "Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks", in *International symposium for ICS & SCADA cyber security research (ICS-CSR)*, Sep. 2014. DOI: 10.14236/ewic/ics-csr2014.5.

[45] X. Liu, M. Shahidehpour, *et al.*, "Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems", *IEEE transactions on smart grid*, vol. 8, no. 3, pp. 1330–1339, May 2017, ISSN: 1949-3053. DOI: 10.1109/TSG.2016.2622289.

[46] D. Jin, Z. Li, *et al.*, "Toward a cyber resilient and secure microgrid using software-defined networking", *IEEE transactions on smart grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017, ISSN: 1949-3053. DOI: 10.1109/TSG.2017.2703911.

[47] M. Chlela, D. Mascarella, *et al.*, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks", *IEEE transactions on smart grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018, ISSN: 1949-3053. DOI: 10.1109/TSG.2017.2667586.

[48] G. Chalamasetty, P. Mandal, and T. Tseng, "SCADA framework incorporating MANET and IDP for cyber security of residential microgrid communication network", *Smart grid and renewable energy*, vol. 7, pp. 104–112, Mar. 2016. DOI: 10.4236/sgre.2016.73007.

[49] V. Kounev, D. Tipper, *et al.*, "A secure communication architecture for distributed microgrid control", *IEEE transactions on smart grid*, vol. 6, no. 5, pp. 2484–2492, Sep. 2015, ISSN: 1949-3053. DOI: 10.1109/TSG.2015.2424160.

[50] Y. Yang, K. McLaughlin, *et al.*, "Stateful intrusion detection for IEC 60870-5-104 SCADA security", in *2014 IEEE power and energy society general meeting conference & exposition*, 2014.

[51] Y. Li, P. Zhang, *et al.*, "Active synchronous detection of deception attacks in microgrid control systems", *IEEE transactions on smart grid*, vol. 8, no. 1, pp. 373–375, Jan. 2017, ISSN: 1949-3053. DOI: 10.1109/TSG.2016.2614884.

[52] J. Inoue, Y. Yamagata, *et al.*, "Anomaly detection for a water treatment system using unsupervised machine learning", in *2017 IEEE international conference on data mining workshops (ICDMW)*, Nov. 2017, pp. 1058–1065. DOI: 10.1109/ICDMW.2017.149.

[53] M. H. F. Ahamed, U. D.S. D. Dissanayake, *et al.*, "Modelling and simulation of a solar pv and battery based dc microgrid system", in *2016 international conference on electrical, electronics, and optimization techniques (iceeot)*, 2016, pp. 1706–1711. DOI: 10.1109/ICEEOT.2016.7754977.

[54] B. Xiao, M. Starke, *et al.*, "Development of hardware-in-the-loop microgrid testbed", in *2015 IEEE energy conversion congress and exposition (ECCE)*, Sep. 2015, pp. 1196–1202. DOI: 10.1109/ECCE.2015.7309827.

[55] W. Liu, J. Kim, *et al.*, "Power converters based advanced experimental platform for integrated study of power and controls", *IEEE transactions on industrial informatics*, pp. 1–1, Apr. 2018, ISSN: 1551-3203. DOI: 10.1109/TII.2018.2830382.

[56] B. Xiao, M. Starke, *et al.*, "Implementation of system level control and communications in a hardware-in-the-loop microgrid testbed", in *2016 IEEE power energy society innovative smart grid technologies conference (ISGT)*, Sep. 2016, pp. 1–5. DOI: 10.1109/ISGT.2016.7781245.

[57] C. Robillard, "Network and system management using IEC 62351-7 in IEC 61850 substations: Design and implementation", Master's thesis, Concordia University, 2018.

[58] F. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with lstm", in *9th international conference on artificial neural networks*, Sep. 1999, pp. 850–855. DOI: 10.1049/cp:19991218.

[59] A. Albarakati, B. Moussa, *et al.*, "Openstack-based evaluation framework for smart grid cyber security", in *2018 IEEE international conference on communications, control, and computing technologies for smart grids*, Aalborg, Denmark, Oct. 2018.

[60] OPAL-RT Technologies, *Hypersim: The power system simulator of tomorrow*, 2018, Available: https://www.opal-rt.com/systems-hypersim/.

[61] OpenStack Foundation, *OpenStack: Open source software for creating private and public clouds*, March 2018, Available: https://www.openstack.org/.

[62] J. Park, J. Candelaria, *et al.*, "Dc ring-bus microgrid fault protection and identification of fault location", *IEEE transactions on power delivery*, vol. 28, no. 4, pp. 2574–2584, Oct. 2013, ISSN: 0885-8977. DOI: 10.1109/TPWRD.2013.2267750.

[63] NetSNMP, *NetSNMP*, 2013, Available: http://www.net-snmp.org/.

[64] ——, *Net-SNMP Distributed MIBs*, 2014, Available: http://www.net-snmp.org/docs/mibs/.

[65] S. Consortium, *SQLite*, June 2018, Available: https://www.sqlite.org/index.html.

[66] A. Burger, *SNMP Trap Translator*, 2013, Available: http://www.snmptt.org/.

[67] Elastic, *Elasticsearch*, 2018, Available: https://www.elastic.co/products/elasticsearch.

[68] MongoDB, *What is MongoDB?*, 2018, Available: https://www.mongodb.com/what-is-mongodb.

[69] Elastic, *Kibana*, 2018, Available: https://www.elastic.co/products/kibana.