DEVELOPMENT OF A FAULT DETECTION MODEL FOR CYBER PHYSICAL POWER SYSTEM

Hafiz Saleem

A Thesis Submitted in Partial Fulfilment of The Requirements for the Degree of Master by Research in Electrical Engineering

DEPARTMENT OF ELECTRICAL ENGINEERING

COLLEGE OF ENGINEERING AND SCIENCE

VICTORIA UNIVERSITY
MELBOURNE AUSTRALIA

December 2018

ABSTRACT

This thesis investigates and implements a fault detection scheme for cyber-physical power system (CPPS). An un-interruptible supply of energy is the biggest challenge faced by the power engineers. Due to the involvement of information and communication technology (ICT), the behavior of the power grid has transformed completely in recent years. The evolution of the existing grid system has resulted in bidirectional power flow. That means the entities once only consumed power now can generate and send power back to the main grid, behaving as a microgrid.

The grid is made up of microgrids, which in turn is the combination of different generators that are mostly installed at the consumer end to generate electrical power for consumers' own use, whilst the additional power can be sent to the grid. To manage the power systems with microgrids and bidirectional power flow, Smart Grid (SG) is developed to efficiently manage the bulk power system across the network. SG expands the existing capabilities of grid generation, distribution, and transmission to provide a system capable of handling future requirements for renewable energy generation, electric vehicles and the demand side management of electricity. SG is based on the CPPS, which is vulnerable to cyber-attacks, where an intruder can change the information sent or received from the grid.

As the purpose of this study is to find the best model to detect fault in the grid. A hypothetical scenario of a hacker intruding in the SG is considered the effect of line outages on SG is discussed when there is an attack from any hacker that altered the information of phasor measurement unit (PMU). Power World Simulator is used to simulate IEEE 13-Bus and 39-Bus systems, having renewable energy generators to test the SG after line outage. In addition, two techniques i.e. Phasor Angle Measurement Algorithm & Alternating Direction Method for Multipliers (ADMM) to detect line outage are implemented and compared to find pre-outage

power flow and transmission line failure. ADMM was found to be more robust and simpler to implement.

DECLARATION

"I, **Hafiz Saleem**, declare that the Master by Research thesis entitled, "**Development of a Fault Detection Model for Cyber-Physical Power System"** is no more than 60,000 words in length including quotes and exclusive of tables, figures, appendices bibliography, references, and footnotes." The thesis contains no material that has been submitted previously in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work."

Signature……  …… **Date:** 11-06-2019

ACKNOWLEDGMENTS

I am extremely grateful to my supervisor **Professor Akhtar Kalam**, for believing in me and giving me a chance to be under his supervision. His endless support, invaluable comments and encouragement have been very important in my learning process throughout this research project. Special appreciation goes to my co-supervisor **Adjunct Professor, Aladin Zayegh** for his positive comments and suggestions, and **Elizabeth Smith** for her precious time in assisting me with enrolments and other school matters.

I also like to thank the staff and postgraduate students of the College of Engineering and Science at Victoria University **(VU)** for extending their help throughout this work. Likewise, thanks to my friends and colleagues **Abdulrahman**, **Sajjad**, **Salman,** and **Srilal**, for sharing their talents and priceless time during this study.

Finally, I wish to express my gratitude to my family and my parents for their undying support and continuous encouragement. I am especially indebted to my wife **Maria**, for her unconditional love and support, to my daughters **Fatima** and **Ayesha**, who inspired and strengthened me.

Thank you very much.

And above all to the Almighty **ALLAH**.

PUBLICATIONS

Saleem H, Kalam A, Gulraiz A, "***Effect of Line Outages on Cyber-Physical Power System"*** The Third International Conference on Electrical and Electronic Engineering, Telecommunication Engineering and Mechatronics (EEETEM2017), April 26-28, 2017, Beirut, Lebanon.

Table of Contents

Contents

LIST OF TABLES

LIST OF FIGURES

List of Figures

LIST OF ACRONYMS & SYMBOLS

ADMM	Alternating Direction Method of Multipliers
ALASSO	Adaptive least absolute shrinkage and selection operator
AMI	Advanced Metering Infrastructure
AMR	Automatic meter reading
BAN	Building area network
CPPS	Cyber physical power system
DFIG	Doubly-fed induction generator
DLCD	Distributed Line Change Detection
DoS	Denial of service
FACTS	Flexible AC Transmission
FAN	Field area network
GMRF	Gaussian Markov random field
IAN	Industrial area network
IP	Internet protocol
LAN	Local area network
LASSO	Least absolute shrinkage and selection operator
LQV	Learning vector quantization
MAC	Media access control
MPD	Matching pursuit decomposition
NAD	Normalized angle distance
PCC	Point of common coupling
PDC	Phasor data concentrator

List of Acronyms

PMU	Phasor measurement units
PMU	Phasor Measurement Unit
PTDF	Power transfer distribution factor
RES	Renewable energy sources
SCADA	Supervisory control and data acquisition
SDH	Synchronous Digital Hierarchy
SO	System operator
SONET	Synchronous Optical Network
WAMS	Wide area measurement systems
WAN	Wide area network
WC	Wavelet coefficients
WDM	Wavelength Division Multiplexing
$\overline{H_n}$	The measurement matrix,
M_n	Number of measurements within n-th PDC area.
N_l	Number of lines in the whole system
$\overline{g_n}$	Additive Gaussian noise vector
Y_m	The maximum amplitude of the waveform,
ω	The radial frequency given in rad/sec
t	The time of waveform can be calculated using the ratio of 2π & ω
ϕ	The phase shift produces in the circuit.

CHAPTER 1

Introduction

1.1 Problem's Outline

Today's power grid does not only depend on pure electrical components, it is also equipped with sensors to provide measurement at the highest data rate and resolution. Due to addition of many sensor measurements (which have added complexity to the power networks) there is a need of Cyber Physical Power System (CPPS) which can provide simulation and modelling for assessing the characteristics of selective networks fabrics. Figure 1.1 shows the new power grid infrastructure having all the complexities faced by this time.

One of the biggest challenges that human race is facing today, is un-interruptible energy supply for our long-term energy needs that have minimum impact on the environment. Conventional grids are having extreme pressure to deliver the increasing demand for power, as well as to provide a controlled and efficient supply of electricity using available technologies **[1].** A growing demand for reliable energy and other technological developments have inspired the development of a Smart Grid (SG). This electrical grid improves the existing capabilities of the grid's generation, transmission, and distribution systems to offer a system which is capable of handling upcoming requirements for distributed generation, electric vehicles, renewable energy sources and the consumer side management of electricity **[2].** Wide area measurement and management systems, automated substation and advanced metering infrastructures (AMI) are deployed to attain these objectives **[3].** Increased use of information and communication technology (ICT) to achieve the required aims and objectives of SG results in the growth to CPPS. However, it is difficult to understand the dependencies between Cyber and power domains, and the impacts of Cyber issues on the Power System.

1.2 Problem Statement

"Considering the importance of SG it is imperative that any faults to the operation of grid are detected live. This study aims to find the most robust and technique of detecting fault in a CPPS."

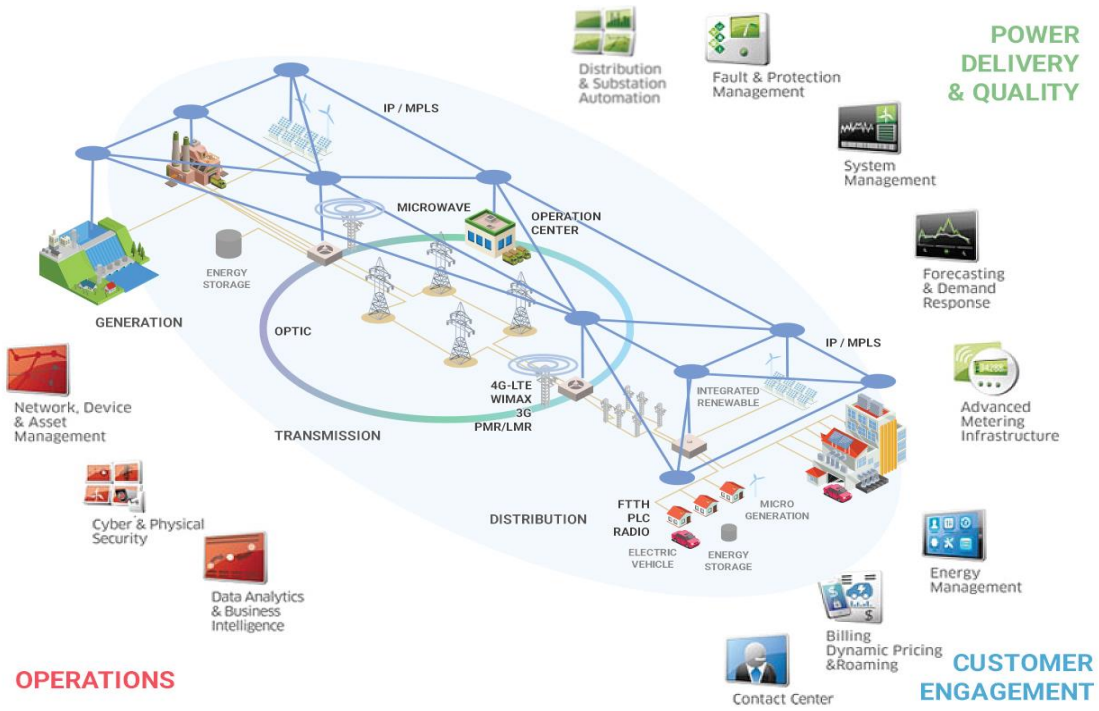

Figure 1.1 Smart Power Grid Physical Infrastructure [4].

1.3 Methods Applied in the Past

Various methods have been implemented with reference to fault detection, power grid weak point prediction, and fault rectification in the last few decades. When it comes to fault identification, a transmission line outage detection scheme is designed **[7]** based on measurement of phasor angle information. In addition, this method is also designed for multiple line failure identification **[8]**. A power network adaptation of the worst configuration heuristics is developed, combined with linear programming algorithm in reference **[9]** to forecast Grid fragile areas. Another research is done on fault identification using four features selection criteria method including 1) stepwise regression, 2) hypothesis test, and 3) stepwise selection

by Akaike's information criterion **[10]**. Least absolute shrinkage and selection operator (LASSO)/adaptive least absolute shrinkage and selection operator (ALASSO) are compared to identify their applicability **[10]**. Petri net [11] proposed a fault detection and identification method, based on which was developed a mechanism to capture the modeling details of the protection system of the distribution network. Likewise, Ruiz-Reyes has proposed a discrimination method on voltage sag and transient voltage stability in **[12]**. It uses the matching pursuit decomposition (MPD) with sinusoid dictionary for feature extraction and Learning Vector Quantization (LVQ) for discriminating several types of voltage signals.

After the fault in power grid is detected and identified, the next step is to find its geographic location and estimate its region of impact. For this purpose, a fault location method is proposed based on Gaussian Markov Random Field (GMRF) using the phasor angle measurements across the buses in SG **[13] [14]**. Furthermore, a wavelet-based method is designed for fault detection and location **[15] [16]**. It uses the maximum wavelet coefficients (WCs) of the voltage and frequency signals in the state of fault disturbance. Moreover, a connection between the wavelet coefficients and variation in power is examined to increase the accuracy of load and fault location calculation **[17].**

1.4 Research Gap

While studying CPPS, certain key issues emerge in the so-called general-purpose computing. In any software, the time required to perform a specific task could be an issue of performance, not accuracy. In general, a longer time to finish any task is not appropriate and hence less appreciable. However, in CPPS, performing a task (like fault detection and its immediate remediation) is time critical. Minor delay or less accurate fault detection may lead to a catastrophic cascade of failures throughout the system **[5].** Risks posed to the Cyber infrastructure, conventional, unconventional and physical part of the power system, collectively determine the security of the grid. The literature on the consistency of power

systems inspecting the overlaid cyber components is limited and that of their mutual interdependence nearly does not exist **[6].**

Cyber-Physical Systems (CPS) are quite common in power systems and are expected to operate reliably in front of catastrophic failures and other external threats on the power network. Today's Power Grids, having current carrying components and embedded communication **[6]**, computational and control networks are fast emerging as one of the complex and largest CPS. This kind of complications proposed to attain the advanced levels of flexibility, effectiveness and fault resistance, can cause more catastrophes of complicated nature thus reducing the system reliability **[6].**

Therefore, robust fault detection, isolation, and rectification have become one of the biggest challenges today to full fill the promises of SG. The aim of this study is to design a model for fault detection which will be one step closer to the self-healing SG. To fulfil this, there is a need to address all the potential issues related to SG, including protection from cyber-attacks. Assessing the possible attack effect on the system requires an assessment of grid's reliability on the cyber infrastructure and its capability to resist major failures **[31]**. In addition to that, a much-detailed analysis of cyber-physical relationship within the grid is required to determine the inevitability of cybersecurity efforts **[2].**

1.5 Aims and Objective

The above literature suggests that the robust fault detection, isolation, and rectification has become one of the biggest challenges to fulfill the promise of SG. Based on the discussion methods applied in the past and research gap, the current study is focussed to test different algorithms on power network model for fault detection, which enable the use of SG efficiently. This study will contribute to the following aspects of SG:

- Secure operation of SG
- Live fault identification
- Accuracy in determining fault location
- Provide a reliable data and information network
- Enable efficient generation and distribution using renewables
- Maintaining security of supply by ensuring integration and interoperability

1.6 Thesis Layout

The first chapter provides an introduction to the thesis and outlines the problems in the smart grid due to security measures. The chapter also provides information about the existing methods but at this point, it is unclear which method is more efficient as there is no such comparison available between the results of proposed methods. Chapter 1 also explains aims and objective of the thesis, which is to provide better security and reliability to the SG.

The second chapter gives complete background of SG in the form of literature review. It contains detailed explanation of working procedure of SG. SG infrastructure is also explained in this chapter which provides information about how any power system behaves like a bidirectional network. This chapter constitutes more than 30% of this thesis, it contains a complete explanation about physical layer in SG which is related to the actual physical system of the grid. Cyber infrastructure provides details of electronic system and communication and service systems. All the measurement is sent and received by means of communication service and cyber infrastructure is responsible for it. Security layer operation is also explained in this chapter, which gives an overview of the security measures required for the smart grid. Components of the SG are also explained in this chapter to have complete information about

smart grid functionality. In the later part of this chapter security threat which is expected to face in future are discussed, in addition to that current challenges of SG are also explained.

SG model is explained in the third chapter. Before the start of actual testing, it is necessary to know the functionality of SG. When it comes to power systems there are some parameters which are considered to explain the working of a power system i.e. smart grid equivalent model is considered for testing and evaluation purposes. SG as a CPPS is modeled in this chapter too. In the fourth chapter, all the selected work related to SG is discussed. As some of the existing methods are tested on different power networks in the end their results are compared to show which one is more efficient. In that way, it is also easy to find out any improvement possible in the existing algorithms, to provide better security and reliability for the SG.

CHAPTER 2

Background and Literature Review

2.1 Smart Grid

According to University of Michigan **[32]**, in the last 50 years, power networks evolved from the single grid network to a complex interconnected electric grid, having electricity generation at notable scale of (1000-4000 MW) to main load centers which is further divided into a large number of individual customers. To provide the required amount of energy, large power stations are built based on hydro, coal, oil, and gas energy. However, this system became unreliable by the end of 20th century and one major reason being unable to meet energy needs as per demand forecast. Many challenges are faced by modern power networks, including security threats, privacy issues, complexity in managing high power networks with intermittent supply, continuous supply of electricity during peak demand, digital and analog controlled devices synchronization and to fulfill government's aim to employ more renewable energy in the system. These issues require the development of an automated, flexible, self-balancing, intelligent and integrated electric network that utilizes the modern ICT techniques to manipulate and share information.

Smart Grid is reported to be the most viable solution for all above-mentined issues. It is a complex system categorized as the bidirectional flow of electricity with a capability of monitoring and controlling the variations in power plants as shown in Figure 2.1. It also responds to the consumer request regarding the switching of individual appliances. It is an intelligent, widely distributed energy delivery network which holds all the information of utility and customers connected with it. It is a collection of controlling energy and monitoring devices, networking, software and communications infrastructure which are installed ubiquitously in

electricity distribution grid, homes, and businesses. This complete system acts as a heart of the grid and for customers, it is considered as a nervous system that provides monitoring and controlling of energy digestion comprehensively in real time. It can also be called as the Internet for Energy.

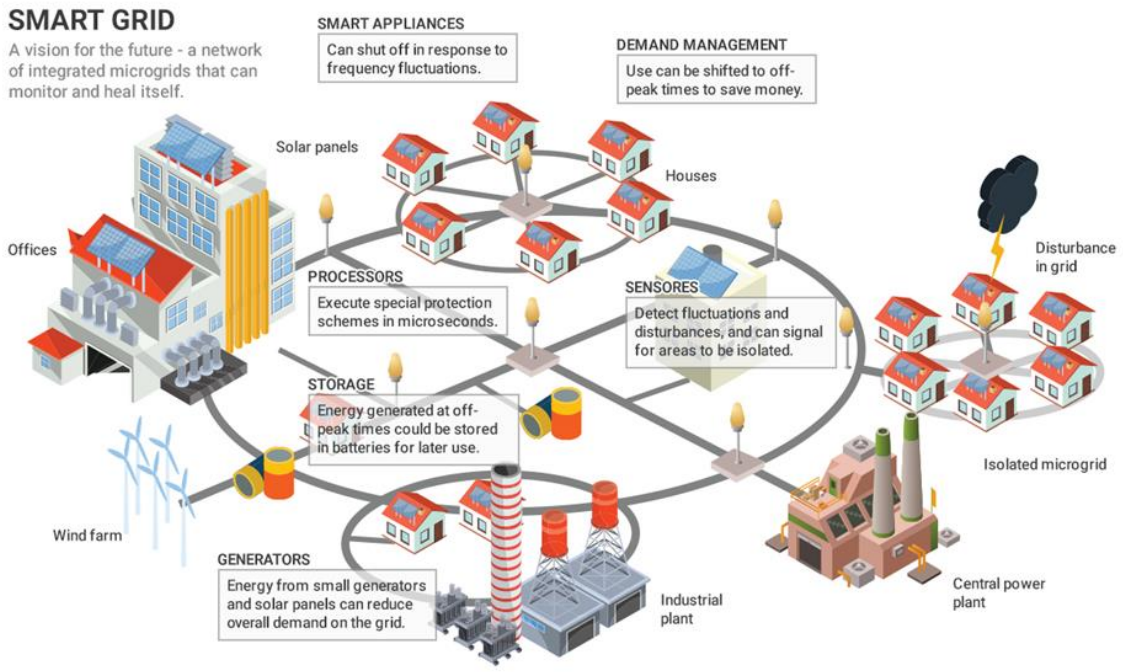

Figure 2.1 Smart grid vision [19].

As shown in Figure 2.2, the evolving smart grid is dedicated to forcing the CIT to develop the reliability and sustainability of the operation of energy, so that energy can be transferred and received efficiently. Phasor measurement units (PMU) can directly measure the complex voltages and currents. Smart meters are employed between the end-users and the distribution network. That abundant measurement of data having all the information of any grid becomes a major challenge when it comes to computation and data analysis.

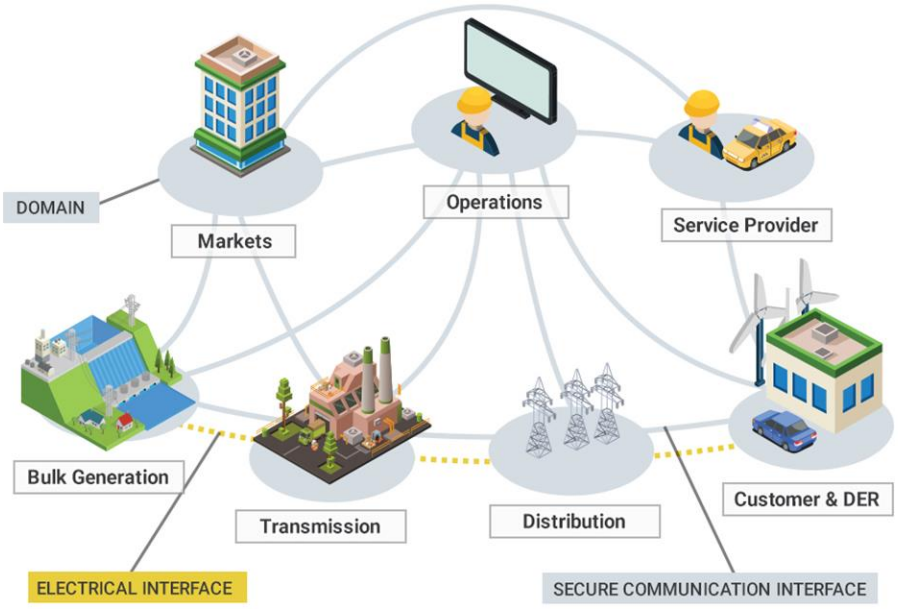

Figure 2.2 Smart grid [19].

2.2 Smart Grid Infrastructure

Smart Grid has become bidirectional in nature after the addition of renewable energy and various sources of generation as shown in Figure 2.3. Transmission lines are used to send energy to customers. Meanwhile, SG enables a two-way electricity flow in which the users can prodcue as well as consume and send back electricity to the grid and this mechanism is known as prosumer. In addition to that, it uses modern technologies for communication and data transfer between consumer and grid. Similarly, from a functional point of view, SG comprises of seven basic parts:

- Generation
- Transmission
- Distribution
- Service Provider
- Operations

- Customer
- Markets

Meanwhile,

- Power flow system layer
- Security layer and
- Cyber Infrastructure of the Grid

are three major sections that describe the SG from a technical viewpoint.

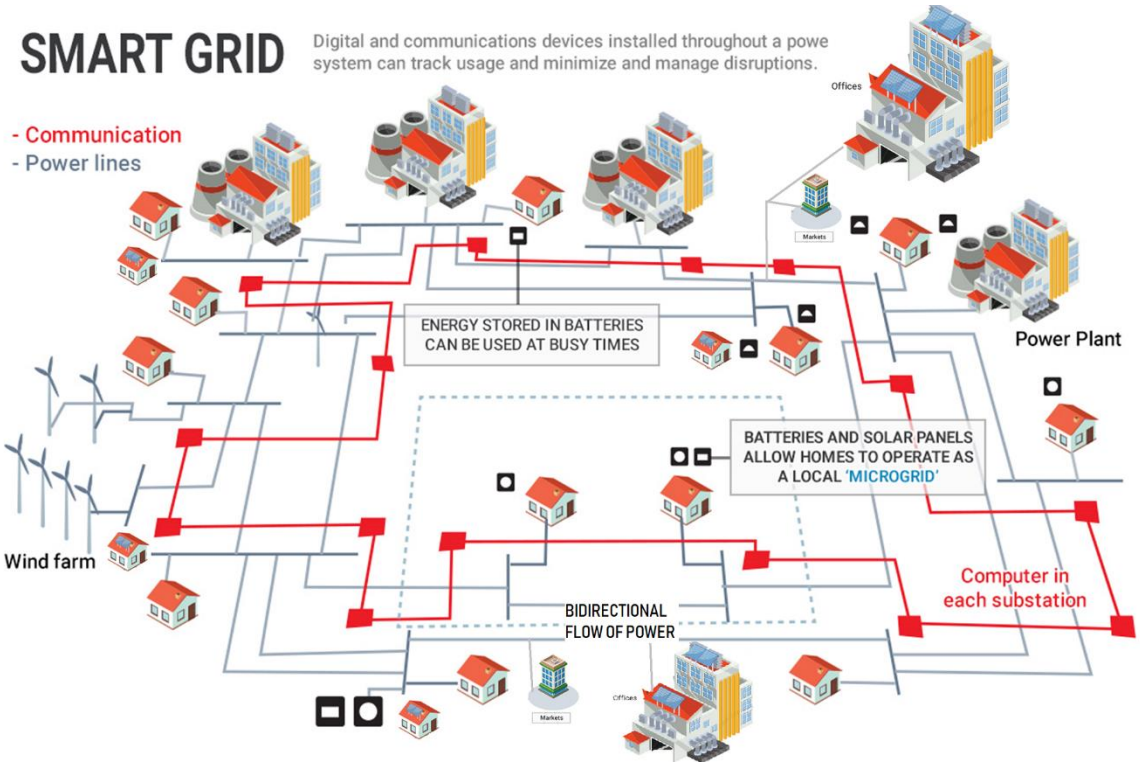

Figure 2.3 Overview of smart grid architecture [20].

2.3 Power Flow System Layer

This layer links the power generation side to the transmission line as shown in Figure 2.4 and extends to the distribution networks and finally to the consumers. Electricity in power grid is produced by different distributed generators (renewable and traditional) integrated into the common grid exchanging data and control information. This layer carries information about generators through a transmission line which is used for energy management and efficient delivery of power. Due to a continuous demand of energy supply to a wide array of consumers under varying circumstances, maintaining continuity and stability is challenging. For instance, low cost power is generated through Solar Panels during the day, but it is insufficient to cover peak demand i.e. SG must adopt a strategy to manage this demand using a combination of renewable and other energy sources. Thus, information plays a key role by providing the SG a more accurate description of the system, accelerating its performance and precision while assisting it to adopt more informed decisions.

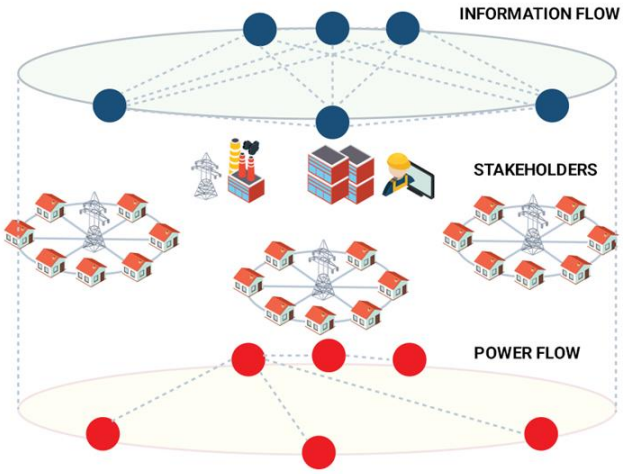

Figure 2.4 Power flow layer [21]

2.4 Cyber Infrastructure

Cyber infrastructure consists of electronic information, communication & service systems as shown in Figure 2.5. Electronic information flow is controlled by the communication technologies (power communication networks and protocols). Following parameters form the grid are used to send and receive information:

- Control Commands and Information
- Data Monitoring
- Metric and Management System

Due to monitoring and metering equipment, there is a large amount of data produced by the grid that needs to be controlled through analysis, incorporation, and optimization. Thus, information management of the power grid through integrity accomplishes the aim of interoperability between equipment.

Information metering and measurement are further divided into following subcategories:

- Smart Monitoring,
- Smart Metering,
- Smart Measurement.

Smart Meter is a tool for obtaining data from consumers and controls other devices as well. Advanced metering infrastructure (AMI) systems are used for automatic meter reading (AMR) that collects data and information used for diagnostics, power consumption, status from energy meter and load it into a central database to be analyzed and processed. Smart Meter records consumption and sends this information to the utility for monitoring and billing. Smart monitoring and measurement is established through sensors, which are mainly wireless networked and connected to phasor measurement units (PMU). PMUs are connected through Ad-hoc wireless sensor networks. These networks are a collection of sensor nodes without a

fixed structure (because sensors are prone to failure and the network topology changes), in which wireless devices are used having radio frequency as a network interface. Information management is related to the process of data manipulation, integration, analysis, and optimization of a large amount of information coming from the measurements sensing devices.

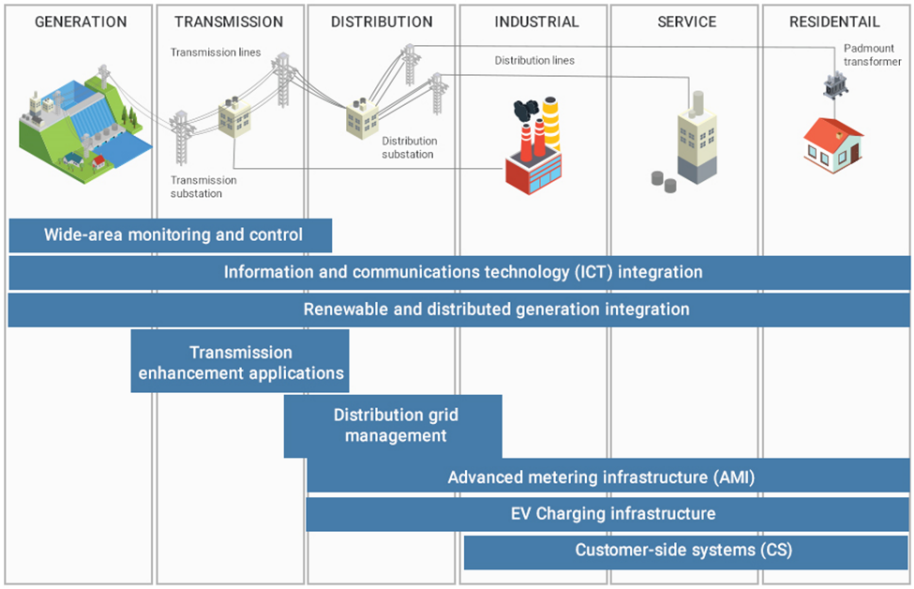

Figure 2.5 Cyber Infrastructure [22].

Buses that require connecting control centers, markets and generators are Wide area network (WAN), Local area network (LAN), Field area network (FAN), Building area network (BAN) and Industrial area network (IAN). All these buses are task-specific like WAN connects remote devices. SDH (Synchronous Digital Hierarchy), WDM (Wavelength Division Multiplexing) and SONET (Synchronous Optical Network) are the technologies used by WAN to enable multiple carrier signals integrated onto a single optical fiber. Local area network (LAN) is used to connect local users using ethernet technology standardized as IEEE 802.3 which enables users to connect over copper and fiber cables. In addition, Wireless LAN standardized as IEEE 802.11 is used in LAN which works on the terrestrial microwave, communication satellites and cellular systems. As the name implies, Field area network (FAN)

connects devices in the field including transformers, switches, sensors, actuators etc. In order to connect intelligent household devices like Zigbee, home area network (HAN) is used. For commercial purposes, building area network (BAN) is preferred. Like in offices where there is a higher demand of energy in comparison with domestic homes. Industrial area network (IAN) is used for the control of industrial machines and others devices such as servers, computers, DCS etc.

An efficient and reliable data exchange system in the electricity grid network has to fulfill some objectives which are: Quality of Service, avoid delays, varying sampling intervals, and no packet loss. Likewise, safety is also one of the major concerns and there must be no security failures in the system. Advanced security methods must be provided to enhance security in case of cyber attacks. Twenty for hour availability of the network system is required for the real-time Smart Grid having wide area coverage.

2.5 Security Layer

In power industry, security is essential to install equipment that can improve power grid performance from generation to transmission, to keep power losses at the lowest level and improve the quality of power at the consumer side. Connecting different equipment together can increase the complexity of the system and such system will have an elevated risk of security. Consequently, any physical or Cyber security lapse will impact the society at large. There must be a balance between the physical systems, information management systems and Cyber systems to keep power grids safe and secure. Since electricity must be available all the time, it also maintains the constant voltage across the load since there are some sensitive machines in industries which are prone to voltage variations. Figure 2.6 shows the layers of SG infrastructure. It can be clearly seen, in contrast to a traditional grid, flow of power is bidirectional. If an end user has smart metering enabled and have a PV panel installed acts as a generator for surplus energy generated.

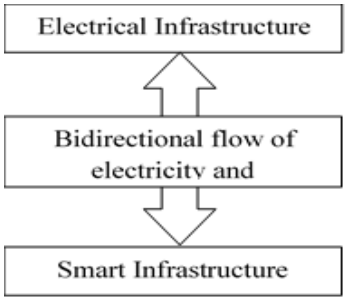

Figure 2.6 Smart Grid infrastructures

2.6 Components of Smart Grid

Main components of a Smart Grid are shown in Figure 2.7 and include:

- Supervisory Control and Data Acquisition (SCADA), Phasor Measurement, Flexible AC Transmission (FACTS), Advanced Conductors
- Substation Automation
- Distribution Automation
- Advanced Metering

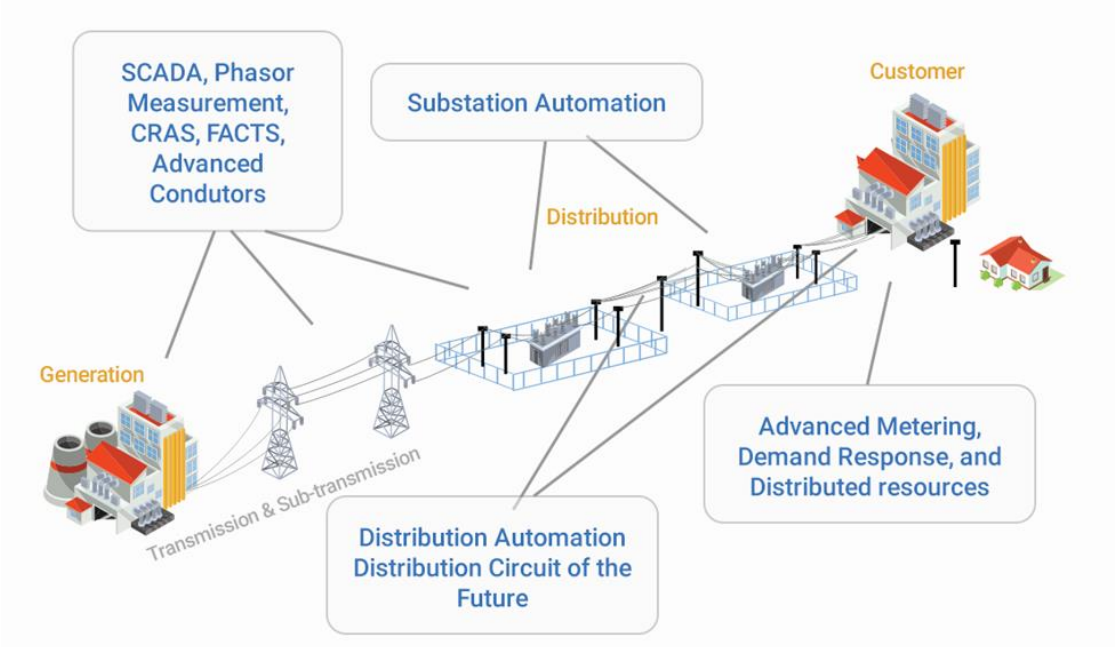

Figure 2.7 Main Components of Smart Grid [29]

2.6.1 SCADA, Phasor Measurement, Facts and Advance Conductors

SCADA system is used at the generation side, transmission side and sub-transmission to allow complete control on the generation and transmission of power. In case of any fault, SCADA system indicates it. Meanwhile, Phasor Measurement Units (PMUs) are installed across transmission lines to get a measurement of voltage and phase shift in a timely manner. Synchro-phasors are measured by PMU, they are synchronized with time for accuracy. PMU is 100 times faster than SCADA system and record the condition of the grid with accuracy. This technology is used for real-time operations. PMUs transmit information on voltage levels and phase angles to help detect faults in real time. FACTS are also deployed by power network. These devices can supply reactive power (inductive or capacitive) efficiently according to the requirement thus improving power quality and transmission line efficiency. After the major development in power electronics, these devices not only make the transmission line performance better but also make it possible to use for long distance.

2.6.2 Automation

Automation is the process of controlling and managing key grid process with human intervention. Power System Automation is divided into different components as per their functions;

- Sensor
- Interface equipment
- Controllers
- Actuators

Figure 2.8 shows the block diagram of process automation.

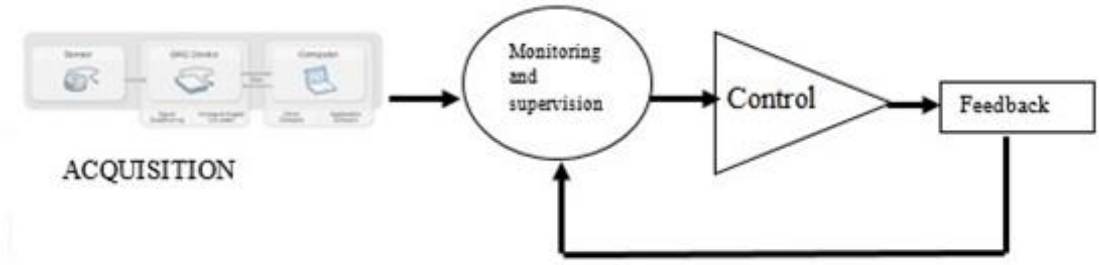

Figure 2. 8 Power System Automation

2.6.3 Substation Automation

Substation automation has drawn the attention in last few decades because it benefits the utility in many ways. Unlike traditional SCADA, it provides better information and has a capability to process further for improved operation and maintenance. Moreover, it gives remote access to the smart electronic devices/relay information, event logging and video coverage for security purposes. It also enables smart metering and voltage/reactive power management. After the addition of latest microprocessor-based relays and other smart devices, rich functionality and flexibility are possible which in turn reduces cost monitoring and diagnosis of faults occurring in the power systems. Many other smart devices/IEDs gives an opportunity to use network interfaces such as internet protocol (IP) and Ethernet etc. For instance, IP network can enhance the capabilities of substation by means of fault analysis and data logging for precautionary maintenance of equipment. Furthermore, fiber optic-based communication is quite common now, utilities use it at some substations. Substation operation can be seen in Figure 2.9.

Figure 2.9 Substation Automation [23].

2.6.4 Distribution Automation

Smart Grid technology is implemented on the electrical grid distribution system, where local power lines and nearby substations are connected. It increases the reliability of distribution system and enhances the utility operation ultimately improving smart control and live monitoring.

The distribution automation revolutionized the control technologies, computing power becomes embedded in the single products in the distribution system. It allows different devices to intellect with the operating conditions of the grid of its surroundings, and according to the requirement, it adjusts its performance to improve the flow of power and its optimization. In case of a fault, an IED can be an important part of the power system which can help avoid fault state efficiently. This process is done in advance that is why there will be an early indication of fault thus enabling the utility to replace the faulty device before an outage. Figure 2.10 shows how IEDs are implemented in a substation a typical substation automation scenario.

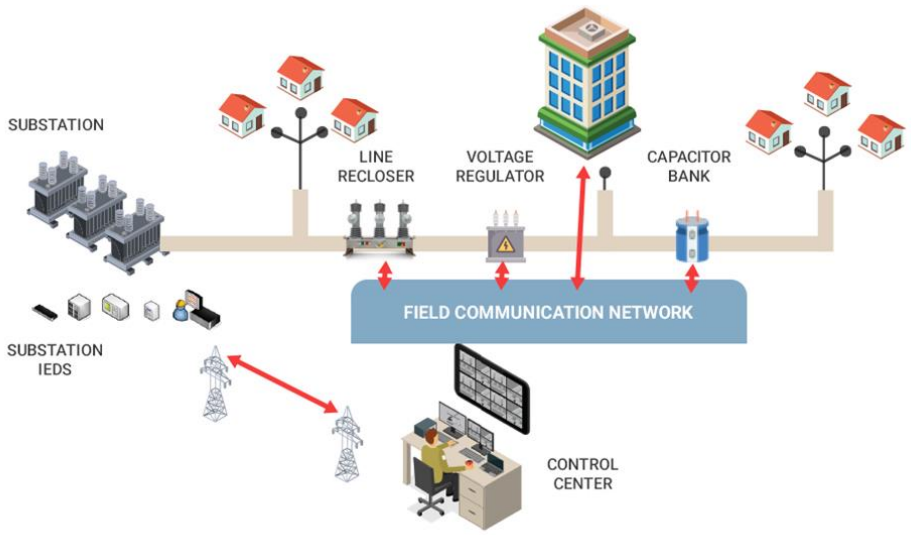

Figure 2.10 Typical Distribution Automation System [24]

2.6.5 Advanced Metering Infrastructure

Advanced metering infrastructure (AMI) is not a single technology, rather it is a completely configured system which should be integrated into old and new power system applications as shown in Figure 2.11. AMI includes domestic network systems, which consist of smart meters, thermostat communication networks for transferring information to data centers and data synchronization into new and existing software platforms. Advanced metering gives an opportunity to the existing power system to update itself according to the new technological system. Smart meters are also the part of the advanced metering infrastructure and is installed on the consumer side to send the readings of power consumed and generated by the customers. Since it is installed at the consumer home, the consumer can be aware of their energy consumption. It also enables the user to utilize energy efficiently by means of the smart thermostat to modulate electricity demand, which also fulfills the scenario of energy conservation. Meanwhile, the utility also employs a current or improved system that collects and analyzes AMI information and data to improve consumer service and operation. For instance, AMI gives a feedback regarding power quality and customer outages to the utility which enables it to find out grid deficiencies.

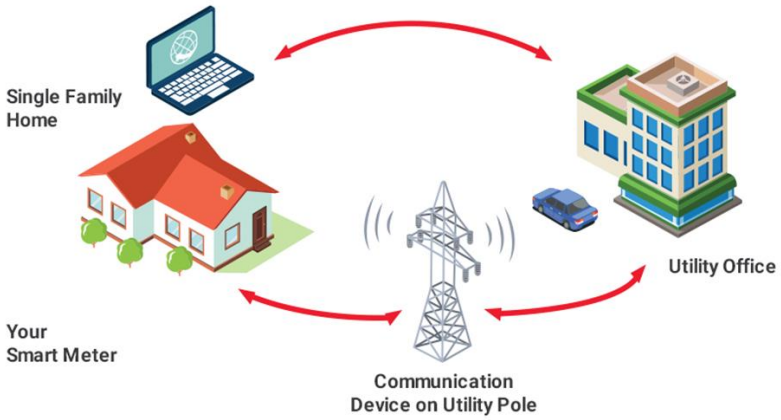

Figure 2.11 Advanced Metering Infrastructure Systems (AMI) [25].

2.7 Cyber Security Objectives

Smart Grid is highly dependent on the communication network. Therefore, there is no compromise in the security when it comes to data transmission and receiving. This is because a slight change in the measurement values could result in a catastrophic condition for the grid. Cybercrime is not new in today's era and SG could also be affected by a minor security breach in the network.

Smart Grid follows three objectives to maintain the cyber security including availability supply, the integrity of network and confidentiality (the most important one) as shown in Figure 2.12. According to the National Institute of Information and Technology recommendations, there is a strong security requirement for both cyber and physical system. Cyber security section defines comprehensive security concerns and a need of secure SG information and network system. Physical security section is concerned with the physical part of the system including equipment, environment issues, and employee security problems. Since the focus of this thesis is limited to data and information network, therefore the issues of physical security are not discussed. A well secured Smart Grid has following attributes:

Availability: Ensures there is a continuous access to use information and data, as reliability is one of the major aspects of SG. Any loss of information could disturb delivery of power to the desired nodes, which could have resulted in the unavailability of required information for the grid.

Integrity: In any network, there is always a chance of receiving false information by means of hacking or any other way. In such condition, it is necessary that the SG infrastructure must not lose its integrity by giving unauthorized access to the network.

Confidentiality: Smart Grid exchange vulnerable information among network which is not appropriate for everyone, there is a restriction on information access to protect personal privacy and information.

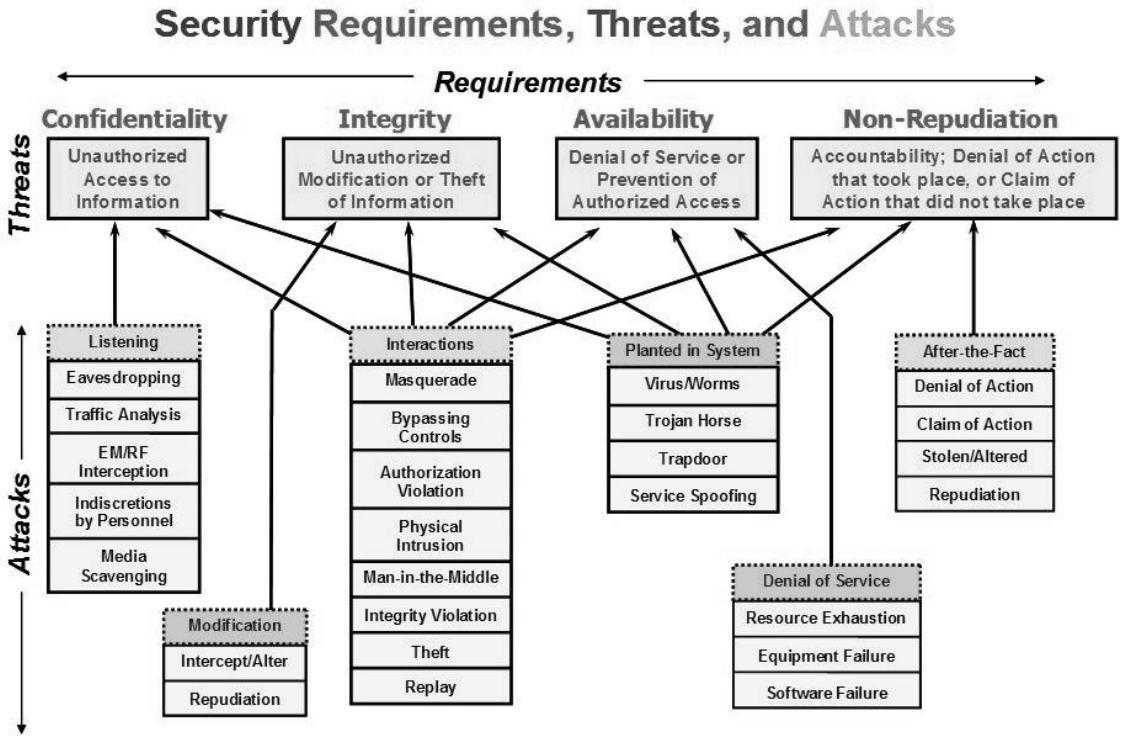

Figure 2. 12 Cyber Security Objectives Requirement [26].

In comparison with traditional power networks, SG must have an attack identification and self-healing operating system. Since it is an open communication network expanded over large geographical locations, it is a daunting task to ensure all part of the node to be highly secured from network threats. Thus, continues operation is required for profiling, comparing and evaluating the network traffic state which is done by a communication network, so that in case of fault there is a clear indication and once the fault is cleared a change in network traffic state must confirm it. In addition to that communication network must possess a resilience property, to ensure proper operation of the system even during the attack. The SG network joins millions of devices and users, there is a requirement of identification and authentication of the connected user to avoid any security breaches. Whenever a device tries to access smart grid information system, it must follow a procedure which includes three steps:

- Identification,

- Authentication
- Access Control

After passing all these steps the specific user may have access to smart grid information system. To ensure the network resources are only used by the authorized person or device and blocks unauthorized users from accessing the vulnerable data and information system. To meet the above scenario, it is necessary that all nodes must be equipped with cryptographic functions for data encryption and authentication. Unlike other conventional networks, information delivery is time critical and security dependent for transmission and distribution automation. Internet and SG usually contrast with each other, as for networks in SG, it cannot always follow secure and protected communication channels. To balance communication efficiency, some compromises are required in the architecture of communication algorithm for the SG. In contrary with the internet, SG follows strong security scenarios to attain secure and effective data delivery for highly critical power systems. The enforcement of conditions of security for communication networks, combined with a physical system to ensure that SG will have a comprehensive safety to complete the goal of internet and energy.

2.8 Smart Grid and Security Threats

Smart Grid covers whole power system of any country, which may have security threats from enemies. It could be an easy target for any rival to destroy power network to break into the utility secretly. Smart Grid security can be compromised by getting access to the communication system which depends completely on a set of networks. Cyber-attacks can interrupt security measures of the SG and it is necessary to comprehend serious weaknesses in the Power Grid in the state of cyber-attack. All possible network attack classes will be discussed in this section, the mainly network system can be classified different classes having different intensity and targets.

2.8.1 Classification of Attacks

Security threats are divided into two types: malicious handlers and existing misbehaving handlers (those who want to take more access than provided as per the user policy). While malicious users have no personal gain in illegally acquiring the network access, still they have an objective to disturb the network data and information. Although both types of users are hazardous for the communication network since both violate the security protocols. In SG, malicious users are more problematic than selfish ones, since thousands of smart devices are acquired for monitoring and controlling the power network. If malicious attacks occur on the network, it could result in a disastrous situation for power system operator's due to the widespread outage. This scenario is not permitted in any power system, especially for SG. In this literature, it is not possible to cover all types of attacks as SG is a huge system having complexity at various levels. Only those attacks will be considered which has a relation with security objectives of SG i.e. availability, integrity, and confidentiality. Availability is closely related to the continuous service supply, so possible attack covers this objective is a denial of service (DoS). In this kind of attack, the user tries to put delays, blockages and corrupt the network communication, it sends and receives false data packets to modify the information in the SG. The only aim in these conditions is to get access to the communication system. Denial-of-service targets one of the objectives of SG which is the availability of service and it is necessary to study network weaknesses in the grid when DoS threat gets activated. Consequences of DoS attacks are severe, it can badly deteriorate the performance of communication system and all make electronic devices defective.

2.8.2 Denial-of-Service attacks

There are many ways to perform DoS attacks including physical layer attacking, media access control (MAC) layer attack, and attacks through transport or network layers. In physical layer attack, the most effective way to launch this attack is through channel jamming specifically for wireless communications. Attackers are only required to get an access through network channels, rather than authorized ones. Thus, it becomes a straightforward task for an intruder to introduce DoS attack at the physical layer. Since SG heavily relies on the wireless technology, wireless network blocking turns out to be the common physical layer attack in such networks. According to the latest study, wireless jamming attacks can be catastrophic as it is responsible for an extensive range of deterioration to the network performance of substation systems, by delaying the transfer of time-dependent information and to complete DoS. Media access control layer attacking is another way to deliberately degrade the performance of the network. Since MAC layer is responsible for trustable P2P communication, an attacker can change the MAC parameters to enter a compromised device so that better opportunities can be utilized for accessing the network by degrading the performances of other devices who are sharing the same channel for communication. Spoofing is more harmful attack since it targets two main objectives of the SG security i.e. availability and integrity. Spoofing is done by changing the opened address field parameters in media access control frame, can disguise itself as an added device to send false data to other electronic devices. For instance, in power distribution system, a defected node broadcast address resolution protocol data to cut off some networks of the power system which could completely change the measurements of the predicted failures. Network layer can also be used to perform DoS attacks. Transfer control protocol model says that the network layer is responsible for delivery of information over a wide communication network. Because of these attacks, ends to end communication efficiency will be degraded severely.

According to recent studies, the transport/network layer DoS attack has a serious impact on the power system performance. The current study on the effect of buffer-flooding on the distributed network protocol-based SCADA network with practical SCADA system software and hardware revealed that SCADA system in the SG can easily be harmed by the DoS attack. Application layer attacks are considered as a lower layer attacking where it focuses on the bandwidth of transmission in communication channels, i.e. routers and computers. It targets CPU or I/O bandwidth of computer, disables the it to utilize its complete capabilities by sending thousands of computationally intensive requests. Smart Grid can be a potential victim of an application-layer denial of service attacks because most of the communication and computing devices are equipped with limited resources for computation. It is noted that in contrast with the internet, SG must have a delay constrained network since any delay in data and information delivery is harmful to power system. Therefore, for SG network, there is no need to completely shut down the system, an intruder can launch a weaker attack to deliberately delay the transmission of time-critical data and information which in result disturb the timing pattern for data receiving and sending. For instance, if attacker delays the message delivery at protection node to trip the specific breaker, it could cause worst scenario for power system infrastructure.

2.8.3 Attacks on Integrity and Confidentiality

These attacks are not like denial of service attacks which could be launched at many layers. Such attacks generally occur at the application layer, as they try to control information in the grid. Attacks on integrity attempt to modify data to damage critical information exchange in the SG. Intruder normally targets customers information and status values of power system because such information is important for both customer and utility companies, different approaches are applied in power system to secure data reliability. There is always a risk of integrity attacks, as such attacks directly violate the protection of SG. False data injection can be done at different levels. For instance, if an attacker changes the phase measurement unit

(PMU) data then there is no other way to predict any failure or maybe there is no failure in actual but due to false data injection, it shows any indication of a power outage in the network. Fake data injection method was designed to affect the state estimation of SCADA system, based on several assumptions that an intruder has already had access to some devices, meters and successfully planted fake data to the SCADA center. Research has been done after the introduction of fake information attack methods, significant research efforts have been done in giving analysis and counter measures such attacks for SCADA system. There is an ongoing research focusing on designing and counterattacking new ways of forge data addition attacks. False data injections scope has been further widened to the electricity market, where a deliberate act to manipulate the market prices for electricity has been implemented. Which couldn't damage SG physically but cannot avoid substantial financial losses. Another special attack can be classified as false data injection attack which is load redistribution attack where measurements at different bus bars and line flow are attackable. According to different research, above attacks are done by gaining access to specific meters to change its recorded value at a certain interval of time.

Intruders aiming privacy have no intentions to change data sent to power networks in comparison with attackers focusing integrity. They usually focus on network communication channels to attain required information, which is customers account details and electricity meter readings. Wiretappers and traffic analyzers are some illustrations of attacks on confidentiality and these attacks have no impact on the operation of communication network but due to increased awareness and information about customer privacy, its social impacts have gained an attention in the recent times. It is noteworthy that space to execute attacks against confidentiality and integrity is that attacker can be authorized to the SG and holding an access to critical data. Therefore, access control and authentication are also vital to avoid smart grid from such kind of attacks.

2.8.4 Smart Grid Critical Security Requirements

In the past, most of the focus was on SCADA Systems and Power Substations while considering cyber security attacks on Grids. Still, communication scenario can be extended to phase measurement unit synchronization in WAN network and smart metering in the advanced metering infrastructure network. To consider a study on Smart Grid security, NIST suggests some cases for security concern. Based on those cases, a complete analysis of network susceptibilities has been provided. These cases are classified into two types: distribution and transmission operation, and AMI and home-area networks. In distribution and transmission operation communication highly depend on time for controlling, monitoring and protection of the power system, any delay in the message delivery could result in extreme condition. Communication is mainly on interactions between customers and utilities in advanced metering infrastructure and home-area networks.

2.8.5 Distribution and Transmission Operation

Distribution and transmission systems are important components in power systems, as these are solely responsible for the delivery of power from the utility to customers shown in Figure 2.13. Millions of power system equipment are deployed for control and monitoring reasons and this equipment’s are integrated with SCADA server for centralized management. For these systems, it is important to have a continuous and reliable operation since any outage in the transmission line can produce instability in the Smart Grid. Meanwhile, confidentiality is not important as there is no such exchange of data.

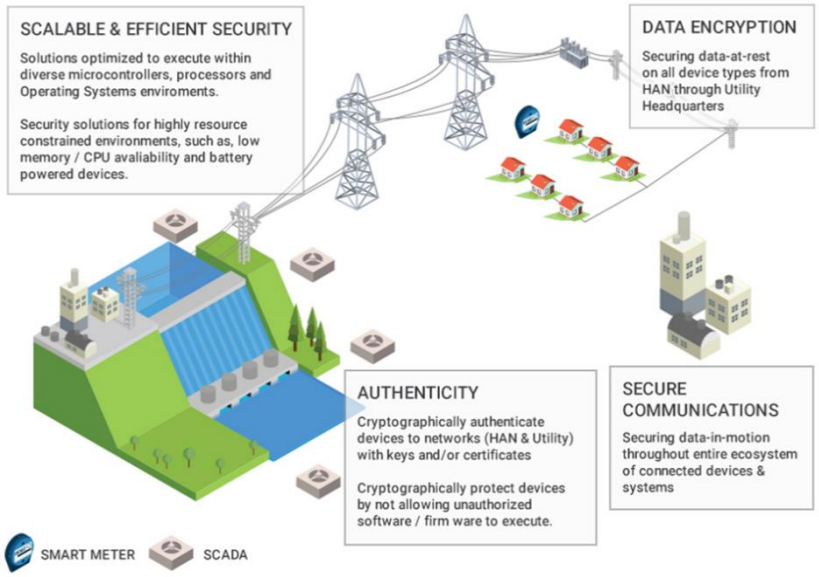

Figure 2. 13 Smart Grid and Security [27]

2.9 Challenges for Smart Grid

Different solutions have already been developed but those solutions cannot be applied to SG system as it is a time critical system. Smart Grid carries different security threats and for that reason, it has different security objectives. For instance, it focuses on the human safety, equipment, and transmission line protection etc. While IT network considers three objectives of security which are confidentiality, integrity, and availability. In addition, the conventional network provides extra protection at the centralized network where all the data locates, but in SG, security is required at the edge and center of the network. The conventional network has a well-defined operating systems and protocols but for SG, different operating systems and protocols are required at different levels. Service quality is measured differently in IT network, under fault conditions it is acceptable to restart the devices but for SG availability is an important aspect of the security, there must be a continuous supply of data and information all the time. These differences create a barrier between SG system and conventional IT system, there is a need of different security solutions for SG since solutions available in IT network systems cannot be applied to the SG due to the difference in security objectives.

The major challenges in SG security are shown in Figure 2.14. Some of the major challenges that SG is going to face are that these systems are designed without considering the preventive measures for security, all the new security features must not have any effect on the performance of grid functionality, wireless access to electronic devices must be controlled and monitored efficiently and all the proposed new solutions must be capable of adopting all smart grid features.

After considering all the security threats a SG will have in future, some solutions must be proposed based on following criteria:

- Authentication process must be efficient enough such that network access is given only after following the complete access flow mechanism.
- Virus protection must be available for embedded systems since they rely heavily on software supplied by the company, in addition, it is the responsibility of a supplier to provide a secure storage for a customer so that no one else can use the specific software without authentication.
- An assessment must be done yearly to identify weakness in the current system to make sure that the network can identify new security threats. All devices must have clear information about the source and destination where they receive and send data and it can be done using IP security.

Figure 2.14 Challenges for Smart Grid [28].

CHAPTER 3

Smart Grid Model

This chapter covers the basic knowledge of electrical power circuits having an alternating current. It is divided into two parts, in the first part basic concepts of electrical grid is discussed. Smart Grid modelling is discussed in the later part of this chapter which is also shown in Figure 3.1.

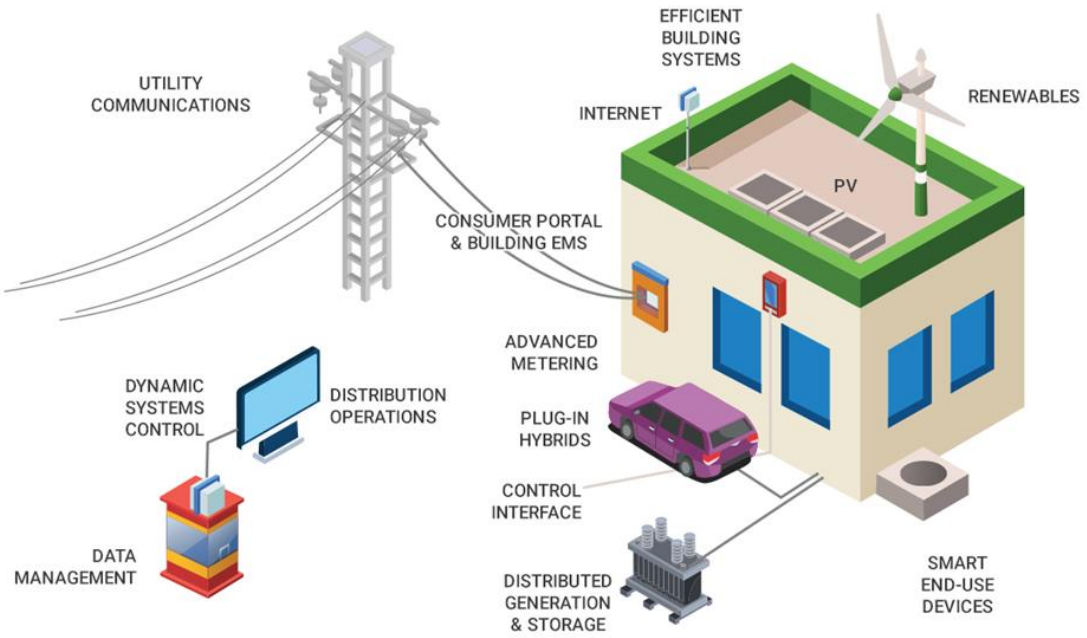

Figure 3.1 Smart Grid Model [29].

3.1 AC Circuits Basics

AC circuits produce sinusoidal voltage and current, its phasor representation is given by the following equation.

$$Y(t) = Y_m\,(sin\,\omega t + \phi) \tag{3.1}$$

Where Y_m is the maximum amplitude of the waveform, sin functions represent the sinusoidal shape of the waveform, ω is the radial frequency given in rad/sec, t is the time of waveform and can be calculated using the ratio of 2π & ω and ϕ is the phase shift produced in the circuit. Above equation was derived by maximum amplitude (Y_m) and phase shift (ϕ), where these parameters are defined by a complex number having magnitude of $Y_m/\sqrt{2}$

$$y = \frac{Y_m}{\sqrt{2}}\, e^{i\phi} \tag{3.2}$$

Above equation is called phasor, while its magnitude can be represented by rms of Y(t).

Where $Y(t) = \frac{Y_m}{\sqrt{2}}$

$$Y(t) = \sqrt{\frac{1}{T}\int_{t0}^{t0+T} a^2(t)dt} \tag{3.3}$$

Where T is the total period of waveform, during the ideal sinusoidal working of grid, both voltage and currents are sinusoidal signals having 50 Hz frequency for Europe and 60 Hz for America. Mathematically below equations express the condition for voltage and current.

$$\mathrm{I(t)} = \mathrm{I_m}(\sin \omega t + \phi_i) \tag{3.4}$$

$$\mathrm{V(t)} = \mathrm{V_m}(\sin \omega t + \phi_v) \tag{3.5}$$

Where

$$i = \frac{i_m}{\sqrt{2}}\, e^{i\phi_i}\,,\; v = \frac{V_m}{\sqrt{2}}\, e^{i\phi_v}$$

Units for voltage and current are volts and amperes respectively.

Resistance, Impedance and Admittance:

For DC circuits, resistance is represented by the ratio of voltage and current. While in AC circuits, impedance is considered as the summation of resistance and reactance which include complex components as well (i.e. X_L and $X_{c)}$. It is also calculated by the same method as for resistance, but impedance will have phase shift due to AC signal voltage and currents. Unit for both resistance and impedance is ohm.

$$R = \frac{V}{I} \tag{3.6}$$

$$Z = \frac{V<\theta}{I<\theta} \tag{3.7}$$

$$Z = R + jX \tag{3.8}$$

Where R is the resistance and X is the reactance.

Inverse of impedance is called admittance which is the ratio of current and voltage in any circuit and is represented by Y and its units is Siemens (S). It is also a complex identity consisting of two parts Conductance (G) and Susceptance (B).

$$Y = \frac{I}{V} \tag{3.9}$$

$$Y = G + JB \tag{3.10}$$

Power in AC circuits:

Power is the product of Voltage and Current. Instantaneous power is defined as

$$P(t) = V(t)I(t) \tag{3.11}$$

$$P(t) = V_m(\sin \omega t + \phi_v) \text{ x } I_m(\sin \omega t + \phi_i) \tag{3.12}$$

$$P(t) = \frac{V_m I_m}{2} \cos \phi - \frac{V_m I_m}{2} \cos(2\omega t + \phi_v + \phi_i) \tag{3.13}$$

where $\theta = \phi U - \phi I$.

Instantaneous power is not helpful to define power transmission and consumption, since in power systems there is more interest in understanding the power sent and received in a time interval greater than 1/60 of a second. That is why an expression is required to get average power for complete cycles for voltage and current and that average power is called active power for any system. It is defined as power consumed in a specified interval of time.

$$P = \frac{1}{T}\int_{to}^{to+T} dt \tag{3.14}$$

$$\mathrm{P} = \frac{\mathrm{V_m I_m}}{2}\cos\theta \tag{3.15}$$

Active power is the power transmitted, generated or consumed by loads or generator. It is measured in watts (W).

Apparent power defines the capacity of equipment and is defined as the power generated by a generator measured in VA (volt-ampere). As operating voltage of any equipment is constant, so current can easily be find out by using apparent power. Hence, equipment ratings are given in volt-ampere (VA).

Another type of power required in transmission and distribution is reactive power which is produced due to reactive component in the power system. It is denoted by Q, and given as:

$$Q = \frac{I_m V_m}{2}\cos\theta \tag{3.16}$$

Since it is consumed by inductive load and generated by capacitive load, it oscillates back and forth through the devices without getting dissipated. From Figure 3.2 it is seen that the reactive power is at the perpendicular which means it is an imaginary part of power while real power is at base which shows that it is a real component having no phase shift.

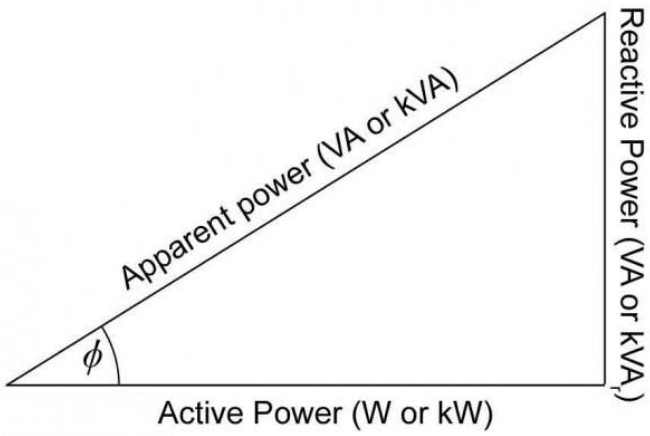

Figure 3.2 Power Triangle

$$P = Re(S)\cos\theta \tag{3.17}$$

$$Q = Im(S)\cos\theta \tag{3.18}$$

3.2 Smart Grid as Cyber Physical Power System

The system that connects the cyber world of computing with the physical power world is referred as cyber physical power system. Communication techniques are used almost everywhere in all types of systems and structures and their operations are closely monitored, controlled, integrated and coordinated by a communication core. Smart Grid is considered as a smart distribution network having two layers including cyber layer and physical layer as shown in Figure 3.3. Cyber layer covers intelligent sensors having sensing, actuating, communication and computational capabilities. While, physical layer carries power generation and distribution systems, which include transmission lines, micro generators, loads and substations.

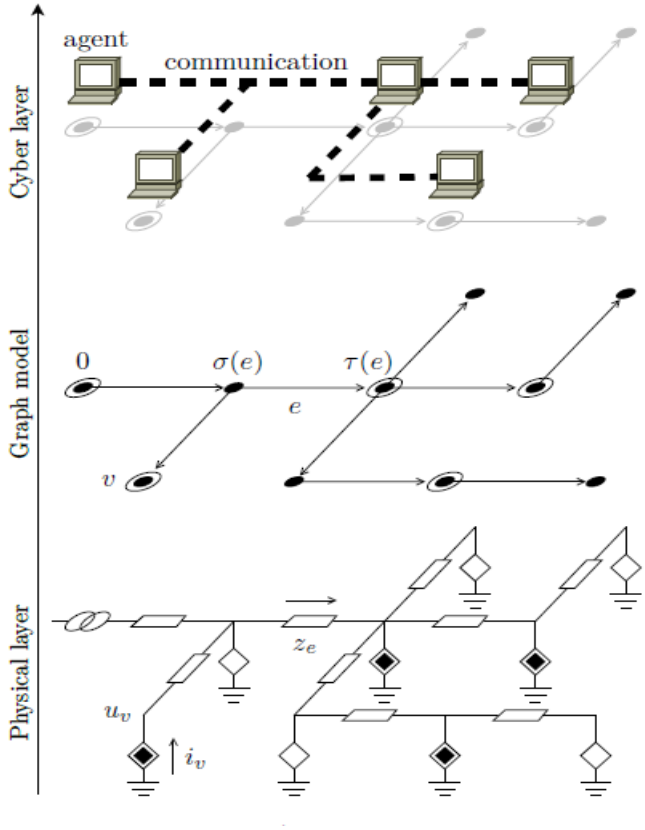

Figure 3. 3 Smart Grid distribution model [57]

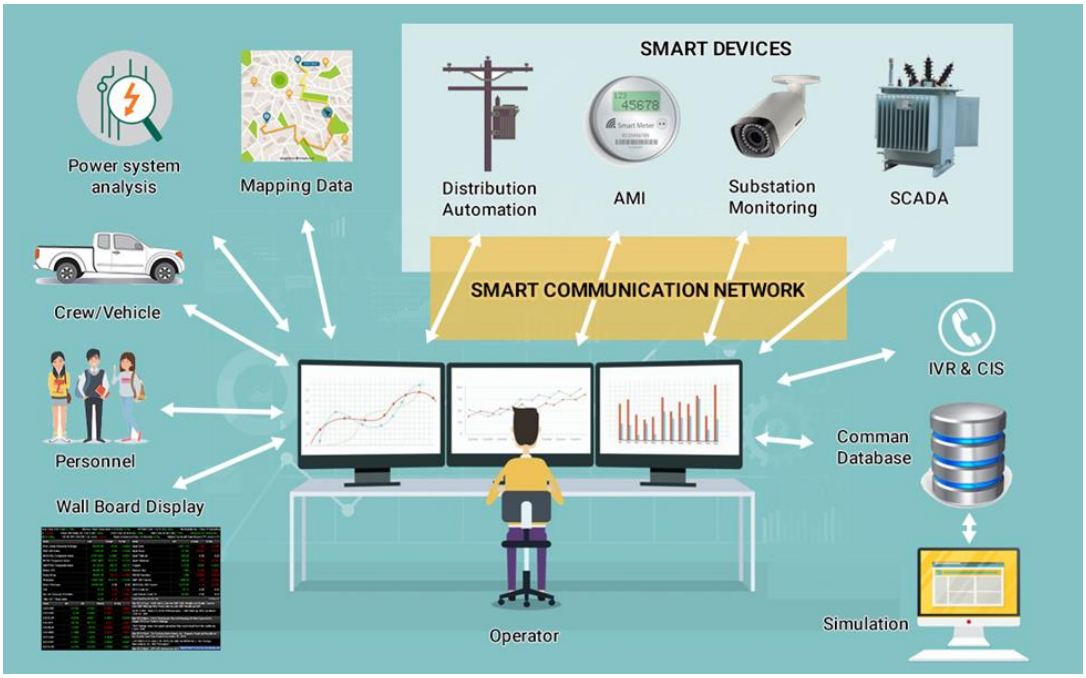

Figure 3.4 Smart Communication [30]

3.3 Electric Grid Model

3.3.1 PHYSICAL LAYER

In Figure 3.4, SG distribution model is shown which consists of three models including physical layer, cyber and graph. Physical layer (Smart Distribution Network) modelled as an equivalent graph given that G = (V, E, σ, τ), where power lines are represented by edges and buses are represented by nodes. Where V is the set of nodes and E is the set of edges for connecting transmission lines. Nodes (Buses) coordinate with loads, generators and PCC (Point of Common Coupling) to the transmission grid.

Above model is described by following quantities

- u_v is the voltage at grid for node v
- i_v is the current injected at node v
- e_e is the current at the edges.
- s = p +iq, where Sv is the apparent power injected at node v, Pv is the real power absorbed at node v and Qv is the reactive power at node v. If real power > zero, then v is injecting real power, if real power < than zero that means it is absorbing real power.

Smart signals and passive loads can be differentiated by the vector of voltages u, as shown below.

$$u = \begin{bmatrix} u1 \\ uG \\ uL \end{bmatrix}$$

Where u1 = voltage at the point of common coupling, uG = voltage at the generation node, ul = voltage at the loads, likewise

$$S_G = P_G + jQ_G \tag{3.19}$$

$$S_L = P_L + jQ_L \tag{3.20}$$

3.3.2 CYBER LAYER:

It is assumed that all the generators or agents and point of common coupling (PCC) communicate through cyber layer. In a Smart Grid, a generator can sense voltages and phase angles using PMU (Phasor Measurement Unit) and this all information is exchanged through cyber layer. Agent also has a capability to perform computational operations which also include implementation of algorithms. However, to send all this information additional communication capability is required. It is also required to have some knowledge of grid parameters including impedance of the line etc.

3.3.3 POWER FLOW IN GRID:

Power flow issue is related with defining the operating state of a power system. AC circuit requires only two types of information on each node to get the complete information. If there are n buses, there is a need to find n complex variables or 2n real variables to find out the exact grid state. A node is divided into three different types:

1. **PQ node**: It is also called load bus, since power absorbed or injected is not dependent on voltage.
$$s = p + iq \tag{3.21}$$
2. **PV node**: It is also called voltage bus, as voltage across this node is fixed, only active power can be absorbed from this bus.
3. **SLACK node**: The node where slack generator is connected is called slack, voltage at this node has no phase shift as main generator is connected on this bus.

For any grid, it is necessary to have at least one slack bus to provide reference point for the whole power system.

CHAPTER 4

Proposed Work

For any power system, it is very difficult for a system operator (SO) to respond swiftly during a fault state to restore the operation of electric power supply after any power outage. Most of the outage management systems follow the method of call aggregation which takes a relatively longer time to identify the faulty device or line. For SG, it is necessary to have an automatic fault detection scheme which improves the stability of the power system. The traditional grid is not equipped with the instruments which can take enough measurements of the distribution network equipment to find the faulty area. Various approaches have been tried to resolve this problem. The current work is focussed to find the best solution for the above stated problem by comparing the results of different existing methods, based on the results obtained from the different method we can comment on the effectiveness of algorithms.

4.1 Analysis of Existing Fault Detection Techniques

Power line outage is a widespread problem faced by power systems. It is important to have complete knowledge of transmission line when there is a need of fault rectification in power grid. In 2003, a blackout in the northeast USA demanded the need of real-time line monitoring for the whole power system. PMUs solved this issue up to some extent by providing direct usage of measurements taken to find out faults in the grid. Currently, PMU based method is the most effective way to find line outage in the power system. Present PMU-based methods for line outage detection use the information from internal and external network model of the complete system to identify the line outages. Single Line Outage Detection Using Phasor Angle Measurements method is one of the methods for line outage detection. However, it contains a

long searching process to get information about the outaged line and works only for single line outage problem. However, the above method is improved to detect double line outage as well but still it requires many more iterations to get the required result.

Single line outage method detects system events with the help of PMU, transformer parameters, and transmission line data. This method follows an assumption that after any fault, the system settles down into a stable state. Once the transients have been removed in response to the fault, phase difference values at the specified buses with respect to pre-event values must be determined. It is essential to find out steady state changes in the phase angles to examine the possibility of a fault occurred in the system.

In another study under the name of "Monitoring for Power-line Change and Outage Detection in Smart Grid via Alternating Direction Method of Multipliers" [18] a different approach was considered based on the wide area measurement systems (WAMS). In this method, PMUs are deployed at various locations in the buses. PMUs are responsible for the measurement of phasors and voltages at the buses. Phasor data concentrator (PDC) are used at the higher levels to collect data from PMUs in the defined regions. After that the method for line outage detection is implemented and the results are transmitted to WAMS to send the collected information to system operators.

Above two methods are considered for this thesis and the results are compared to see the difference between both methodologies. The comparison is done in terms of computational complexity, calculations, and accuracy.

4.2 Computational Techniques

4.2.1 Single Line Detection Using PMU Data:

In this algorithm detection of system events is done using PMU data, such as the phasor angles from the transmission lines and information on interconnections of the system **[7]**. The fast oscillation in phasor angles is not being evaluated and it is assumed that only quasi-steady state values of the measured phasor angles before and after the disruption are compared [7]. Change in phasor angle is Δθ, while K is the number of phasor angles detectable at PMU [7].

$$E^* = arg\,min\,||\,\Delta\theta_{observed} - f(E)|| \tag{4.1}$$

Where E = set of events to be monitored, $f(E)$ relates to an event E as a function to the changes in angle due to the event occurred.

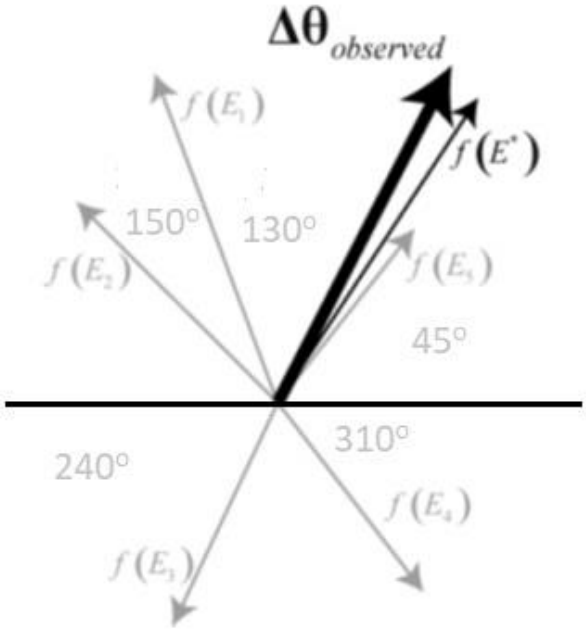

Figure 4.1 **Resolving phasor angles to determine the event that matches the angle changes [7]**

Figure 4.1 shows a visual illustration of the above equation, however, it is limited to a two-dimensional array, while equation (4.1) works for K-dimensional array for phasor angles. According to the above figure, f (E1-5) are least matched events and are coloured grey, whereas

f (E*) event is best matched. This method is for single line detection. It uses PMU measurements and information from transmission lines and transformers to find the accurate node where outage takes place. In addition, this method focuses on the pre-outage flow values of the faulty system. A method of edge detection technique was also used to estimate the occurrence of events as shown in figure 4.1. To achieve the objective in this method, it is necessary to measure the change in angles at the quasi-stable state. Any rapid oscillation in the phase angle needs to be filtered out so that the original signal is extracted only, and low pass filters are used for this purpose.

4.2.2 Multiple Scattered Line Outage Detection

The main objective of this algorithm is to design a multiple scattered line outage scheme where the outage is on more than two lines in different geographical locations. The technique which is employed to detect multiple line outage is called Wide Area Measurement (WAMS) for SG **[18]**. A basic WAMS architecture is shown in Figure 4.2. A Certain number of PMUs are installed in the buses in each area of WAMS, which measure bus voltage phasor and branch-current phasors that applied to the selected buses. This information is then passed on to the phasor data concentrator (PDC). The algorithm is then applied to the data of each PDC separately to detect line outage. The information is then transferred to WAMS and is further passed on to the SCADA system to enable it to take appropriate action **[18].**

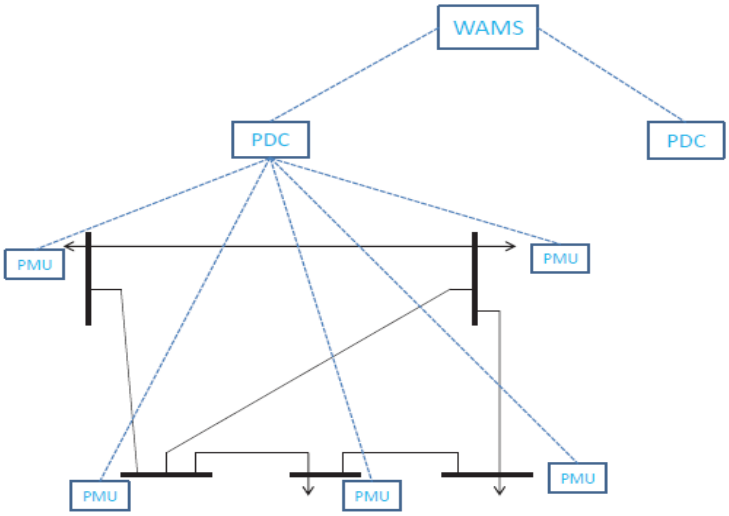

Figure 4. 2 Basis WAMS Architecture [18].

For a typical transmission system, phasor measurement information is expressed in terms of rectangular components of a vector; and $\bar{Y}_n$ can be expressed by the following linear equation [18].

$$\bar{Y}_n = \overline{H_n x} + \overline{g_n} \tag{4.2}$$

Where x = State of the system having all line currents

$\overline{H_n} \in R^{Mn\ x\ 2Ni}$ is the measurement matrix,

M_n = Number of measurements within n-th PDC area.

N_l = Number of lines in the whole system

$\overline{g_n}$ = Additive Guassian noise vector

In this scheme, to perform line outage detection, measurement and prior information of the states are combined [18]. The statistics of previously stored data of line current is denoted by $\bar{x}$, which have normal distribution having mean vector xp and covariance matrix Λp. It is

assumed that the state variables are independent, which indicates Λp is diagonal. At this point, let us assume one central control centre processes the measurements to detect line outage and employ li-norm approximation, leading to the convex optimization criterion below.

$$min_X \frac{1}{2}\|y - Hx\|_2^2 + \lambda \left\| \Lambda_P^{-\frac{1}{2}}(x - x_P) \right\|_1 \tag{4.3}$$

If above equation is decomposed into N PDC areas, then it can be expressed as

$$\min_{Xn} \sum_{n=1}^{N} fn(Xn) \tag{4.4}$$

According to the "cost function" for each PDC is

$$fn(Xn) = \frac{1}{2}\|Yn - \boldsymbol{H_n} X_n\|_2^2 + \Lambda_{pn}\frac{-1}{2}\|(X_n - X_{pn}) \tag{4.5}$$

Where Xn, Hn, Λn, and Xpn are the states involved in n-th PDC. Now, derivation to solve the optimization problem in equation (4.5) is done in a distributed manner. Take xn as the subset of x, which has the states for n-th PDC and also consider Xnm as the value for sharing different states among neighbouring n-th and m-th PDC. Equation (4.3) can be rewritten as

$$\min_{Xn} \sum_{n=1}^{N} fn(Xn) \tag{4.6}$$

Now Alternating Direction Method of Multipliers (ADMM) [18] can be applied from equation 4.1 to solve the line outage detection problem derived in equation 4.5 having a distributed mechanism. Xnm and Zn are introduced as auxiliary variables to be considered for ADMM framework. Equation 4.5 can be expressed as

$$\begin{aligned} &minimize \sum_{n=1}^{N} f_n(x_n) \\ &subject\ to\ \ X_{nm} = v_{nm}\ , m \in N_n; m \in P \\ &X_n - X_{pn} = Z_n \end{aligned} \tag{4.7}$$

This method is also used for transmission line outage detection. However, it follows a different procedure since the convex relaxation technique is applied to find out line failures using the same scenario as in the single line detection technique, where numbers of PMU are limited. In the current thesis, ADMM is also applied to avoid complex computation as in other PMU-based outage detection methods using the 9-bus system as a model shown in Figure 4.4. Although all these methods take raw data that may encounter security issues as well, this method has a limited number of PMU data and there is no use of raw data in order to calculate outage line detection. They use the network of WAMS, in which each area has a number of PMUs installed at the buses to measure bus voltage phasors and branch current phasors that are applied on certain buses. It also uses the phasor data concentrator (PDC), which takes data from the PMU in its area and then a line detection algorithm is applied, but only the calculations after fault detection are sent to WAMS.

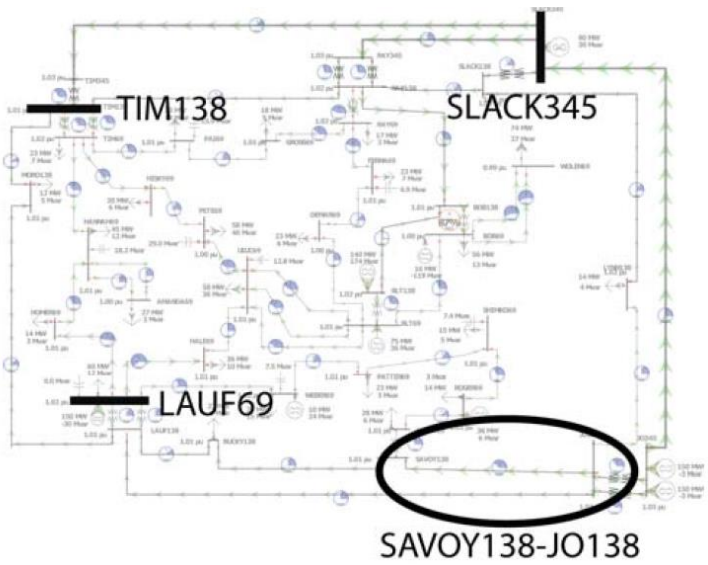

Figure 43 Single Line Diagram 37 Bus System Used for Single Line Detection Method [7].

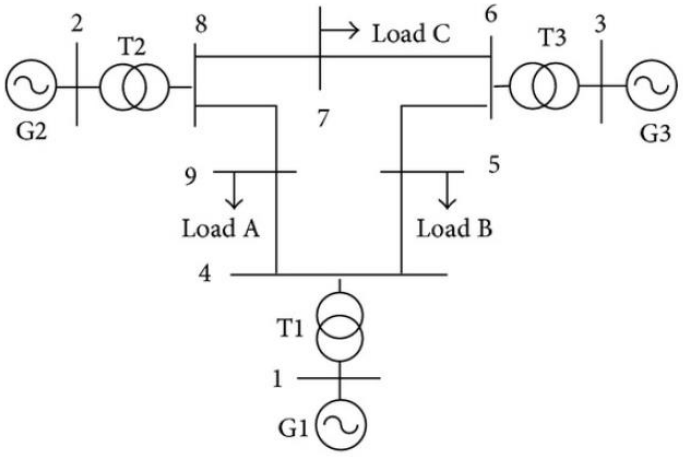

Figure 4.4 Bus test system used in Monitoring for Power-line Change and Outage Detection in Smart Grid Via the Alternating Direction Method of Multipliers.

CHAPTER 5

Results and Discussion

In this chapter, some test cases are considered to test the algorithms discussed in Chapter 4 to distinguish the more robust method of fault detection. It is necessary to have a scheme for the test cases as topologies are designed for SG. Two test cases are considered: one is based on IEEE 9-Bus system and the other is based on IEEE 39-Bus system. As these two cases are primitive, some modifications were required. For instance, the original test cases only utilize commonly used generator types and no renewable energy sources are considered. Now a days, a bulk of energy is provided by renewable energy sources (RES) so there is a need of some distributed generatin connected with the system. In the first phase, test systems with the existing values are shown and then modifications are made to match it with today's SG.

5.1 Introduction to Power World Software

All the test cases use Power World Software and it is a commercial program practice by different power companies in the world. It has the capability of exploring a power system in different ways, such as area transaction economic analysis, short circuit analysis, contingency analysis, DC power flow, power transfer distribution factor (PTDF), contingency analysis and PV/PQ analysis. The software has a load flow solution engine and any power system can be implemented on it using its attractive visual interface or even through text input. For the study of 14-bus and 39-bus system uniform frequency of 50Hz will be considered, since all buses can measure voltage and phase angles we can say all buses contain PMUs. Power World enables to evaluate the whole power system at each instant of time to get the correct measurements before and after the fault arises. All the generators have AVRs that regulate at a scheduled voltage for all PV buses as long as it follows generator MVAR capability limits.

Transmission lines follow pi-model containing all the practical parameters i.e. resistance, reactance and shunt impedance. All loads will be considered as constant value loads. For the testing purpose, all generators are modeled as round rotor machines with quadratic saturation having IEEE Type 1 exciter.

5.2 14-Bus Test System

The 14-bus system represents an equivalent American Electric Power system as of on February 1962. It consists of 14 buses, 5 generators and 11 loads as shown in Figure 5.1 and 5.2. It has five synchronous machines modeled as generators having IEEE type-1 exciters, three of them are synchronous compensators used for reactive power generation. There are a total of 11 loads connected in the system, taking 259 MW and 81.3 MVar.

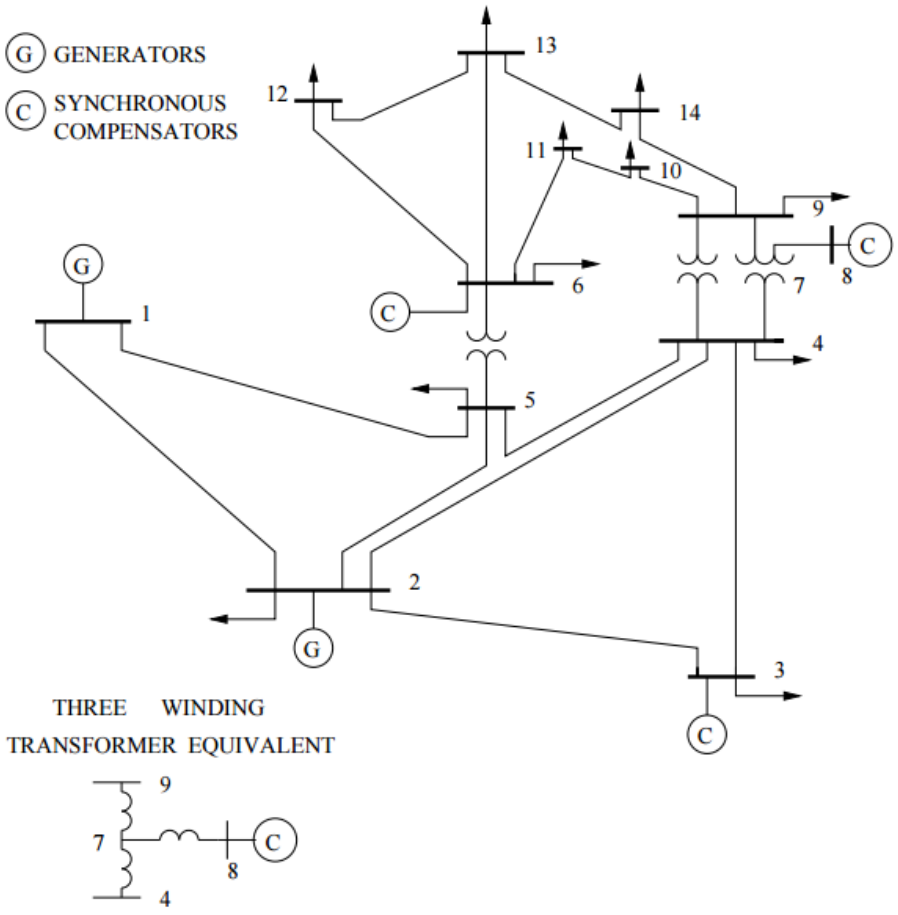

Figure 5.1 IEEE 14-Bus System [33]

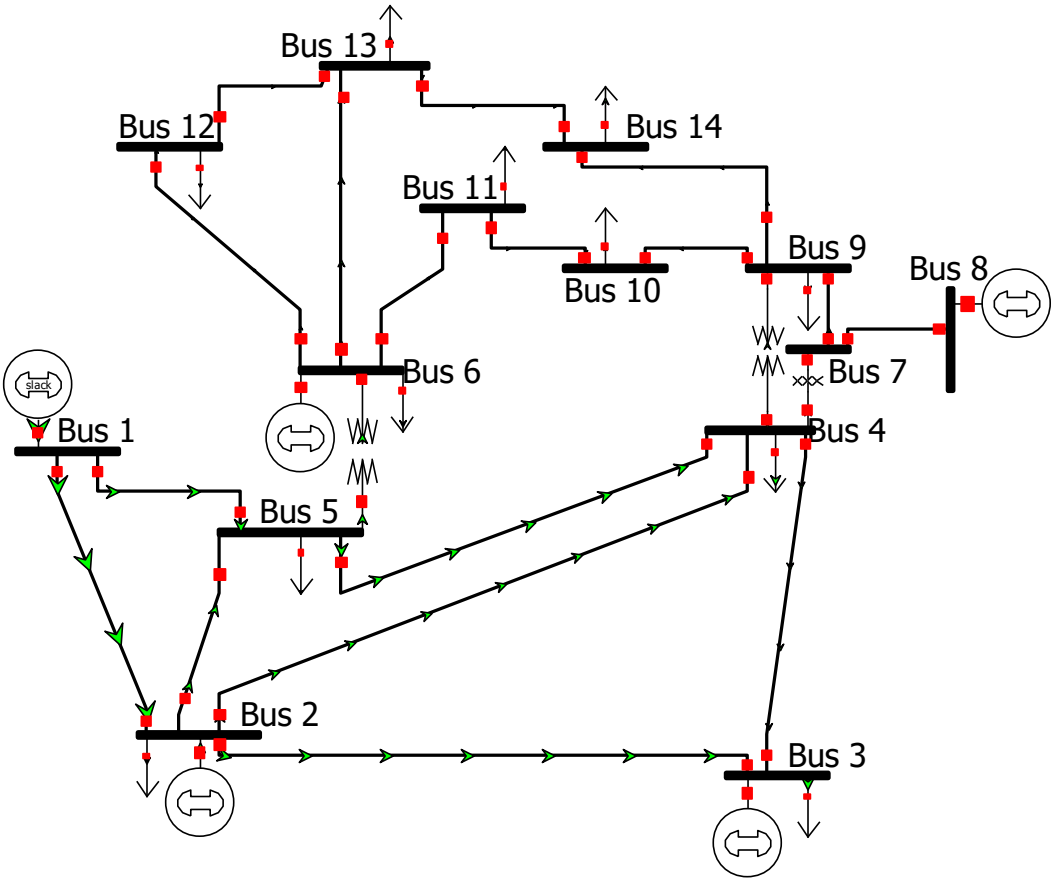

Figure 5.2 IEEE 14-Bus System (Powerworld) [33]

Results and Discussion

BUS PARAMETERS

The below tables show the exact bus parameters

Table 5.1 Bus data [33]

Bus	Type	Pd (MW)	Qd (Mvar)	V (pu)	θ
1	3 (Swing)	0	0	1.06	0
2	2 (PV)	21.7	12.7	1.045	-4.98
3	2 (PV)	94.2	19	1.01	-12.72
4	1 (PQ)	47.8	-3.9	1.019	-10.33
5	1 (PQ)	7.6	1.6	1.02	-8.78
6	2 (PV)	11.2	7.5	1.07	-14.22
7	1 (PQ)	0	0	1.062	-13.37
8	2 (PV)	0	0	1.09	-13.36
9	1 (PQ)	29.5	16.6	1.056	-14.94
10	1 (PQ)	9	5.8	1.051	-15.1
11	1 (PQ)	3.5	1.8	1.057	-14.79
12	1 (PQ)	6.1	1.6	1.055	-15.07
13	1 (PQ)	13.5	5.8	1.05	-15.16
14	1 (PQ)	14.9	5	1.036	-16.04

Table 5.2 Generator data [33]

BUS	Pg (MW)	Qg (Mvar)	Qmax	Qmin	Vg	Pmax
1	232.4	-16.9	10	0	1.06	332.4
2	40	42.4	50	-40	1.045	140
3	0	23.4	40	0	1.01	100
6	0	12.2	24	-6	1.07	100
8	0	17.4	24	-6	1.09	100

Table 5.3 Branch data [33]

Branch no	From Bus	To Bus	r	x	b
1	1	2	0.01938	0.05917	0.0528
2	1	5	0.05403	0.22304	0.0492
3	2	3	0.04699	0.19797	0.0438
4	2	4	0.05811	0.17632	0.034
5	2	5	0.05695	0.17388	0.0346
6	3	4	0.06701	0.17103	0.0128
7	4	5	0.01335	0.04211	0
8	4	7	0	0.20912	0
9	4	9	0	0.55618	0
10	5	6	0	0.25202	0
11	6	11	0.09498	0.1989	0
12	6	12	0.12291	0.25581	0
13	6	13	0.06615	0.13027	0
14	7	8	0	0.17615	0
15	7	9	0	0.11001	0
16	9	10	0.03181	0.0845	0
17	9	14	0.12711	0.27038	0
18	10	11	0.08205	0.19207	0
19	12	13	0.22092	0.19988	0
20	13	14	0.17093	0.34802	0

5.3 Modified 14-Bus Test System (Power world)

After following all the steps mentioned in appendix A, 14-Bus model has been modified to A Smart Grid model which has renewable energy sources in addition to the conventional ones. Figure 5.3 demonstrates a modified 14-Bus system with all characteristics that Australian Power Network carries.

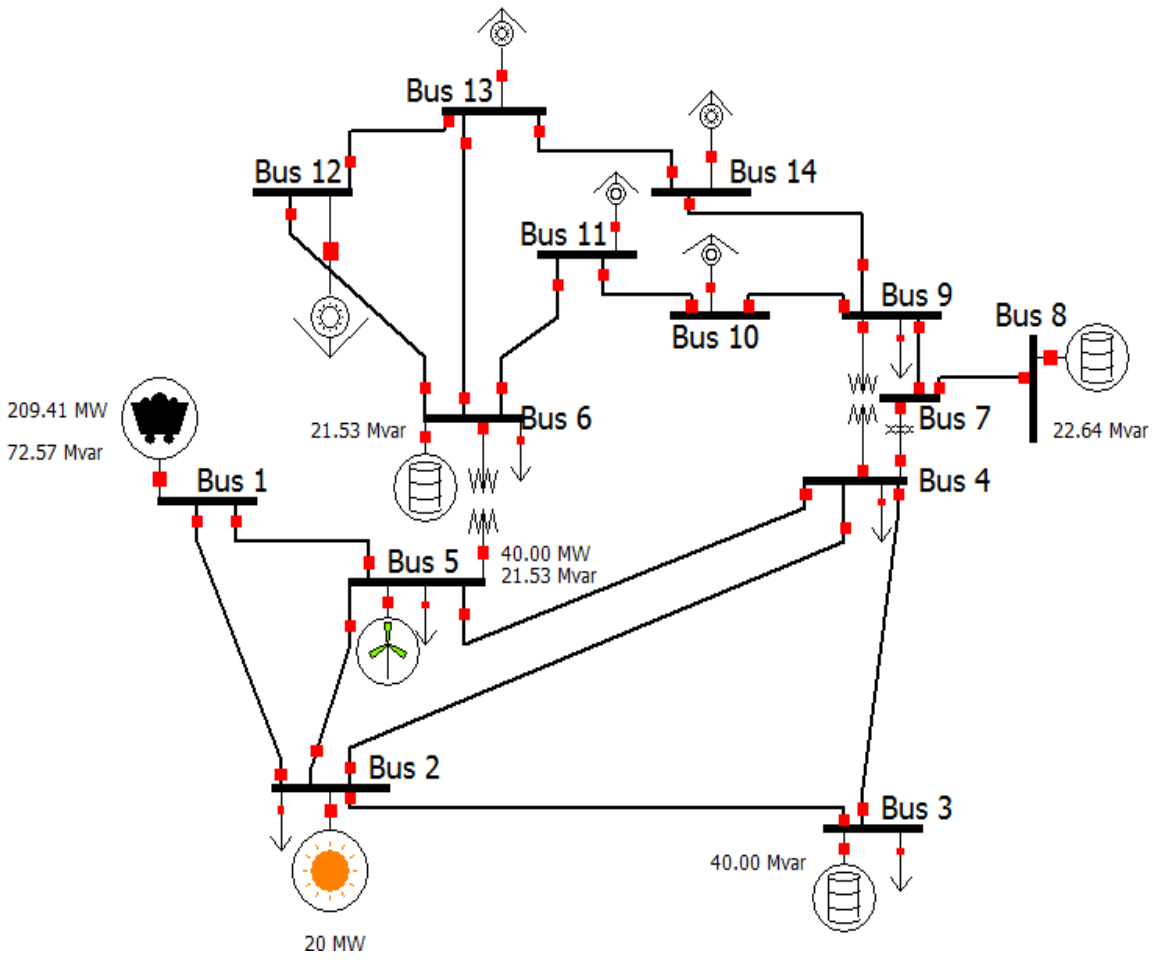

Figure 5.3 IEEE 14-BUS Modified System (Powerworld)

Results and Discussion

BUS PARAMETERS

The below table shows the bus parameters after modification.

Table 5. 4 Bus Data

BUS	Type	Pd	Qd	V (pu)	□
1	3 (Swing)	0	0	1.06	0
2	2 (PV)	21.7	12.7	1	-4.03
3	2 (PV)	94.2	19	0.992	-12.06
4	1 (PQ)	47.8	-3.9	1.00002	-9
5	1 (PQ)	7.6	1.6	1.00539	-7.11
6	2 (PV)	11.2	7.5	1.07	-12.69
7	1 (PQ)	0	0	1.05341	-11.96
8	2 (PV)	0	0	1.09	-11.96
9	1 (PQ)	29.5	16.6	1.04791	-13.48
10	1 (PQ)	9	5.8	1.04439	-13.62
11	1 (PQ)	3.5	1.8	1.05353	-13.28
12	1 (PQ)	6.1	1.6	1.05515	-13.5
13	1 (PQ)	13.5	5.8	1.04956	-13.59
14	1 (PQ)	14.9	5	1.03099	-14.49

Table 5.5 Generator Data

BUS	Pg	Qg	Qmax	Qmin	Vg	Pmax
1	209.41	72.57	0	0	1.06	10000
2	20	-77.1	9900	-9900	1	1000
3	0	40	40	0	1.01	10000
5	40	0	0	0	1	1000
6	0	21.53	24	-6	1.07	10000
8	0	22.64	24	-6	1.09	10000

Table 5. 6 Branch Data [33]

Branch no	From Bus	To Bus	r	x	b
1	1	2	0.01938	0.05917	0.0528
2	1	5	0.05403	0.22304	0.0492
3	2	3	0.04699	0.19797	0.0438
4	2	4	0.05811	0.17632	0.034
5	2	5	0.05695	0.17388	0.0346
6	3	4	0.06701	0.17103	0.0128
7	4	5	0.01335	0.04211	0
8	4	7	0	0.20912	0
9	4	9	0	0.55618	0
10	5	6	0	0.25202	0
11	6	11	0.09498	0.1989	0
12	6	12	0.12291	0.25581	0
13	6	13	0.06615	0.13027	0
14	7	8	0	0.17615	0
15	7	9	0	0.11001	0
16	9	10	0.03181	0.0845	0
17	9	14	0.12711	0.27038	0
18	10	11	0.08205	0.19207	0
19	12	13	0.22092	0.19988	0
20	13	14	0.17093	0.34802	0

5.4 39-Bus Test System

A 39-bus system shown in Figure 5.4 and 5.5 is used for testing purposes. It is modeled as 100 MVA base with 10 generators, 19 loads and 46 lines. The system is based on a 345 kV equivalent model of New England Power System, USA.

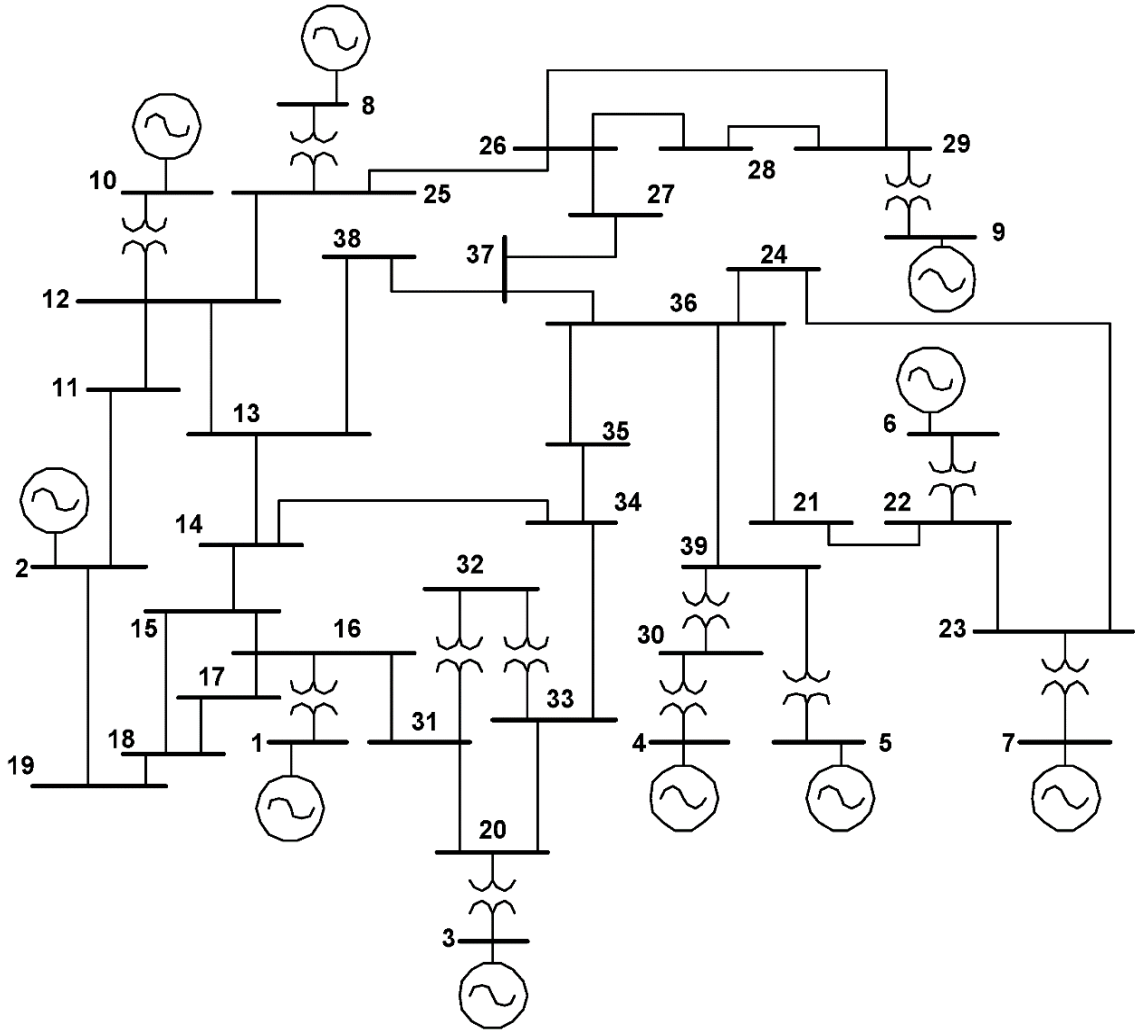

Figure 5.4 IEEE 39-Bus System [33]

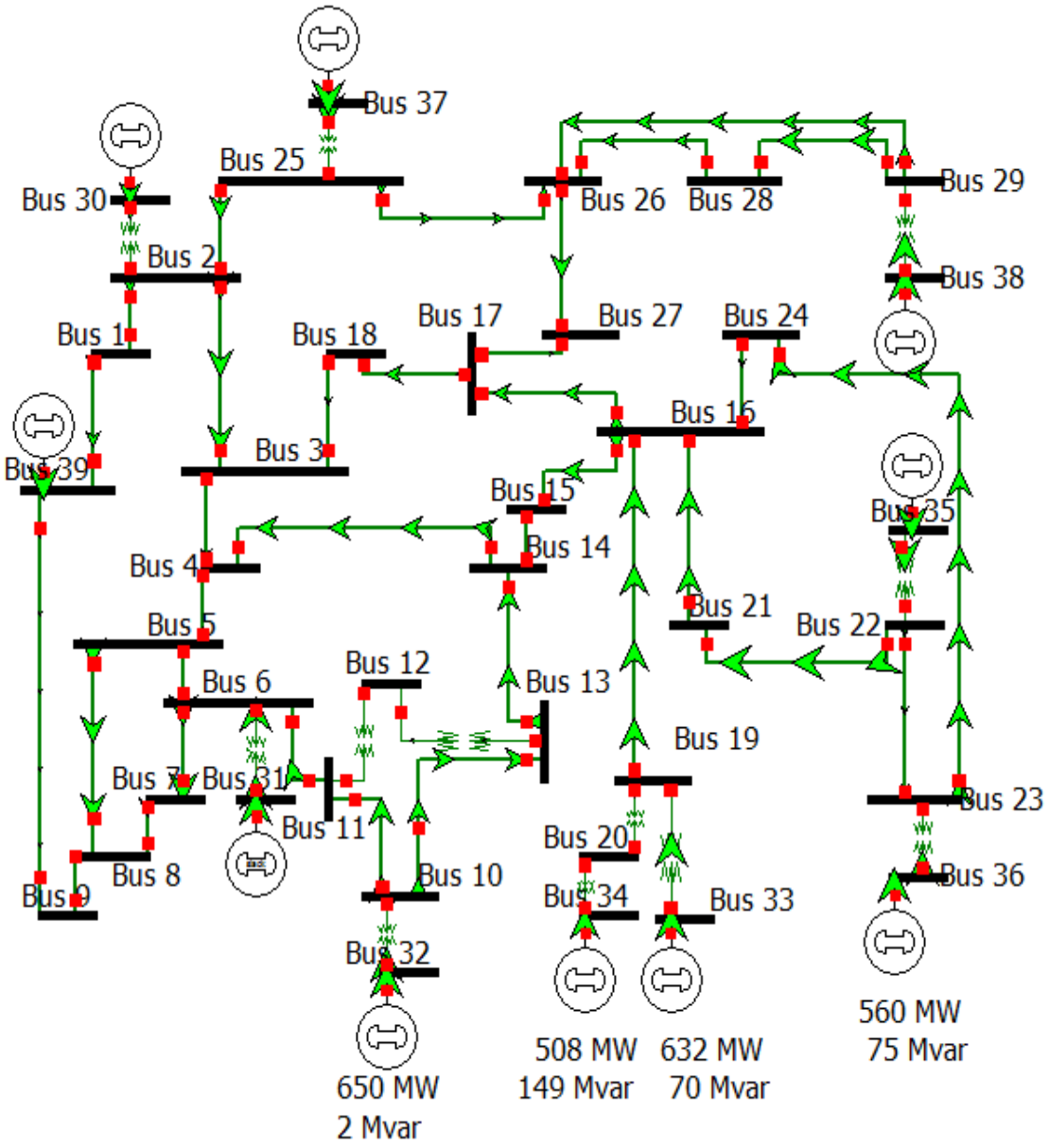

Figure 5.5 IEEE 39-Bus System (Powerworld) [33]

BUS PARAMETERS

Table 5.7 Bus Data [33]

BUS	TYPE	Pd	Qd	Vm	θ
1	1 (PQ)	97.6	44.2	1.039384	-13.536602
2	1 (PQ)	0	0	1.048494	-9.7852666
3	1 (PQ)	322	2.4	1.030708	-12.276384
4	1 (PQ)	500	184	1.00446	-12.626734
5	1 (PQ)	0	0	1.006006	-11.192339
6	1 (PQ)	0	0	1.008226	-10.40833
7	1 (PQ)	233.8	84	0.998397	-12.755626
8	1 (PQ)	522	176.6	0.997872	-13.335844
9	1 (PQ)	6.5	-66.6	1.038332	-14.175442
10	1 (PQ)	0	0	1.017843	-8.170875
11	1 (PQ)	0	0	1.013386	-8.9369663
12	1 (PQ)	8.53	88	1.000815	-8.9988236
13	1 (PQ)	0	0	1.014923	-8.9299272
14	1 (PQ)	0	0	1.012319	-10.715295
15	1 (PQ)	320	153	1.016185	-11.345399
16	1 (PQ)	329	32.3	1.03252	-10.033348
17	1 (PQ)	0	0	1.034237	-11.116436
18	1 (PQ)	158	30	1.031573	-11.986168
19	1 (PQ)	0	0	1.050107	-5.4100729
20	1 (PQ)	680	103	0.991011	-6.8211783
21	1 (PQ)	274	115	1.032319	-7.6287461
22	1 (PQ)	0	0	1.050143	-3.3812763
23	1 (PQ)	247.5	84.6	1.045145	-3.3812763
24	1 (PQ)	308.6	-92.2	1.038001	-9.9137585
25	1 (PQ)	224	47.2	1.057683	-8.83692354

26	1 (PQ)	139	17	1.052561	-9.4387696
27	1 (PQ)	281	75.5	1.038345	-11.362152
28	1 (PQ)	206	27.6	1.050374	-5.9283592
29	1 (PQ)	283.5	26.9	1.050115	-3.1698741
30	3 (SLACK)	0	0	1.0499	-7.3704746
31	2 (PV)	9.2	4.6	0.982	0
32	2 (PV)	0	0	0.9841	-0.1884374
33	2 (PV)	0	0	0.9972	-0.19317445
34	2 (PV)	0	0	1.0123	-1.631119
35	2 (PV)	0	0	1.0494	1.7765069
36	2 (PV)	0	0	1.0636	4.4684374
37	2 (PV)	0	0	1.0275	-1.5828988
38	2 (PV)	0	0	1.0265	3.8928177
39	2 (PV)	1104	250	1.03	-14.535256

Table 5. 8 Generator Data [33]

BUS	Pg	Qg	Qmax	Qmin	Vg	Pmax
30	255	161.762	400	140	1.0499	1040
31	677.871	221.574	300	-100	0.982	646
32	650	206.965	300	150	0.9841	725
33	632	108.293	250	0	0.9972	652
34	508	166.688	167	0	1.0123	508
35	650	210.661	300	-100	1.0494	687
36	560	100.165	240	0	1.0636	580
37	540	-1.36945		250	1.0275	564
38	830	21.7327	300	-150	1.0265	865
39	1000	78.4674	300	-100	1.03	1100

Table 5.9 Branch Data [33]

Branch no	From Bus	To Bus	r	x	b
1	1	2	0.035	0.0411	0.6987
2	1	39	0.001	0.025	0.75
3	2	3	0.0013	0.0151	0.2572
4	2	25	0.007	0.0086	0.146
5	2	30	0	0.0181	0
6	3	4	0.0013	0.0213	0.2214
7	3	18	0.0011	0.0133	0.2138
8	4	5	0.0008	0.0128	0.1342
9	4	14	0.0008	0.0129	0.1382
10	5	6	0.0002	0.0026	0.0434
11	5	8	0.0008	0.0112	0.1476
12	6	7	0.0006	0.0092	0.113
13	6	11	0.0007	0.0082	0.1389
14	6	31	0	0.025	0
15	7	8	0.0004	0.0046	0.078
16	8	9	0.0023	0.0363	0.3804
17	9	39	0.001	0.025	1.2
18	10	11	0.004	0.0043	0.0729
19	10	13	0.004	0.0043	0.0729
20	10	32	0	0.02	0
21	12	11	0.0016	0.0435	0
22	12	13	0.0016	0.0435	0
23	13	14	0.0009	0.0101	0.1723
24	14	15	0.0018	0.0217	0.366

25	15	16	0.0009	0.0094	0.171
26	16	17	0.0007	0.0089	0.1342
27	16	19	0.0016	0.0195	0.304
28	16	21	0.0008	0.0135	0.2548
29	16	24	0.0003	0.0059	0.068
30	17	18	0.0007	0.0082	0.1319
31	17	27	0.0013	0.0173	0.3216
32	19	20	0.0007	0.0138	0
33	19	33	0.0007	0.0142	0
34	20	34	0.0009	0.018	0
35	21	22	0.0008	0.014	0.2565
36	22	23	0.0006	0.0096	0.1846
37	22	25	0	0.0143	0
38	23	24	0.0022	0.035	0.361
39	23	36	0.0005	0.0272	0
40	25	26	0.0032	0.0323	0.531
41	25	37	0.0006	0.0232	0
42	26	27	0.0014	0.0147	0.2396
43	26	28	0.0043	0.0474	0.7802
44	26	29	0.0057	0.0625	1.029
45	28	29	0.0014	0.0151	0.249
46	29	38	0.0008	0.0156	0

5.5 Modified 39-Bus Test System

Figure 5.6 shows an equivalent Australian network. Appendix A shows the way a 39-Bus network is modified to an Australian equivalent network having a variety of generating sources.

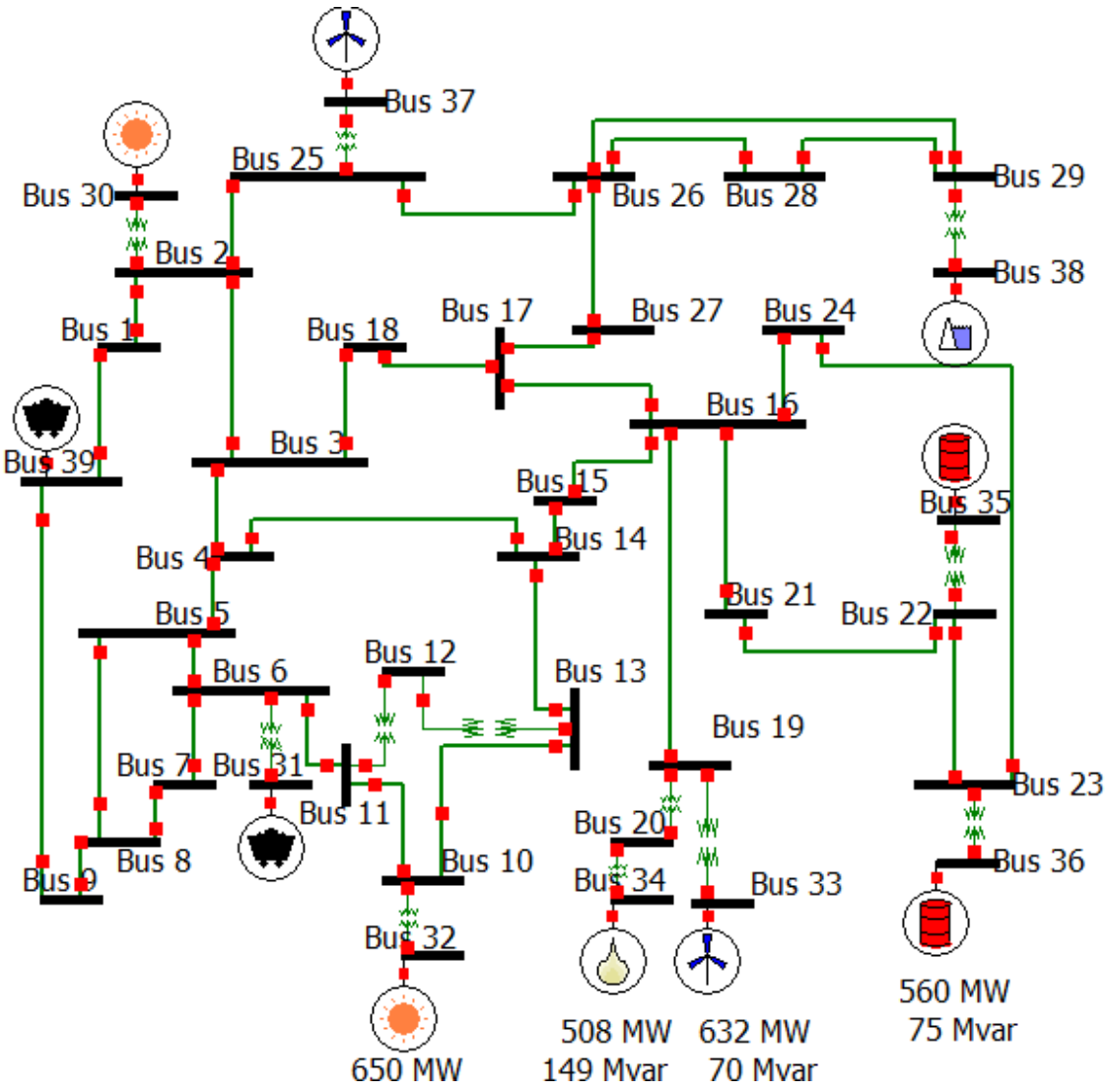

Figure 5. 6 IEEE 39-Bus Modified System (Power world)

BUS PARAMETERS

Table 5.10 Bus Data

Bus	Type	Pd	Qd	V(pu)	□
1	1 (PQ)	0	0	1.05178	-8.57
2	1 (PQ)	0	0	1.05988	-6.13
3	1 (PQ)	322	2.4	1.05655	-8.95
4	1 (PQ)	500	184	1.05919	-9.78
5	1 (PQ)	0	0	1.07359	-8.77
6	1 (PQ)	0	0	1.07428	-8.14
7	1 (PQ)	233.8	84	1.06115	-10.08
8	1 (PQ)	522	176	1.05858	-10.52
9	1 (PQ)	0	0	1.05402	-10.28
10	1 (PQ)	0	0	1.06106	-5.87
11	1 (PQ)	0	0	1.06429	-6.66
12	1 (PQ)	7.5	88	1.04934	-6.64
13	1 (PQ)	0	0	1.0587	-6.52
14	1 (PQ)	0	0	1.05614	-8.03
15	1 (PQ)	320	153	1.04089	-8.31
16	1 (PQ)	329.4	32.3	1.04853	-6.91
17	1 (PQ)	0	0	1.05175	-7.87
18	1 (PQ)	158	30	1.05233	-8.69
19	1 (PQ)	0	0	1.05599	-2.33
20	1 (PQ)	680	103	0.99422	-3.72
21	1 (PQ)	274	115	1.04355	-4.55
22	1 (PQ)	0	0	1.05611	-0.16
23	1 (PQ)	247.5	84.6	1.05132	-0.35

24	1 (PQ)	308.6	-92.2	1.05258	-6.79
25	1 (PQ)	224	47.2	1.06582	-4.69
26	1 (PQ)	139	17	1.06229	-5.97
27	1 (PQ)	281	75.5	1.05173	-7.97
28	1 (PQ)	206	27.6	1.05541	-2.49
29	1 (PQ)	283.5	26.9	1.05357	0.25
30	3 (SLACK)	0	0	1.0475	-3.73
31	2 (PV)	9.2	4.6	0.982	-1.59
32	2 (PV)	0	0	0.9831	1.79
33	2 (PV)	0	0	0.9972	2.87
34	2 (PV)	0	0	1.0123	1.46
35	2 (PV)	0	0	1.0493	4.78
36	2 (PV)	0	0	1.0635	7.46
37	2 (PV)	0	0	1.0278	2.05
38	2 (PV)	0	0	1.0265	7.3
39	2 (PV)	1104	250	1.03	-10.06

Table 5.11 Generator Data

Bus	Pg	Qg	Qmax	Qmin	Vg	Pmax
30	250	83.21	800	-500	1.0475	9999.9
31	571.29	363.94	800	-500	0.982	9999.9
32	650	1.53	800	-500	0.9831	9999.9
33	632	69.67	800	-500	0.9972	9999.9
34	508	148.79	800	-300	1.0123	9999.9
35	650	167.04	800	-500	1.0493	9999.9
36	560	75.45	800	-500	1.0635	9999.9
37	540	-35.35	800	-500	1.0278	9999.9
38	830	-0.47	800	-500	1.0265	9999.9
39	1000	-36.49	1500	-1000	1.03	9999.9

Table 5. 12 Branch Data [33]

Branch no	From Bus	To Bus	r	x	b
1	10	11	0.0004	0.0043	0.0729
2	22	23	0.0006	0.0096	0.1846
3	26	29	0.0057	0.0625	1.029
4	23	24	0.0022	0.035	0.361
5	3	4	0.0013	0.0213	0.2214
6	2	3	0.0013	0.0151	0.2572
7	1	2	0.0035	0.0411	0.6987
8	28	29	0.0014	0.0151	0.249
9	5	6	0.0002	0.0026	0.0434
10	10	13	0.0004	0.0043	0.0729
11	6	7	0.0006	0.0092	0.113
12	6	11	0.0007	0.0082	0.1389
13	3	18	0.0011	0.0133	0.2138
14	7	8	0.0004	0.0046	0.078
15	2	25	0.007	0.0086	0.146
16	1	39	0.001	0.025	0.75
17	4	14	0.0008	0.0129	0.1382
18	13	14	0.0009	0.0101	0.1723
19	26	28	0.0043	0.0474	0.7802
20	26	27	0.0014	0.0147	0.2396
21	5	8	0.0008	0.0112	0.1476
22	25	26	0.0032	0.0323	0.513
23	14	15	0.0018	0.0217	0.366
24	15	16	0.0009	0.0094	0.171

25	16	17	0.0007	0.0089	0.1342
26	16	19	0.0016	0.0195	0.304
27	16	21	0.0008	0.0135	0.2548
28	16	24	0.0003	0.0059	0.068
29	17	18	0.0007	0.0082	0.1319
30	17	27	0.0013	0.0173	0.3216
31	8	9	0.0023	0.0363	0.3804
32	4	5	0.0008	0.0128	0.1342
33	9	39	0.001	0.025	1.2
34	21	22	0.0008	0.014	0.2565
35	31	6	0	0.025	0
36	29	38	0.0008	0.0156	0
37	12	13	0.0016	0.0435	0
38	12	11	0.0016	0.0435	0
39	25	37	0.0006	0.0232	0
40	10	32	0	0.02	0
41	2	30	0	0.0181	0
42	23	36	0.0005	0.0272	0
43	22	35	0	0.0143	0
44	20	34	0.0009	0.018	0
45	19	33	0.0007	0.0142	0
46	19	20	0.0007	0.0138	0

5.6 Security Breach Scenario in Smart Grid

A hypothetical case of a security breach is considered. Let's suppose there is a requirement of extra power at bus-13 from 13.5 to 18 MW. A message is sent from bus-13 to SCADA system for a request of extra power but some hackers took that information and tempered it to different value from 18 MW to 70 MW. Due to this change in information, the generator will supply more power as required which will result in exceeding the branch flow ratings as shown in Figure 5.7. It is seen that a false message violates the total power flow limits condition across different branches (i.e. Bus 1-2, 1-5 and 6-13).

Such incidents clearly show that there is a need for SG security to make the system less vulnerable and there will be a need of security check to predict correct line flows before and after the load change. Figure 5.8 shows power flow before and after load change.

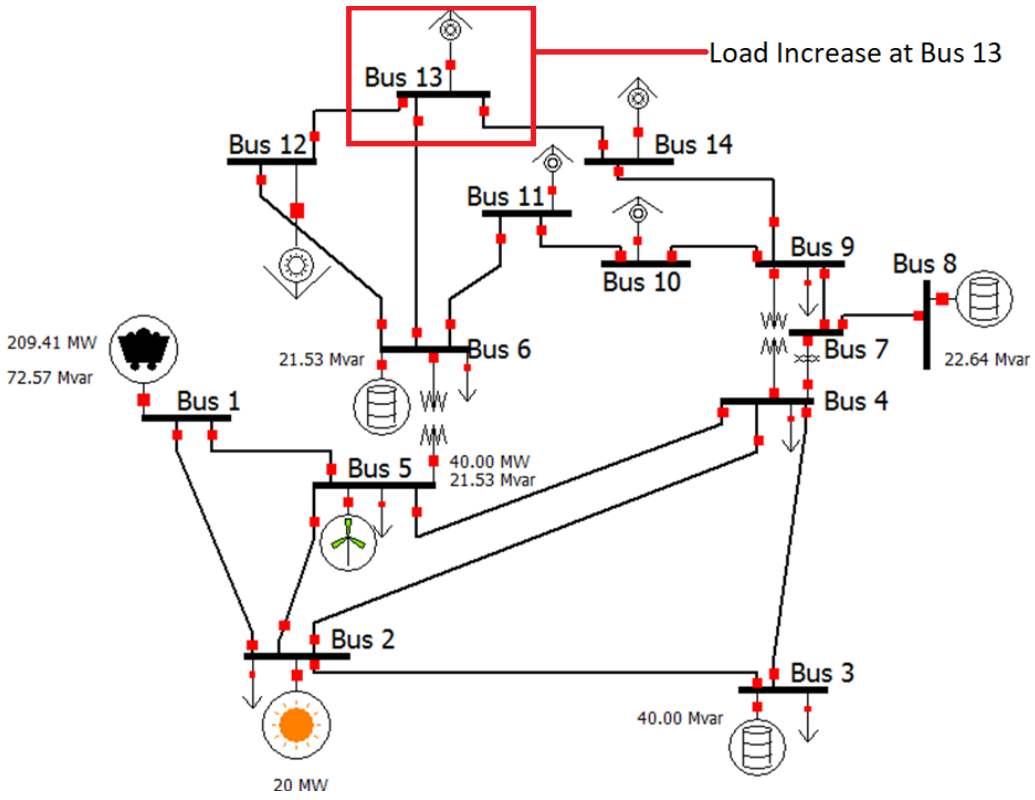

Figure 5.7 14-Bus Modified System

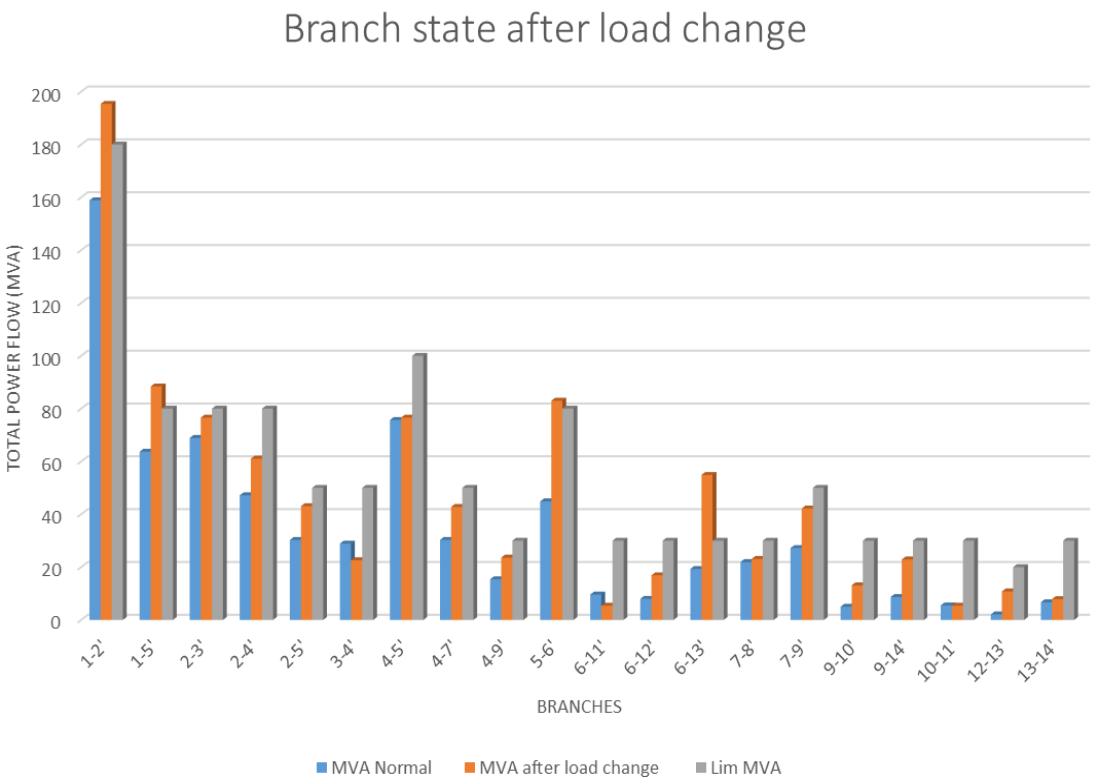

Figure 5.8 Power Flow Before and After the Load Change

5.7 Test Cases Using Different Algorithms

In this section modified 14-bus and 39-bus cases are used to test different algorithm. For the sake of comparison, two algorithms are selected including line outage detection using phasor angle measurement approach and Monitoring for Power-line Change and Outage Detection in SG via the Alternating Direction Method of Multipliers. These two algorithms are applied to see the accuracy in finding out the correct outage line.

From table 5.6 and 5.9, the line to bus admittance matrix can be formed which is used for designing the measurement matrix. PMUs are placed at different buses to get data before and after the fault. The system is assumed to be in the steady state before and after the outage and a fault is injected across different buses using power world transient stability feature.

5.7.1 Phasor Angle Measurement Algorithm

STEPS FOR APPLYING ALGORITHM:

1. For every line

Find $\Delta\tilde{\theta}_{calc}$

$$\Delta\tilde{\theta}_{calc}{}^{Pi} = KB^{-1}\begin{bmatrix}0\\ \widetilde{P}_i\\ \widetilde{-P}_i\\ 0\end{bmatrix} = \widetilde{P}_i KB^{-1}\begin{bmatrix}0\\ 1\\ -1\\ 0\end{bmatrix} = \widetilde{P}_i\Delta\tilde{\theta}_{calc} \tag{5.1}$$

Find $\widetilde{P}_l^{*}$ as given:

$$\widetilde{P}_1^{*} = \frac{\Delta\theta_{Observeed}.\Delta\widetilde{\theta}_{Calc}}{\Delta\widetilde{\theta}_{Calc}.\Delta\widetilde{\theta}_{Calc}} \tag{5.2}$$

NAD value will be calculated using below equation

$$\theta_i = \frac{\cos^{-1}\left|\left(\frac{(\Delta\theta_{Observed})}{\Delta\theta_{Observed}.\Delta\theta_{Observed}}\right).\left(\frac{\Delta\tilde{\theta}_{Calc}}{\Delta\tilde{\theta}_{Calc}.\Delta\tilde{\theta}_{Calc}}\right)\right|}{2} \tag{5.3}$$

$$NAD_i = 2\sin\theta_1 \tag{5.4}$$

Now store the above error value in the indexed array NADVals

$$NADVals_i = NAD_i \tag{5.5}$$

2. Determine the outaged line l^{*} by sorting NADVals

$$l^{*} = \text{argmin } NADVals_i$$

3. Find out pre outage flow on the line using Pi* which best fits the angle observed.

$$\widetilde{P_l} = \frac{P_i}{1-PTDF_{l,l_{from}-l_{to}}} \tag{5.6}$$

$$\mathrm{P_{l^*}}^* = \widetilde{\mathrm{P}}_{\mathrm{l}^*}{}^* \left(1 - \mathrm{PTDF}_{\mathrm{l}^*,\mathrm{l}^*_{\mathrm{from}}-\mathrm{l}^*_{\mathrm{to}}}\right) \tag{5.7}$$

5.7.2 Alternating Direction Method for Multipliers Algorithm

This algorithm is called distributed line change detection (D-LCD)

1. Input parameters:

$$Y_n , H_n , Y_n, \Lambda_n , \Lambda_{pn} , X_{pn} , D_n , \lambda > 0, \rho > 0, \mathrm{k} = 0$$

2. Initialize

$$X_n , \delta_{nm} , Z_n , V_{nm} , S_n$$

3. While stopping criterion not reached do

$$k \to k + 1$$

4. Update X_n^{k+1}

based on

$$x_n{}^{k+1} = (H_n{}^T H_n + \rho D_n + \rho I_n)^{-1} x (H_n{}^T y_n + \rho(D_n r_n{}^k + \mathrm{x}_{pn} + z_n{}^k - (1/\rho)s_n{}^k$$

5. Exchange X_{nm}^{k+1} with its neighbours.

6. Update

δ_{nm}^{k+1} , Z_n^{k+1}

via below equations respectively

$$\delta_{nm}^{k+1} = , \frac{(\mathrm{x}_{nm}^{k+1} + \mathrm{x}_{mn}^{k+1})}{2} \tag{5.8}$$

$$Z_n^{k+1} = S_{(\frac{\lambda}{p})^{pn(-1/2)}} \left(X_n^{k+1} - X_{pn} + \left(\frac{1}{\rho}\right) S_n^k \right) \quad (5.9)$$

7. Update V_{nm}^{k+1} , S_n^{k+1} using below equations

$$v_{nm}^{k+1} = v_{nm}^k + \rho(x_{nm}^{k+1} - \vartheta_{nm}^{k+1}) \; for \; all \; n, m. \quad (5.10)$$

$$s_n^{k+1} = s_n^k + \rho(x_n^{k+1} - x_{pn} - z_n^{k+1}) \quad (5.11)$$

8. End while

5.7.3 14-Bus Network:

Consider a 14-bus network and apply a line outage at two different branches.

a) Simulated Outage at Branch 2-3

A fault is applied at branch 2-3 and the fault occurs 0.5s after the start of the simulation. There is an outage between the transmission line of bus 2 and 3 as shown in Figure 5.9. Once the fault is applied, power flow will be different at all buses and PMUs are installed at different buses to keep a record of these changes in the network.

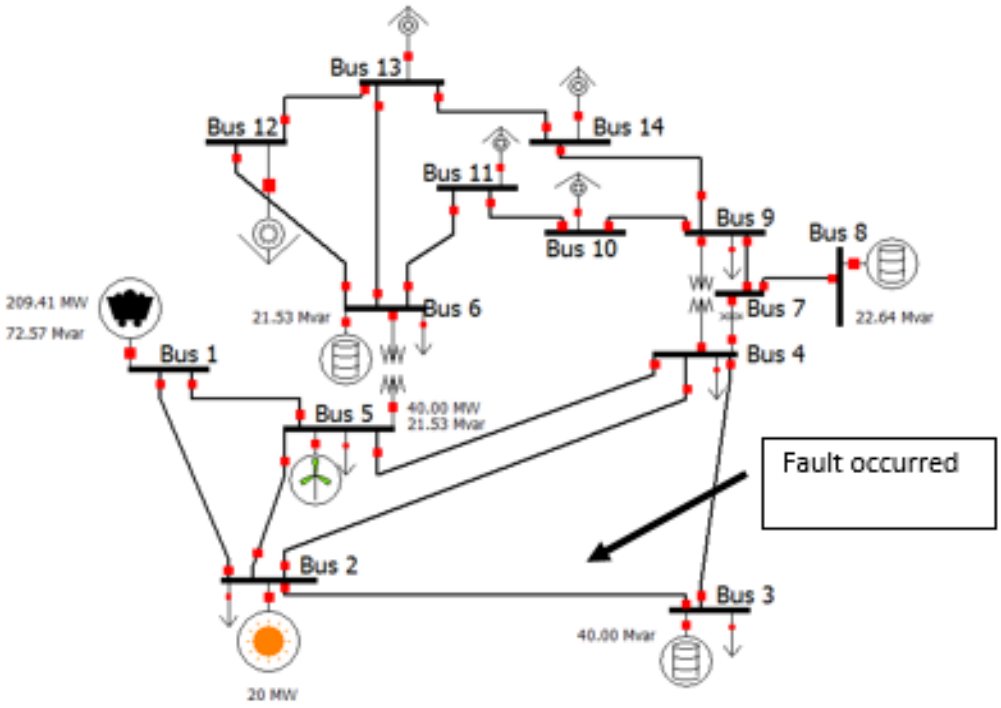

Figure 5.9 Fault Location At 14-Bus Network

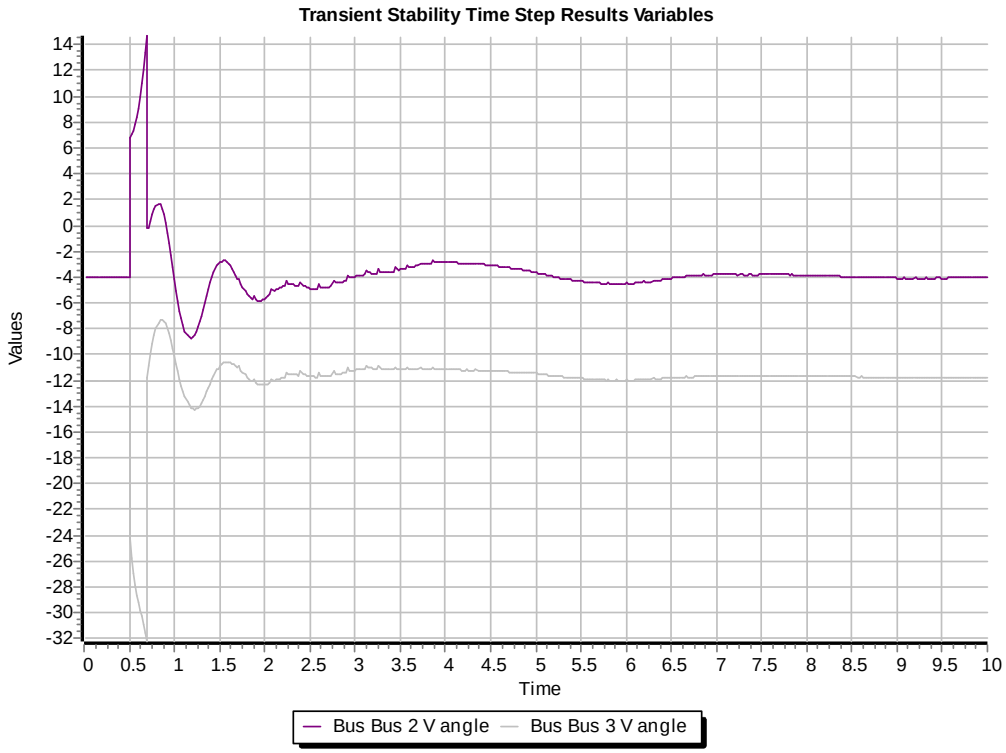

Figure 5.10 Voltage angles at bus 2 and 3 after the fault

It can be seen in Figure 5.10 that when the fault occured, the instability took place at bus 2 and 3 which causeed continues change in angles and settled down after certain intervals.

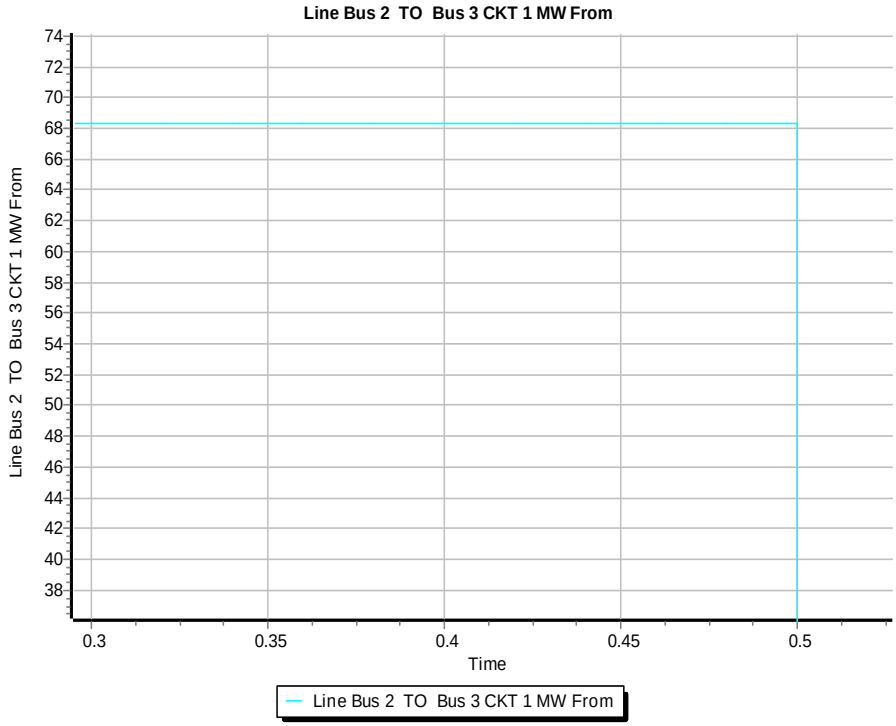

Figure 5.11 Pre-Outage Flow (Bus 2 – Bus 3).

Figure 5.11 shows the pre-outage flow between bus 2 and 3 and these values are to be found out using the selected algorithms. Since fault occurred at 0.5s, the selected transmission lines are disconnected from the system. At the same time when line outage occurred other lines got overloaded because the power taken from the faulty line is transmitted through the other lines.

Moreover, an outage at line 2 to 3 created an instability throughout the system as shown in Figure 5.12. Power flow between bus 3 and 4 also got disturbed after the fault and the line outage is shown in Figure 5.13. It is interesting to see the way the other branches react after the fault. Since fault took place at branch 2-3, it is disconnected but due to this line, other two lines are also removed from the system.

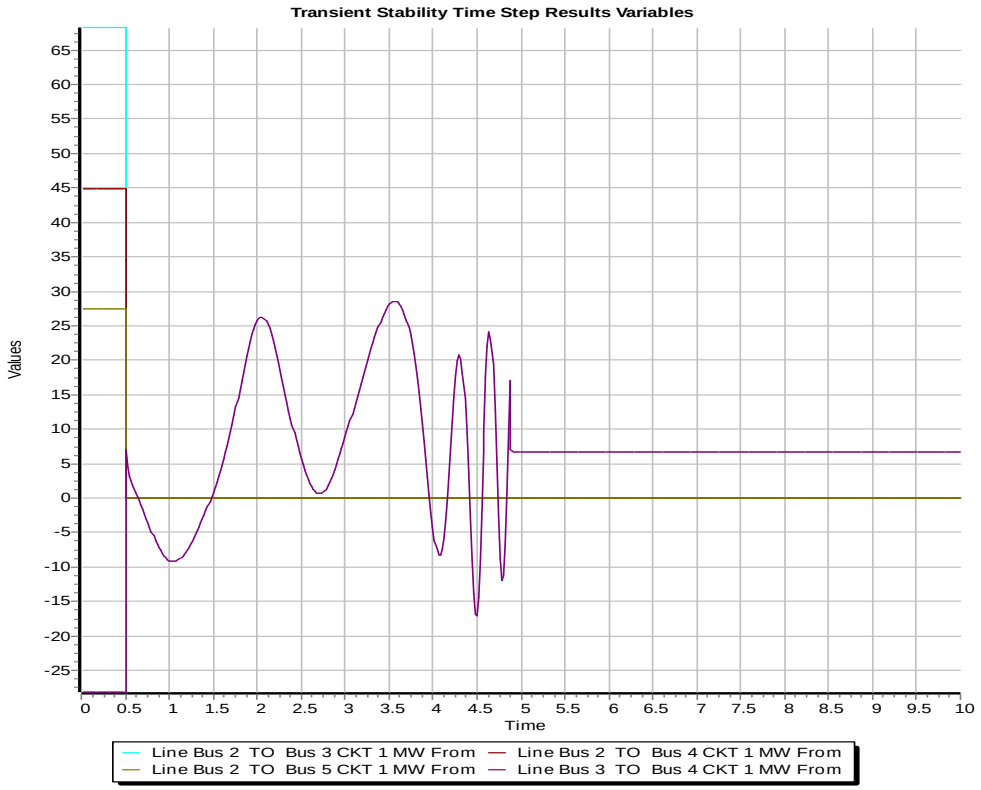

Figure 5.12 Power Flow Between Bus 2 – 3 And Adjacent Buses.

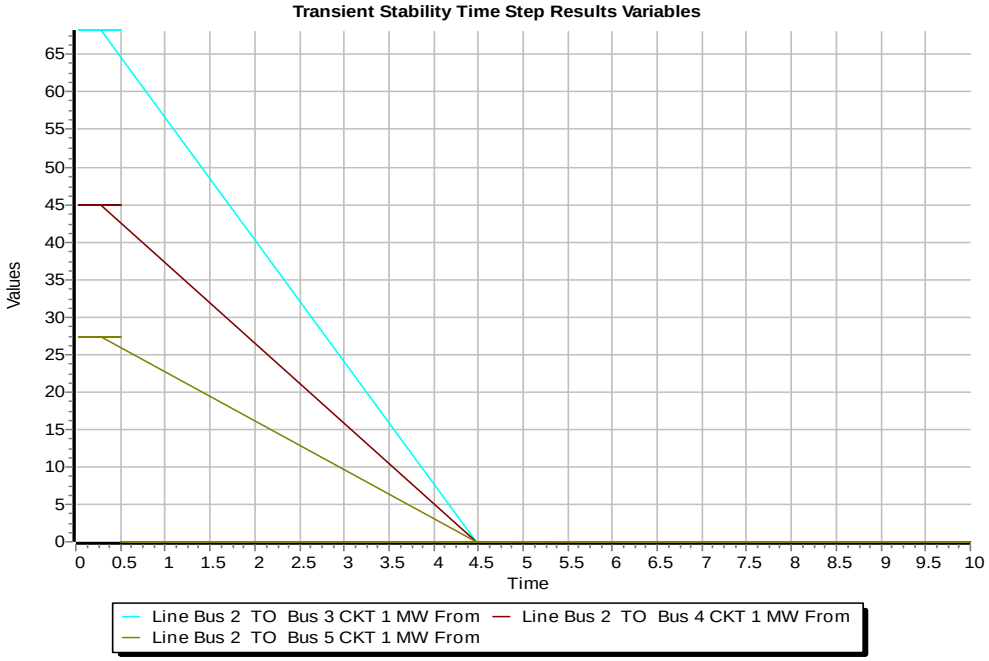

Figure 5.13 Outage Occurred at Other Branches

b) SIMULATED OUTAGE AT BRANCH 1-2

As test a fault is applied at branch 2-3(see Figure 5.14), fault is occurred after 0.5 seconds after the simulation started. There will be an outage between the transmission line of bus 2 and 3. Once the fault is applied power flow will be different at all buses, PMUs are installed to keep a record of these changes in the network.

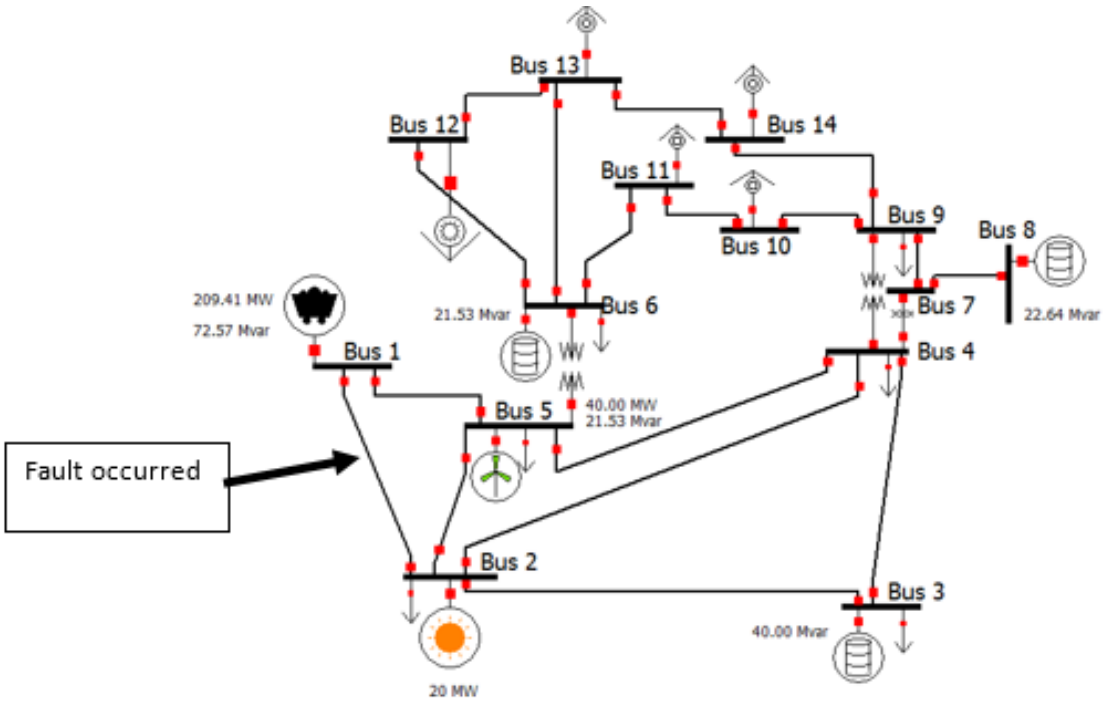

Figure 5.14 Fault State Between Bus 1 and 2

As fault occurred between bus 1-2, a huge oscillation can be seen in Figure 5.15. This is because the outage occurred at the slack bus (see Figure 5.16). Consequently, voltage angles remain unstable as long as there is a fault at line 1-2.

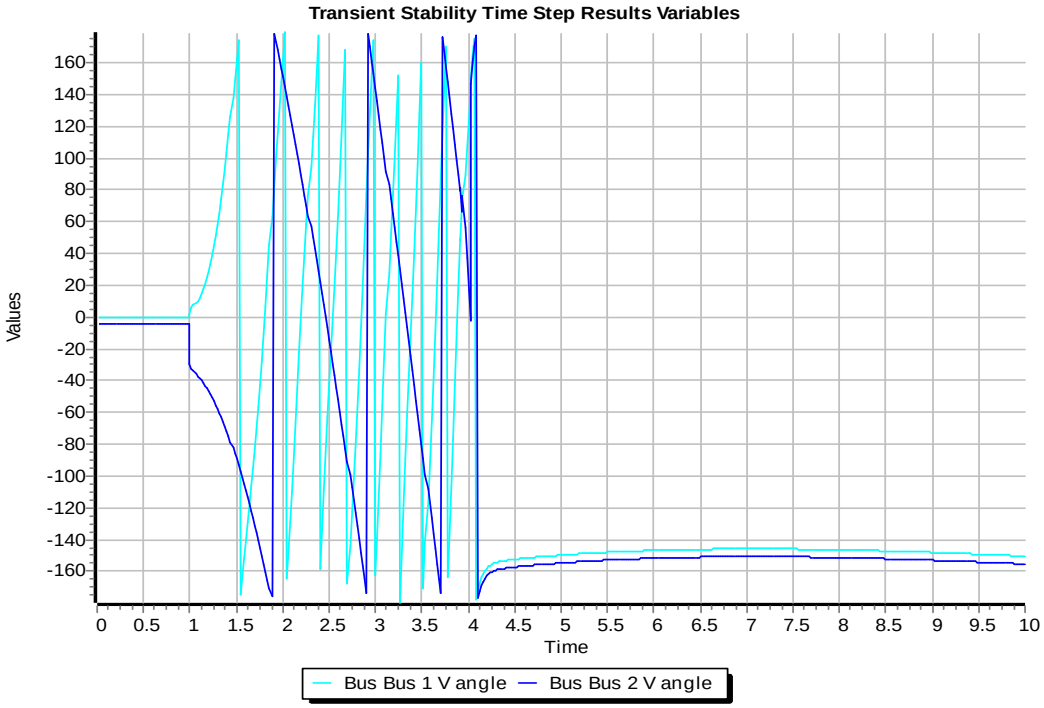

Figure 5.15 Voltage Angles at Bus 1 and 2 After the Fault

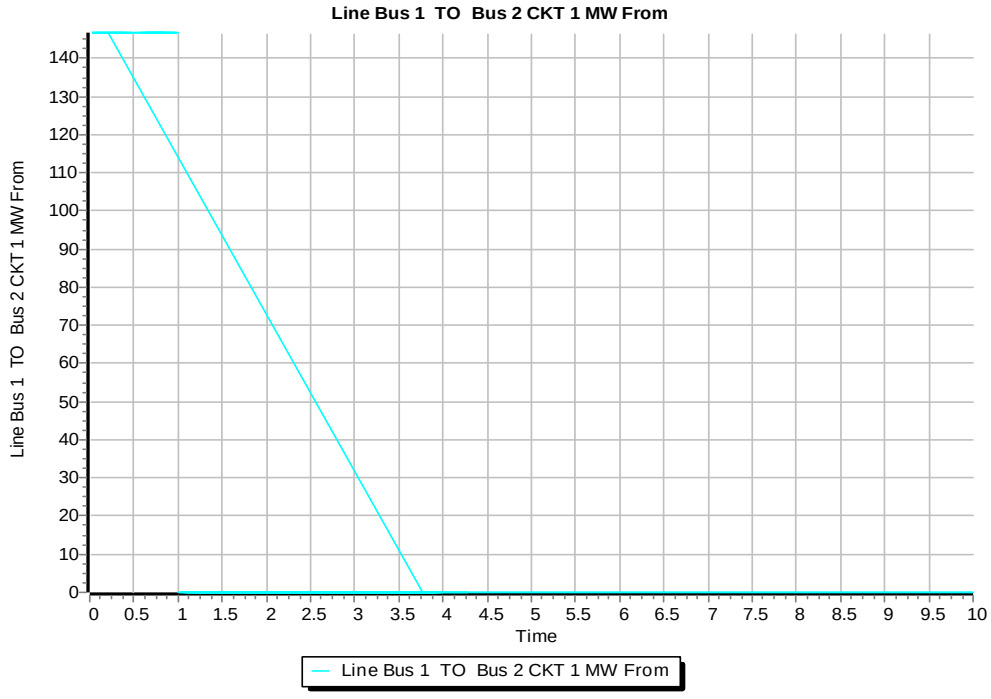

Figure 5.16 Outage at bus1-2.

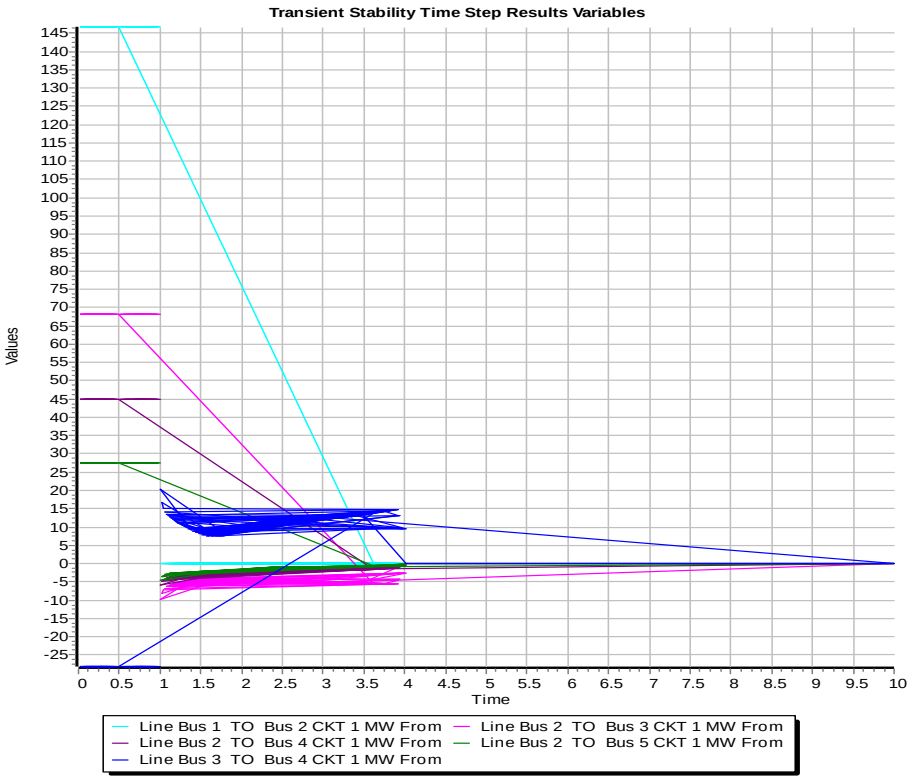

Figure 5.17 Affected Lines Due to Fault Between Bus 1 and 2

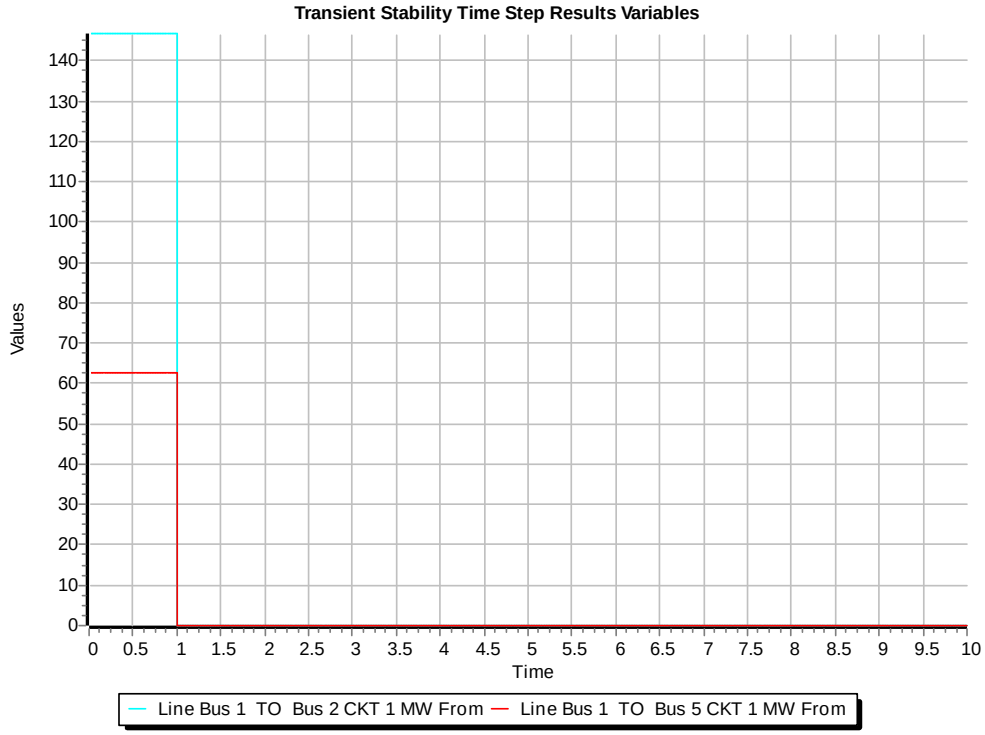

Figure 5.18 Outage occurred at other branches

Results from Phasor Angle Measurement Algorithm

An outage at Bus 2-3:

Table 5.13 Phasor angle measurement results for Outage at bus 2-3

	Bus 2 to 3 (MW)	Bus 2 to 4 (MW)	Bus 2 to 5 (MW)
Pre-Outage Flow (MW)	68.272	44.9459	27.4206
NAD	0.05	0.026	0.027

An outage at Bus 1-2:

Table 5.14 Phasor angle measurement results for Outage at bus 1-2

	Bus 1 to 2	Bus 1 to 5	Bus 2 to 5
Pre-Outage Flow (MW)	146.756	62.656	27.4206
NAD	0.03	0.021	0.025

Results from Alternating Direction Method for Multipliers Algorithm:

Outage at Bus 2-3

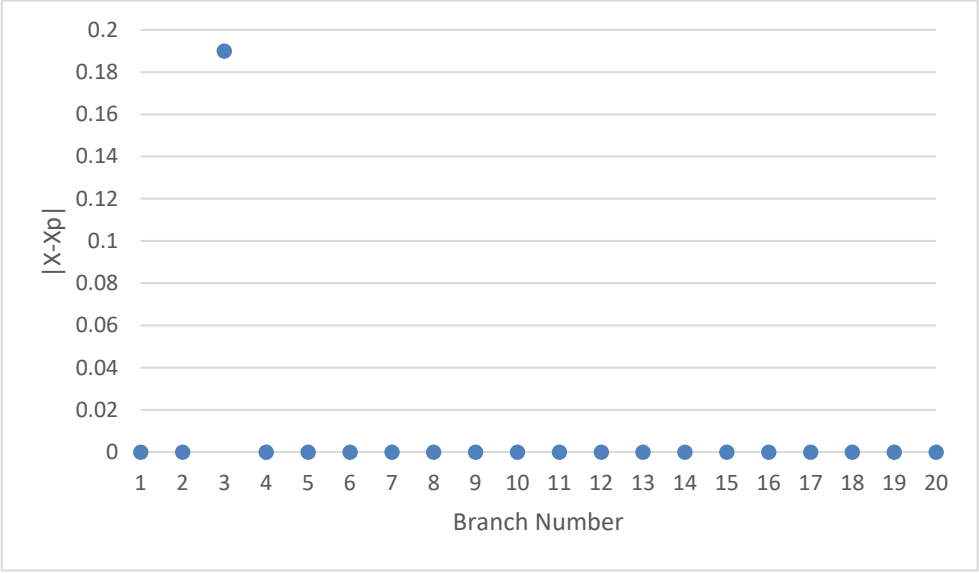

Figure 5.19 Alternating Direction Method for Multipliers Results for Outage at Bus 2-3

Outage at Bus 1-2

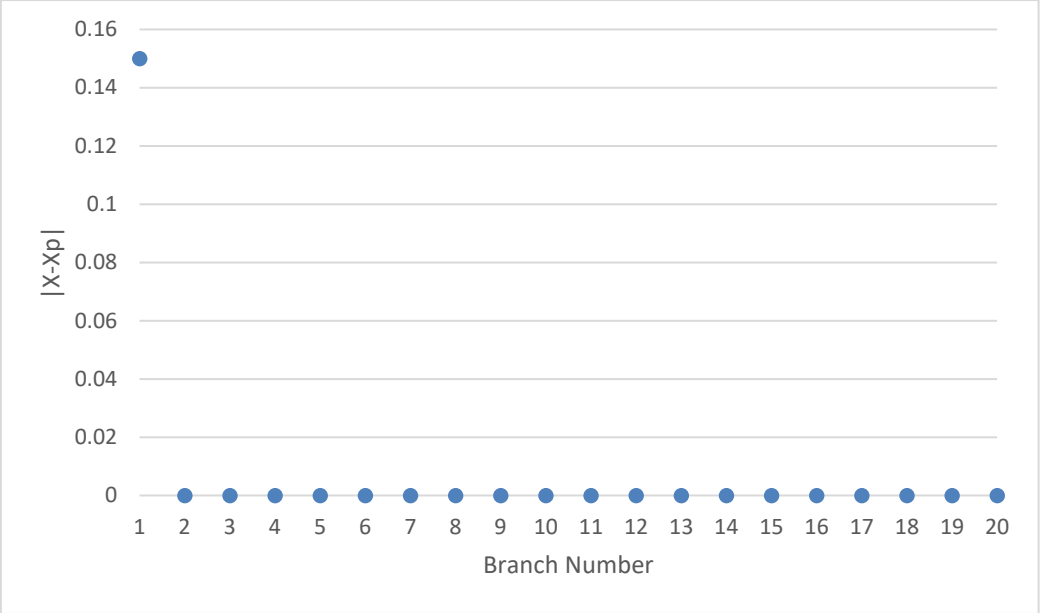

Figure 5.20 Alternating Direction Method for Multipliers Results for Outage at Bus1-2

In Table 5.13 and 5.14, the lower values of normalized angle distance (NAD) indicate the outage line in the system. The pre-outage values of the system are also shown, which are nearly equal to the values we have from power world simulations.

Figure 5.19 and 5.20 show the outage line when distributed line change detection algorithm is applied. This algorithm identifies the branch number having an outage. Figure 5.19 show a clear difference of |x-xp| showing that the branch 3 (bus 2-3) has an outage. Likewise Figure 5.20 identifies that the branch 1 (bus 1-2) is faulty.

5.7.4 39-Bus Network

Now consider 39-bus network. An outage is applied at two different branches.

a) Outage at Bus 23-24

Now fault occurs at branch 23-24 at 0.75 seconds (Figure 5.21), the outage takes place across these lines. Power flow at nearby buses is also affected after the occurrence of the fault thus resulting in a change in the voltage angles and amplitude at nearby buses. PMUs keep the record of all these changes which are installed on different buses.

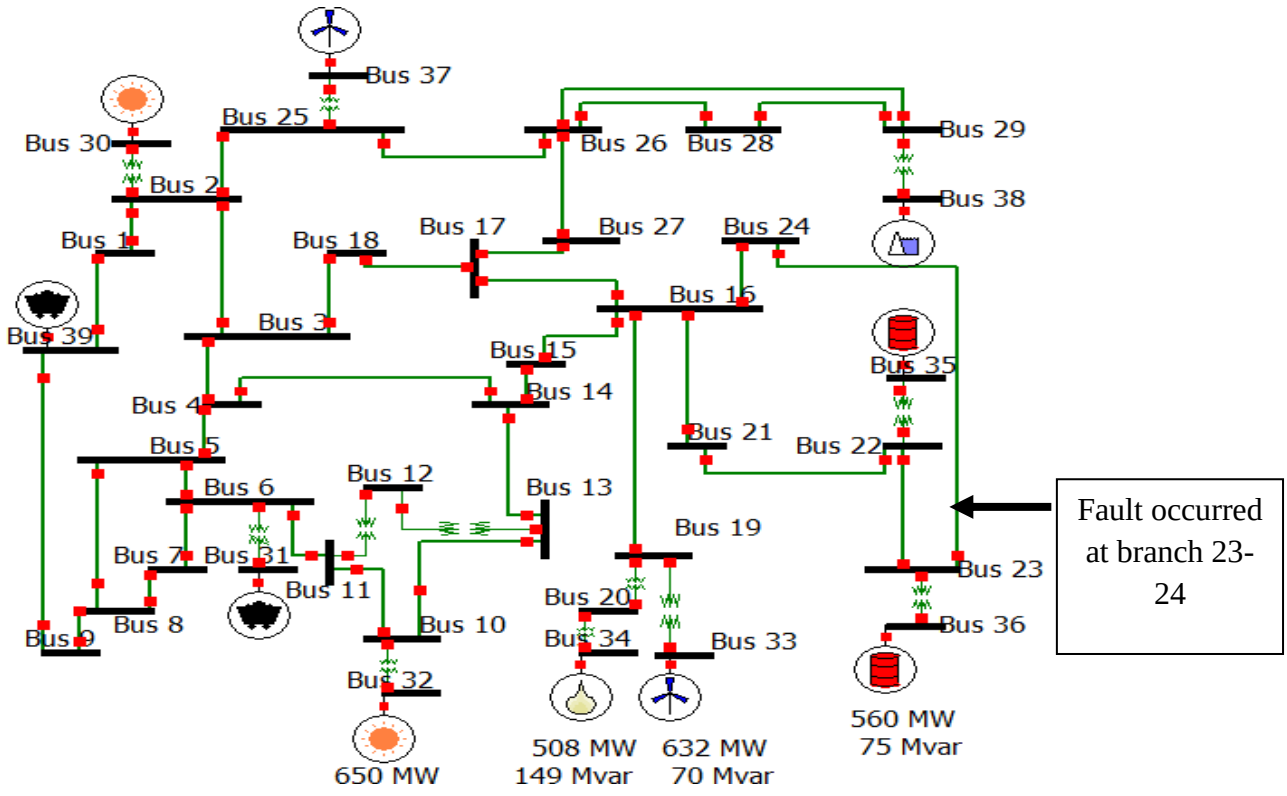

Figure 5.21 Fault State at Bus 23-24

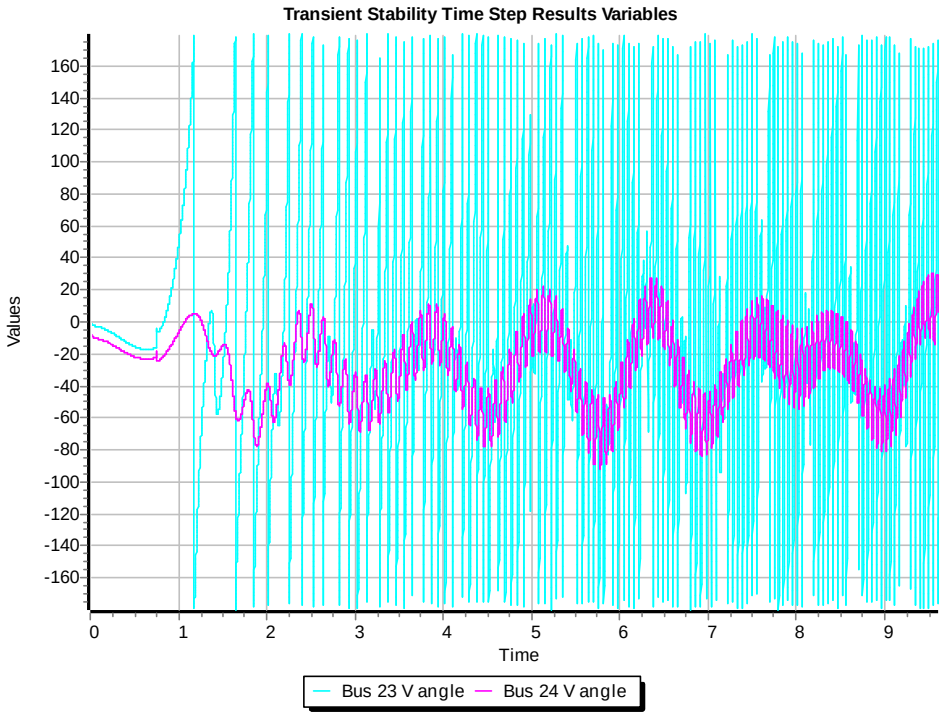

Figure 5.22 Voltage Angles at Bus 23 And 24 After the Fault.

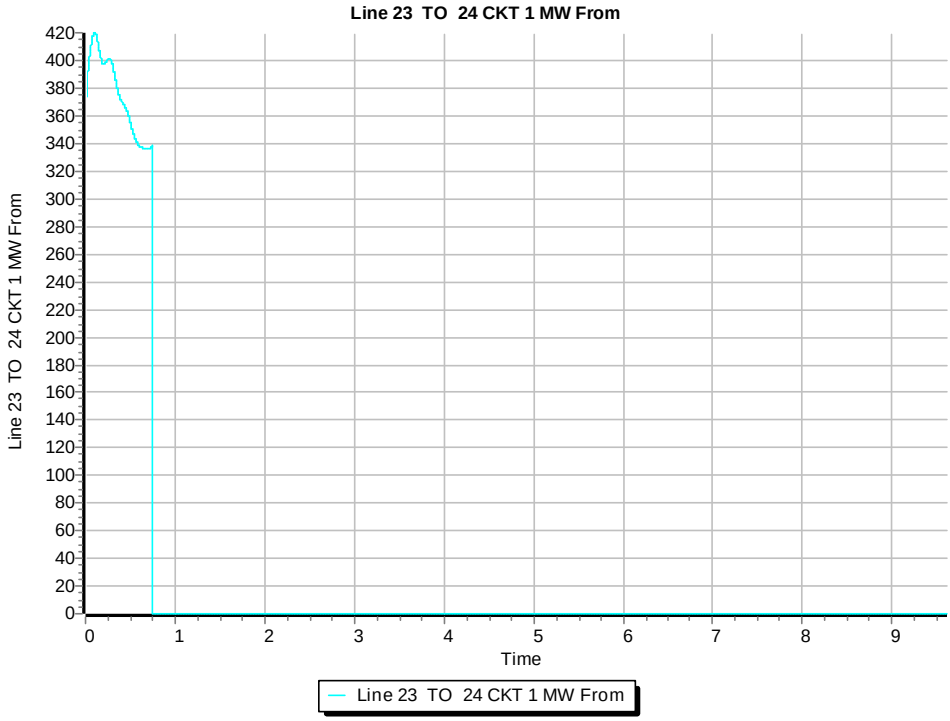

Figure 5.23 Outage at Bus 23-24.

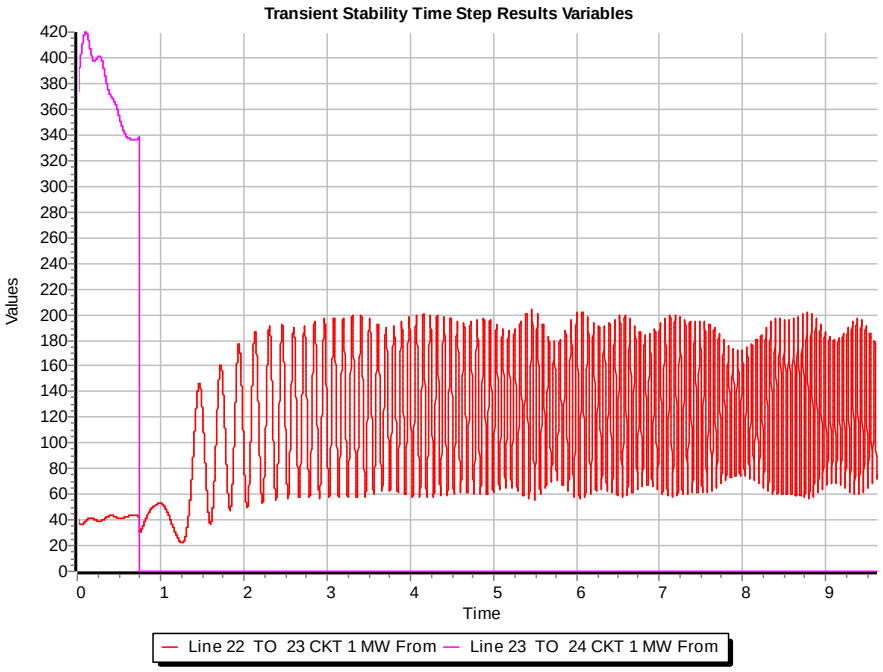

Figure 5.24 Affected Line Due to An Outage at Bus 23-24.

OUTAGE AT BUS 26-29:

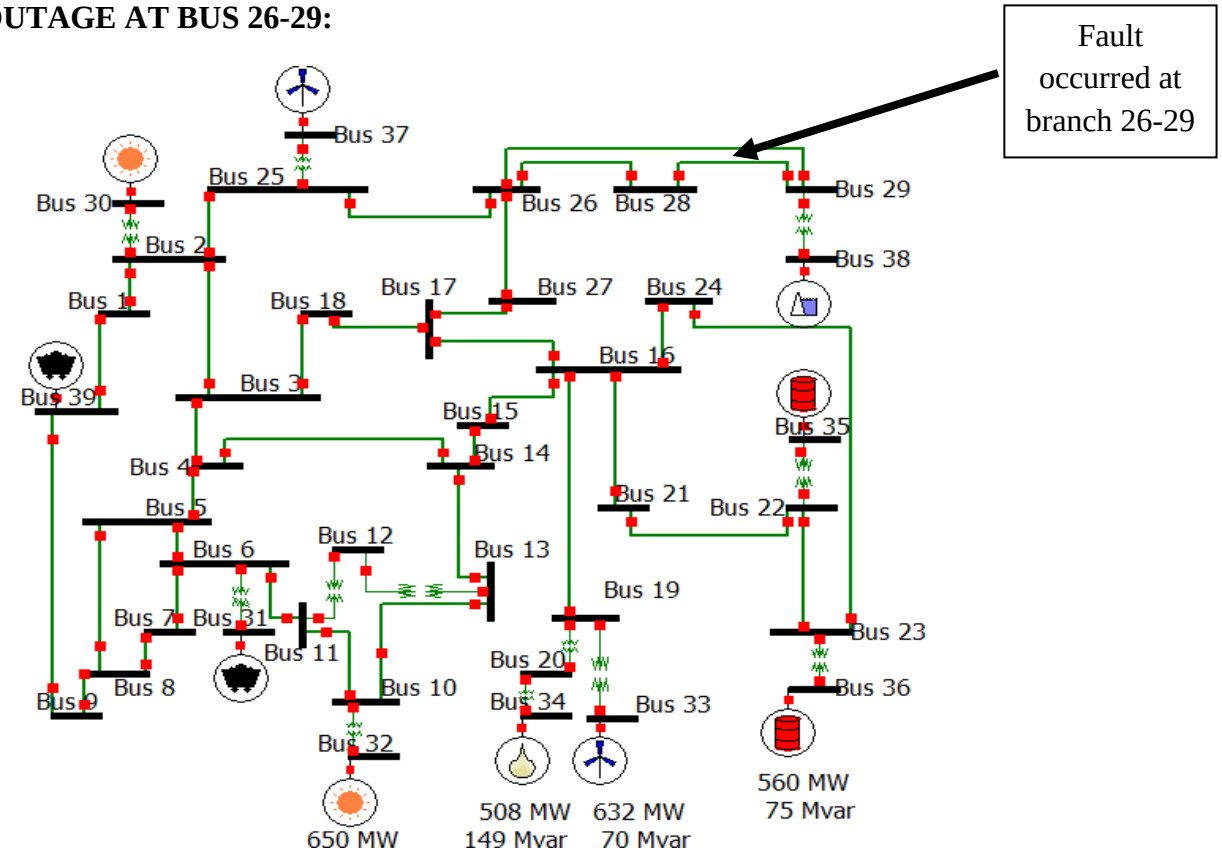

Figure 5.25 Fault State at Bus 23-24.

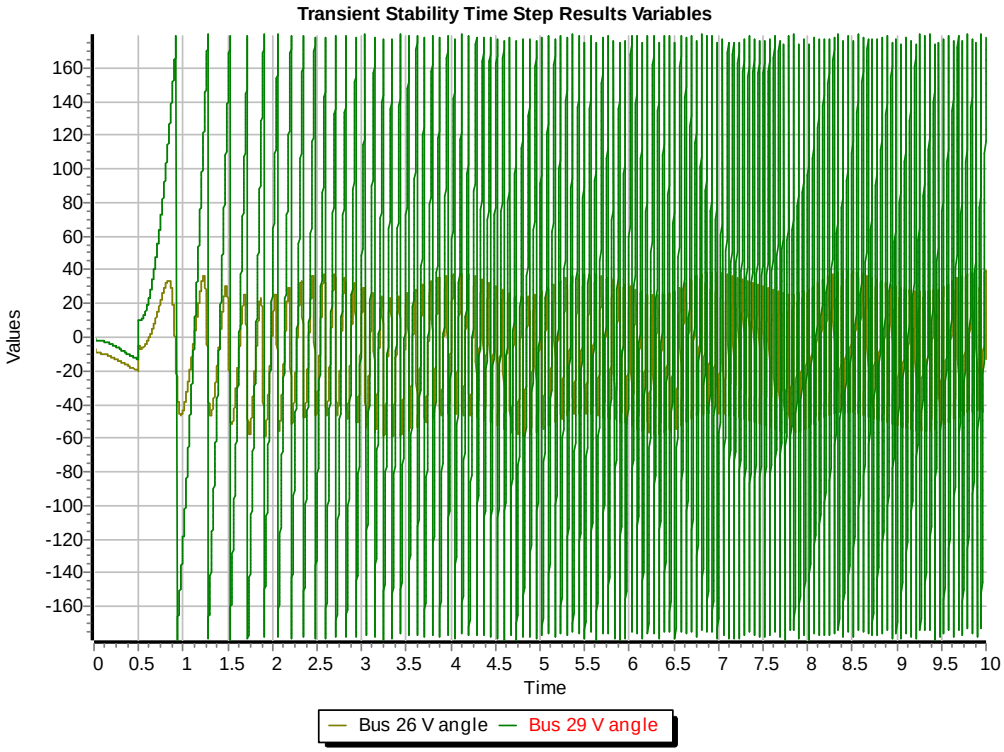

Figure 5.26 Voltage Angles at Bus 26 And 29 After the Fault

Figure 5.27 Outage at Bus 26-29.

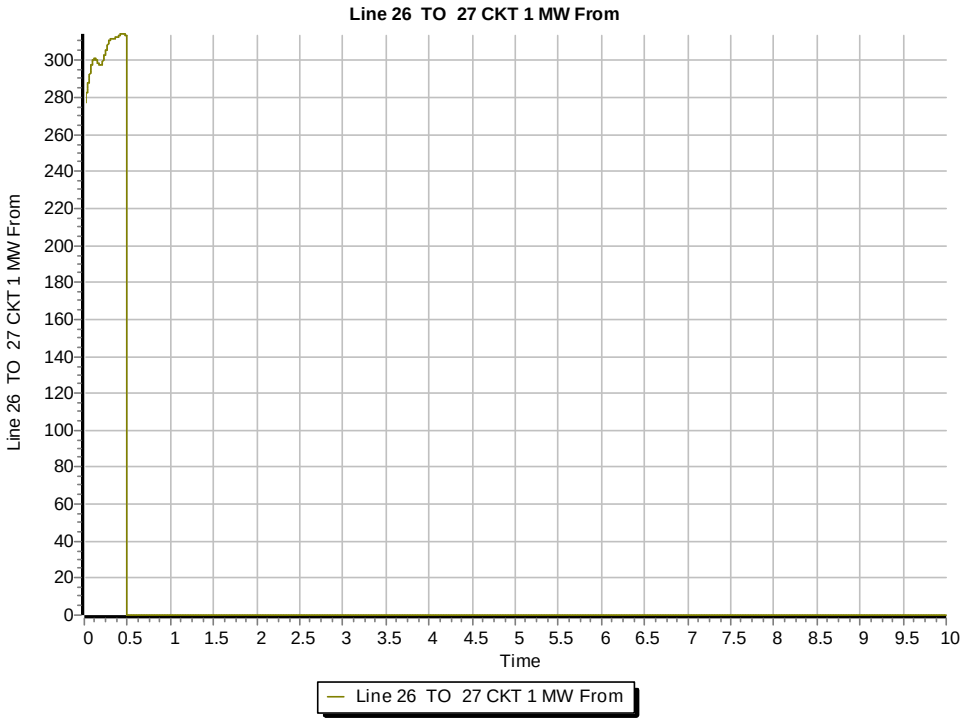

Figure 5.28 Affected Line Due to An Outage at Bus 26-29.

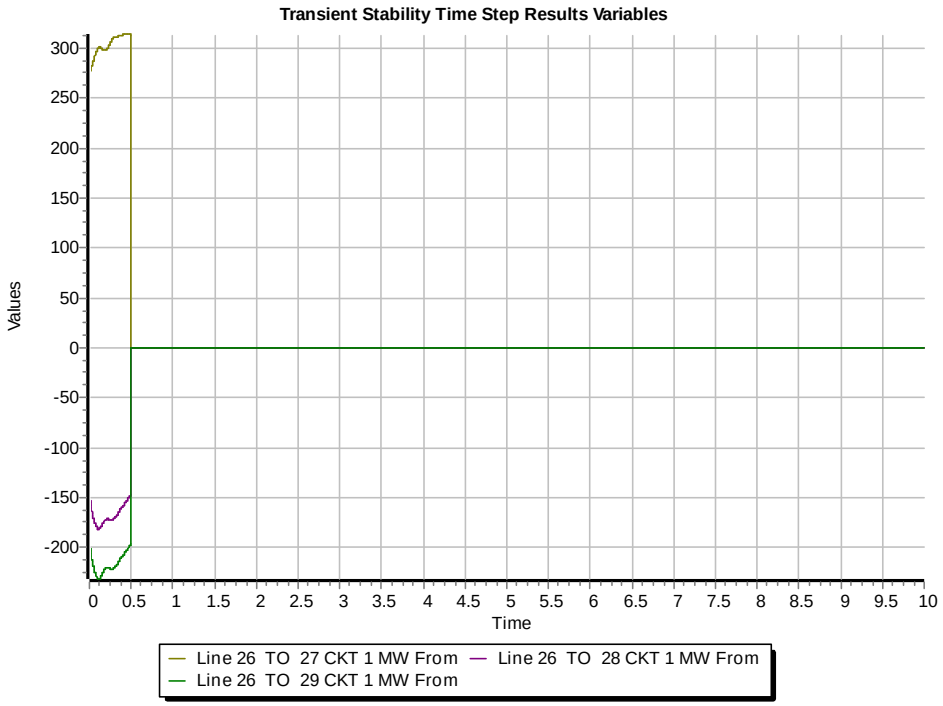

Figure 5.29 Other Affected Lines.

Phasor Angle Measurement Algorithm Results

An outage at bus 23-24

Table 5.15 Phasor Angle Measurement Results for Outage at Bus 23-24

	Bus 23 to 24 (MW)	Bus 22 to 23 (MW)
Pre-Outage Flow (MW)	339	40
NAD	0.09	0.026

An outage at bus 26-29:

Table 5.16 Phasor Angle Measurement Results for Outage at Bus 26-29

	Bus 29 to 26	Bus 26 to 27	Bus 28 to 26
Pre-Outage Flow (MW)	201	310	150
NAD	0.065	0.028	0.035

Alternating Direction Method for Multipliers Algorithm Results:

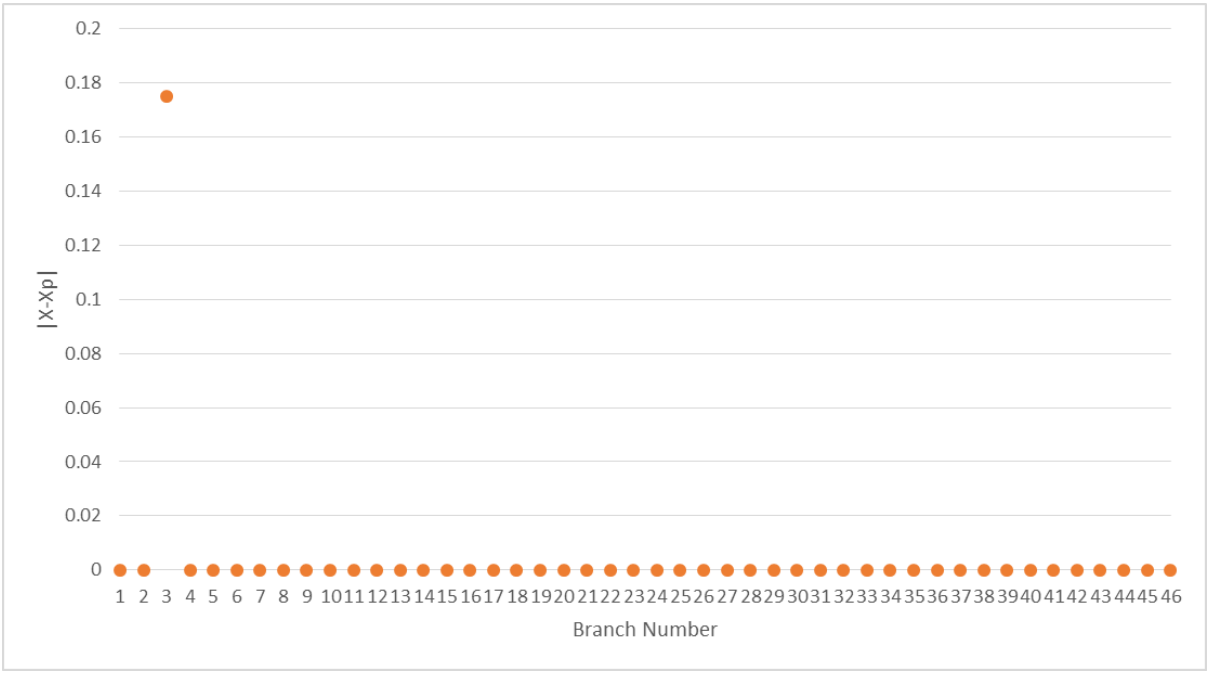

Figure 5.30 Alternating Direction Method for Multipliers Results for Outage at Bus 23-24

Figure 5.31 Alternating Direction Method for Multipliers Results for Outage at Bus 26-29

When the phasor angle measurement algorithm is applied on a 39-bus system, different results have been obtained in comparison with a 14-bus system but still, the outage branch can be detected. In Table 5.15 and 5.16, normalized angle distance (NAD) values indicate the outage line in the system. In addition, it also shows the pre-outage values of the system before the outage occurred, which is nearly equal to the values we have from Powerworld simulations.

Figure 5.32and 5.31 show the outage line when the distributed line change detection algorithm is applied. This algorithm identifies the branch number having an outage, and from the above figure 5.33, the difference of |x-xp| clearly shows that branch 3 (buses 23-24) has an outage. likewise, figure 5.20 identifies that branch 4 (bus 26-29) is faulty.

Both algorithms have successfully identified the outage line for 14-bus and 39-bus systems, but line detection using the PMU data algorithm uses the internal-external network model for the whole interconnected system, in which the goal is to locate the external line outages using the data within the internal system only Single line outage detection using PMU

data follows a complex searching process to find the outage line, but it can only handle the single line outage scenario. In contrast, ADMM methods are less complex compared to single line outage detection, which can increase the efficiency of security in SG monitoring.

CHAPTER 6

Conclusion and Future Work

The complexity, old technology in existing grid and penetration of distribution generation, the concept of smart grid has evolved in recent years. The grid is made up of microgrids, which in turn is the combination of different generators that are mostly installed at the consumer end to generate electrical power for consumers' own use, whilst the additional power can be sent to the grid. To manage the power systems with microgrids and bidirectional power flow, Smart Grid (SG) is developed to efficiently manage the bulk power system across the network. SG expands the existing capabilities of grid generation, distribution, and transmission to provide a system capable of handling future requirements for renewable energy generation, electric vehicles and the demand side management of electricity. SG is based on the CPPS, which is vulnerable to cyber-attacks, where an intruder can change the information sent or received from the grid. The effect of line outages on SG is discussed when there is an attack from any hacker that altered the information of phasor measurement unit (PMU). Power World Simulator is used to simulate IEEE 13-Bus and 39-Bus systems, having renewable energy generators to test the SG after line outage. In addition, two different line outage detection techniques are implemented to find pre-outage power flow and transmission line failure.

In this proposed research, the best algorithm out of all the available algorithms designed so far is addressed and presented on basis of less complexity and smaller time to process. PMU measurement-based method is found the most effective way to find line outage in the power system. Current PMU-based methods for line outage detection require information from internal and external network models of the whole power system to identify the line outages.

Single line outage detection using phasor angle measurements method is one of those methods used in this paper for line outage detection. It involves a long searching process to obtain information about the outage line and works only for single line outage problems in another research named “Monitoring for Power-line Change and Outage Detection in SG via Alternating Direction Method of Multipliers” WAMS containing PMUs are deployed at various locations in the buses. PMUs are responsible for the measurement of phasor and voltage at the buses. PDCs are used at higher levels to collect data from PMUs in the defined region. After that, the method given in this thesis for line outage detection is implemented, and these results are transmitted to WAMS to send the collected information to system operators. This method features low complexity distributed processing, which can enhance the efficiency, security and privacy level in SG monitoring.

Both algorithms have successfully identified the outage line for 14-bus and 39-bus systems, but line detection using the PMU data algorithm uses the internal-external network model for the whole interconnected system, in which the goal is to locate the external line outages using the data within the internal system only Single line outage detection using PMU data follows a complex searching process to find the outage line, but it can only handle the single line outage scenario. In contrast, ADMM methods are less complex compared to single line outage detection, which can increase the efficiency of security in SG monitoring.

In this thesis the impact of the research is studied only detecting fault on the transmission lines which makes the whole process a lot simpler and easy. The function of actual SG is much complicated and involves a lot of other components. A typical SG power system consists of following major components:

- Generators
- Transformers
- Switchgears

- Isolators
- Bus-Bars & Transmission Lines
- Lighting Arresters
- AMI
- Data Acquisition Systems
- HMI

Successful operation of SG is only possible if faults are immediately detected and rectified on all parts of the grid. The scope of study thus, can be widened to detect faults on all these components.

The flexible nature of ADMM method makes it adaptable to any other field where cyber physical systems are used. The study may be applied to detect faults in the operation of autonomous vehicles, smart appliances ,IT networks , data acquisition systems using 5G mobile communication system.

APPENDIX A

STEPS REQUIRED TO MODEL 14-BUS AND 39-BUS NETWORK (With Renewables)

For actual power system studies, it is necessary to have a real power system machine model, below figure shows the type of machine model available for power system studies. GENROU model is chosen, it gives a good approximation of practical synchronous generator having dynamics of interest for transient stability also. Until 2006, around two-thirds of machines in North America are represented by GENROU model. Generator options > Transient Stability > Machine Model > Insert.

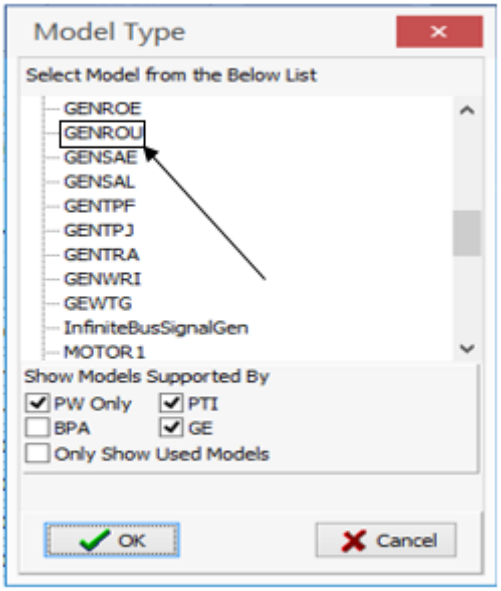

Figure A.1 Selecting GENROU model

Following window will appear having Machine model type as GENROU, as shown on the next page.

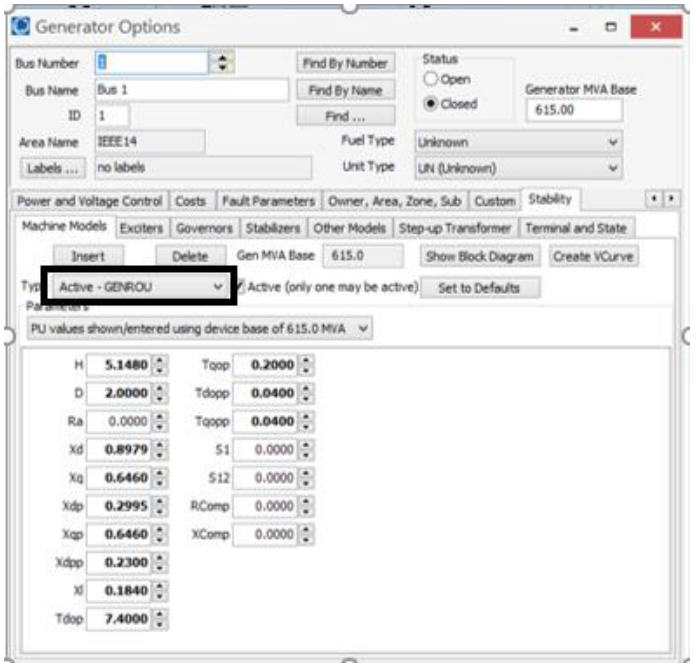

Figure A. 2 GENROU Model is active

In order to maintain the constant output, voltage exciter is used, in power world simulator have many types of exciters. For this system, IEET1 exciter will be used. Generator options > Transient Stability > Exciter

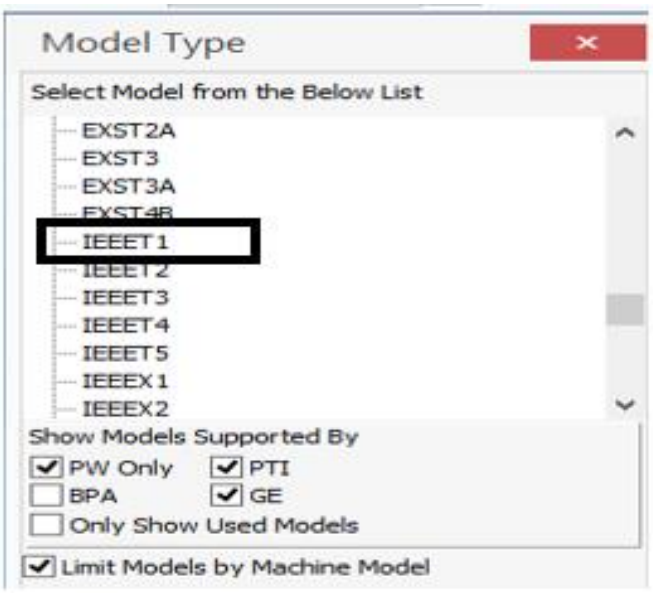

Figure A. 3 Exciter selection

It can be seen that exciter is selected as Active part in the below figure.

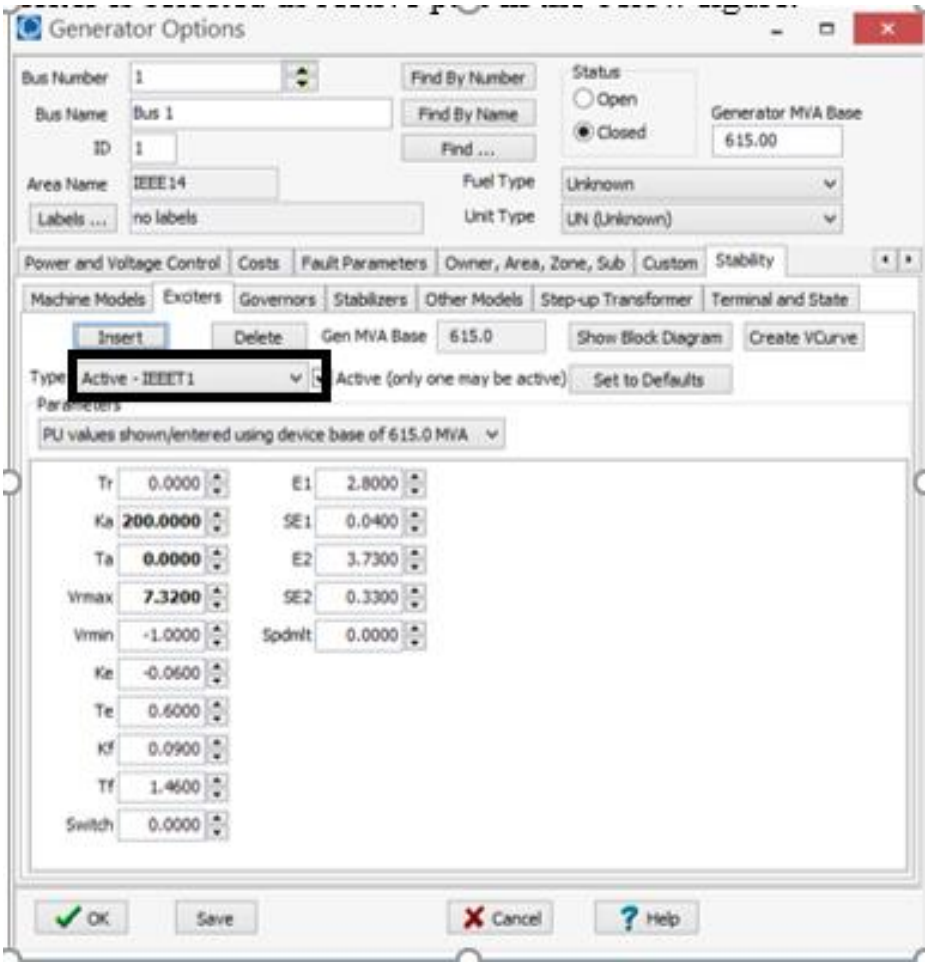

Figure A. 4 Exciter Activated

Wind Turbine Modelling in Powerworld:

Powerworld supports all four types of Wind turbine models.

1. Induction Generators with fixed rotor resistance
2. Wound rotor induction generator with variable rotor resistance.
3. Doubly-fed induction generator (DFIG)
4. Full Converter Generator

In order to consider wind turbine equivalent model in Power world, all the above generator are available for Wind turbine. Follow the same steps as above for inserting GENROU model and select GEWTG machine which represents Doubly-fed induction generator.

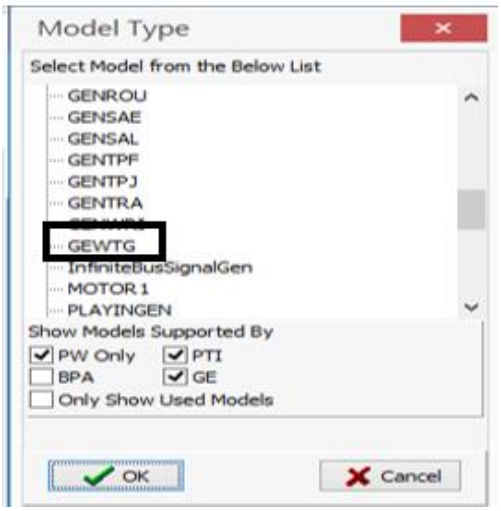

Figure A.5 Selecting GEWTG model.

GEWTG will be selected with all its default values as shown below.

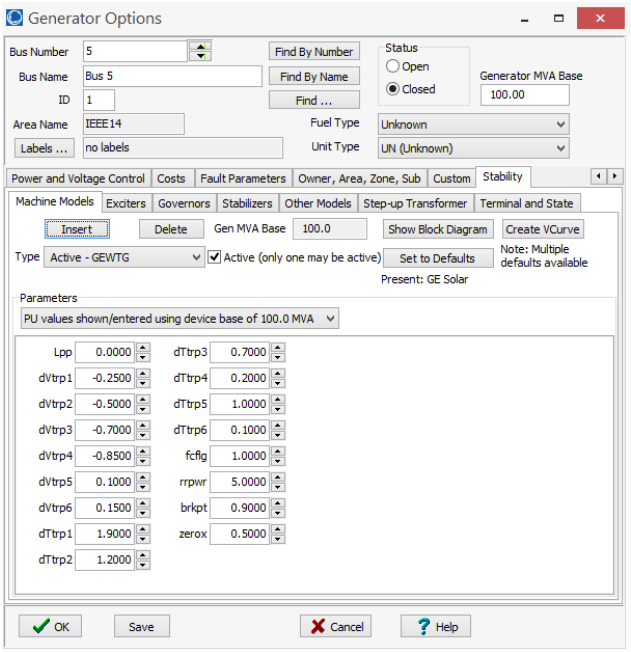

Figure A.6 GEWTG is active

For exciter, EXWTGE model is used to model it as reactive power control Wind turbine.

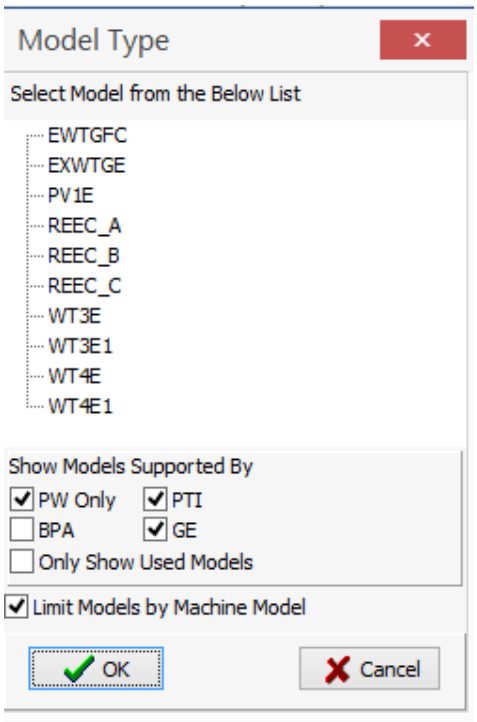

Figure A.7 EXWTG model selection

EXWTGE model is selected as highlighted below.

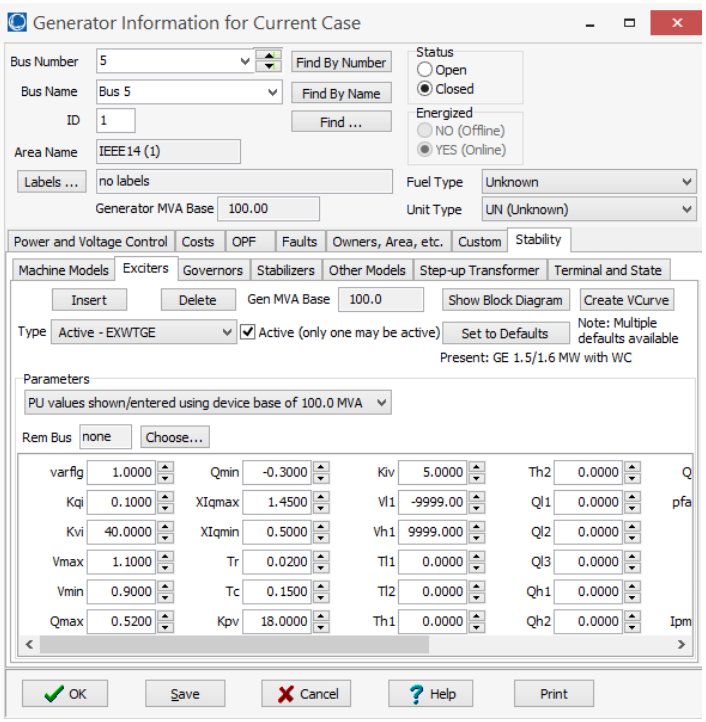

Figure A. 8 EXWTGE is active

Governor model is replaced by WNDTGE type, it models the inertia of wind turbine and its pitch control.

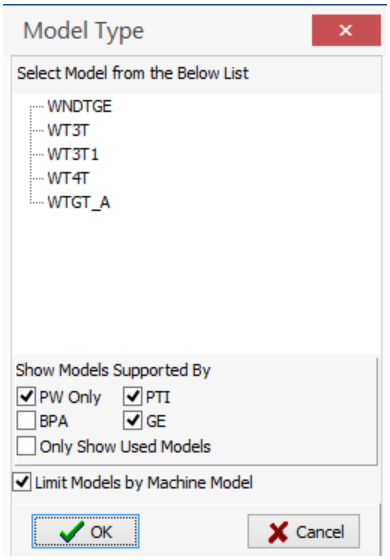

Figure A. 9 WINDTGE MODEL

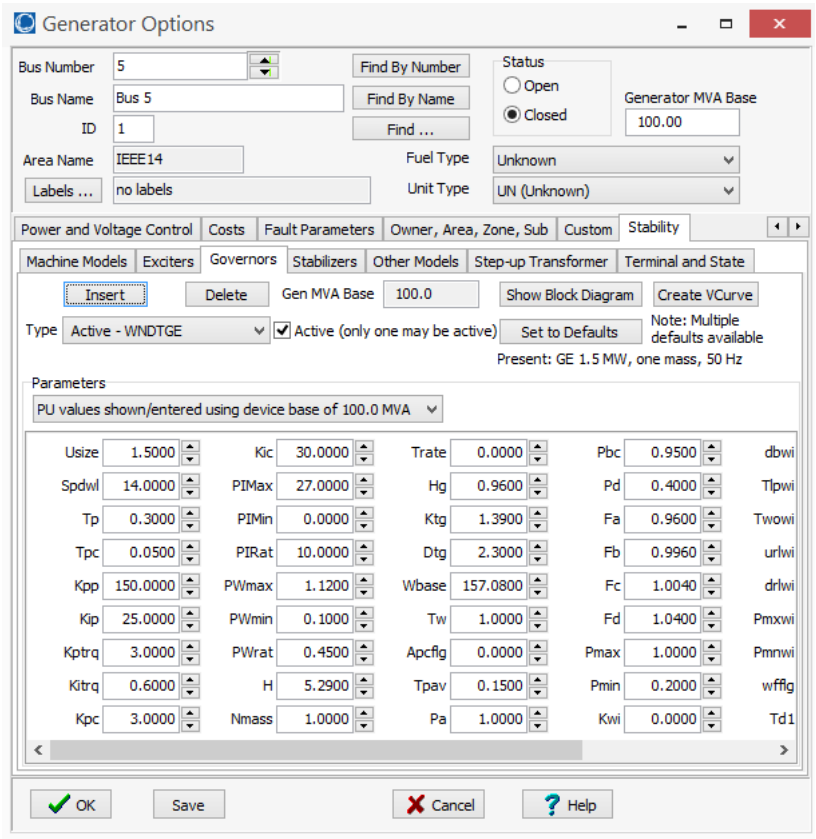

Figure A. 10 WINDTGE is active

PV modelling in Powerworld:

In order to design PV panels' equivalent model, REGC_A is chosen as a solar panel machine model.

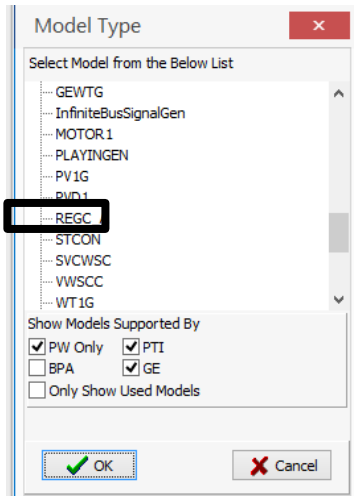

Figure A. 11 ***REGC_A for Photovoltaic***

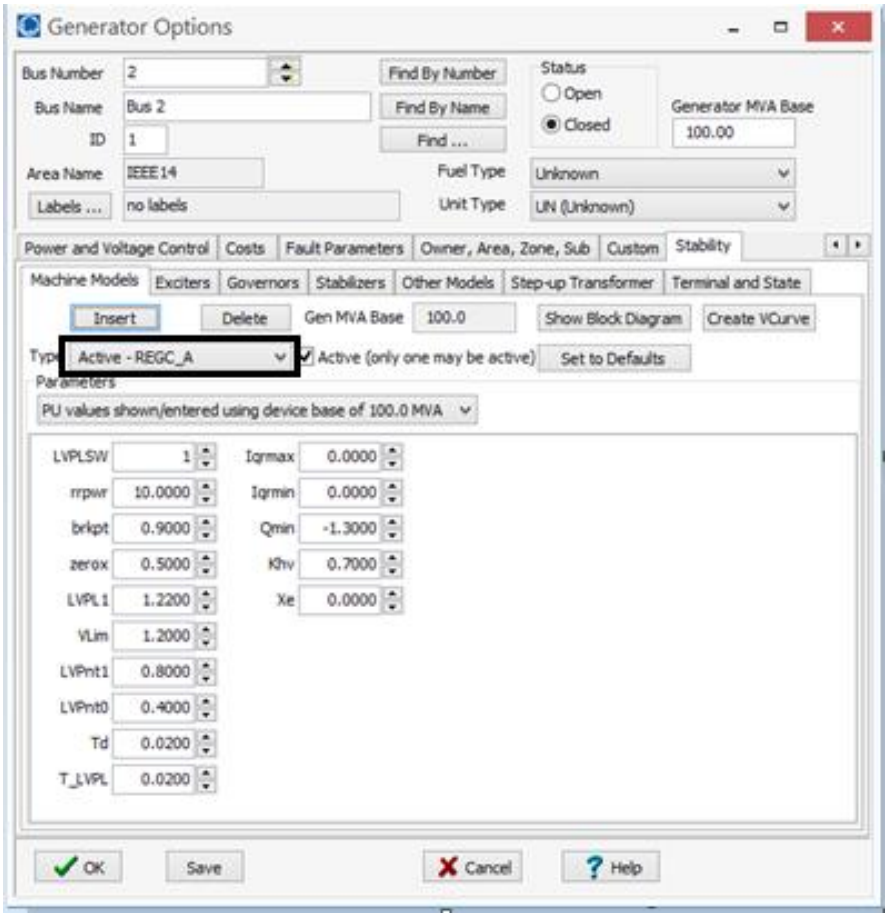

Figure A. 12 REGC_A is active

For Exciter REEC_A is selected.

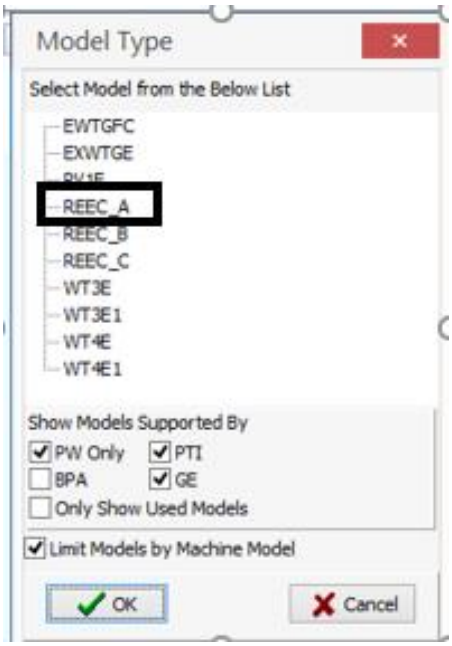

Figure A. 13 Exciter REEC_A

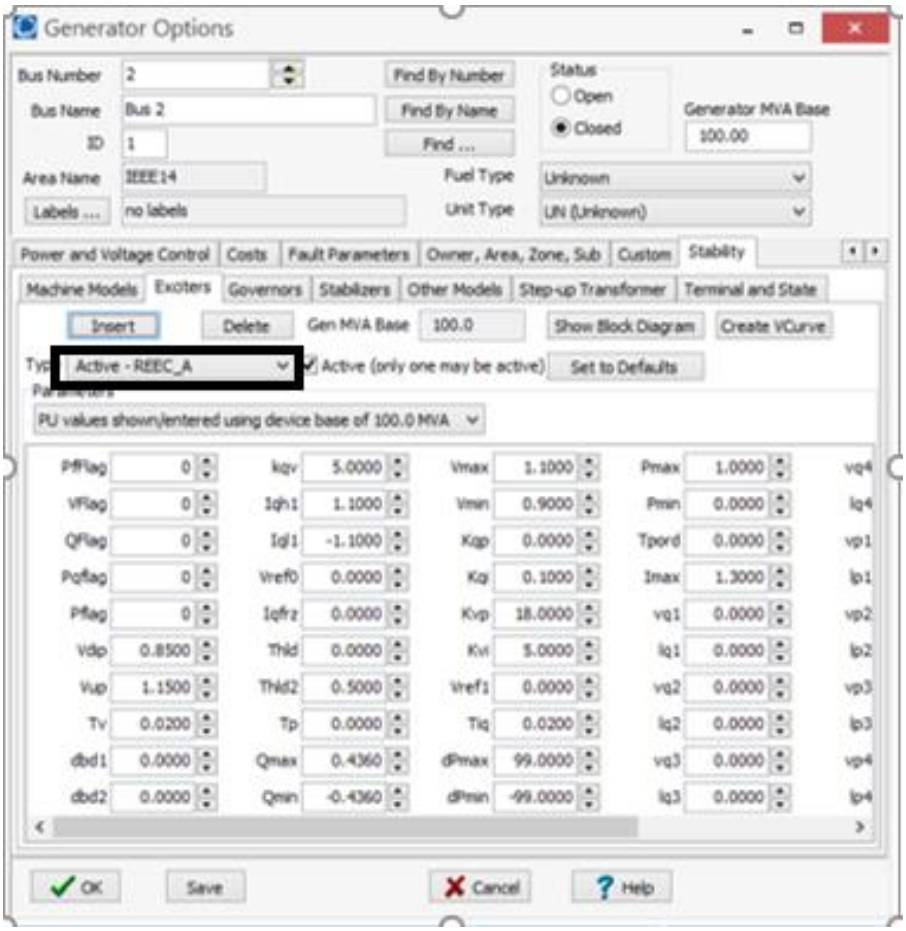

Figure A. 14 REEC_A active

Plant controller is required for PV which can be found in other model types section.

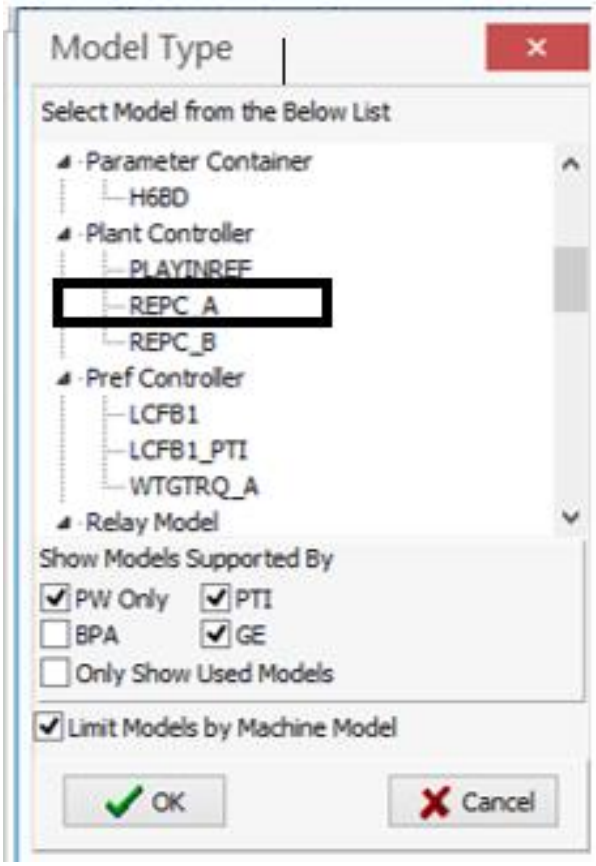

Figure A.15 Plant Controller Model Type

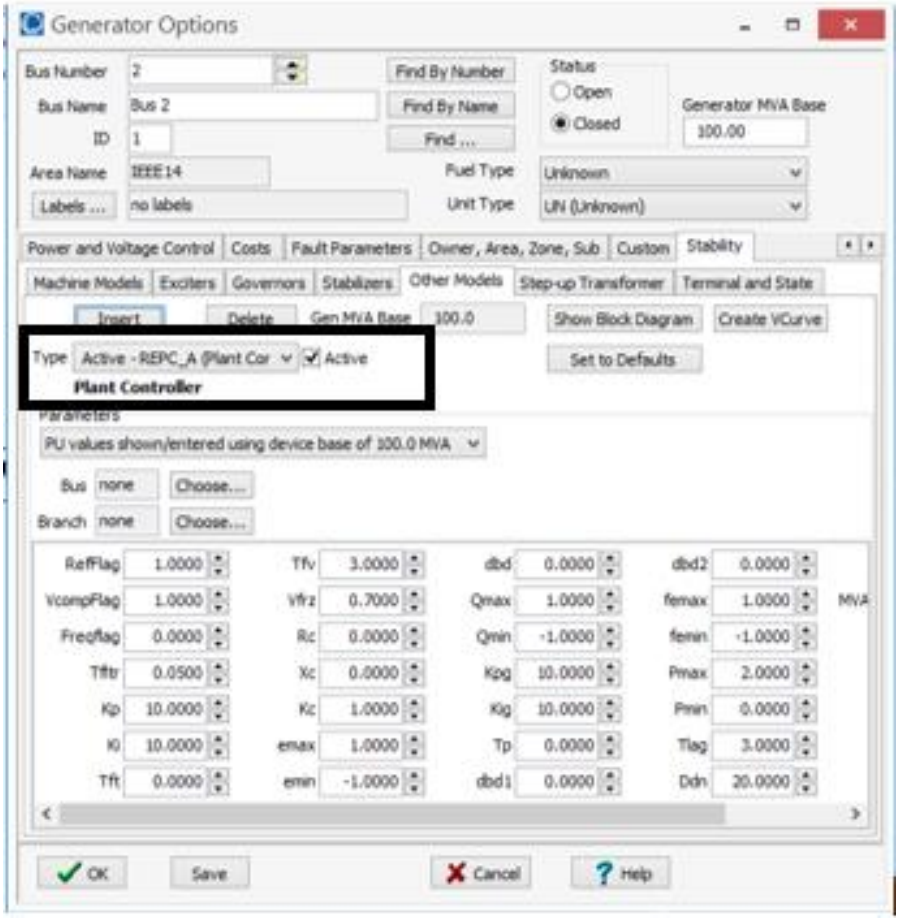

Figure A. 16 Plant Controller activated

LOAD MODELLING FOR THE SMART GRID SCENARIO:

Since distributed generation is an essential of the smart grid, all loads must be modeled as distributed generation load models.

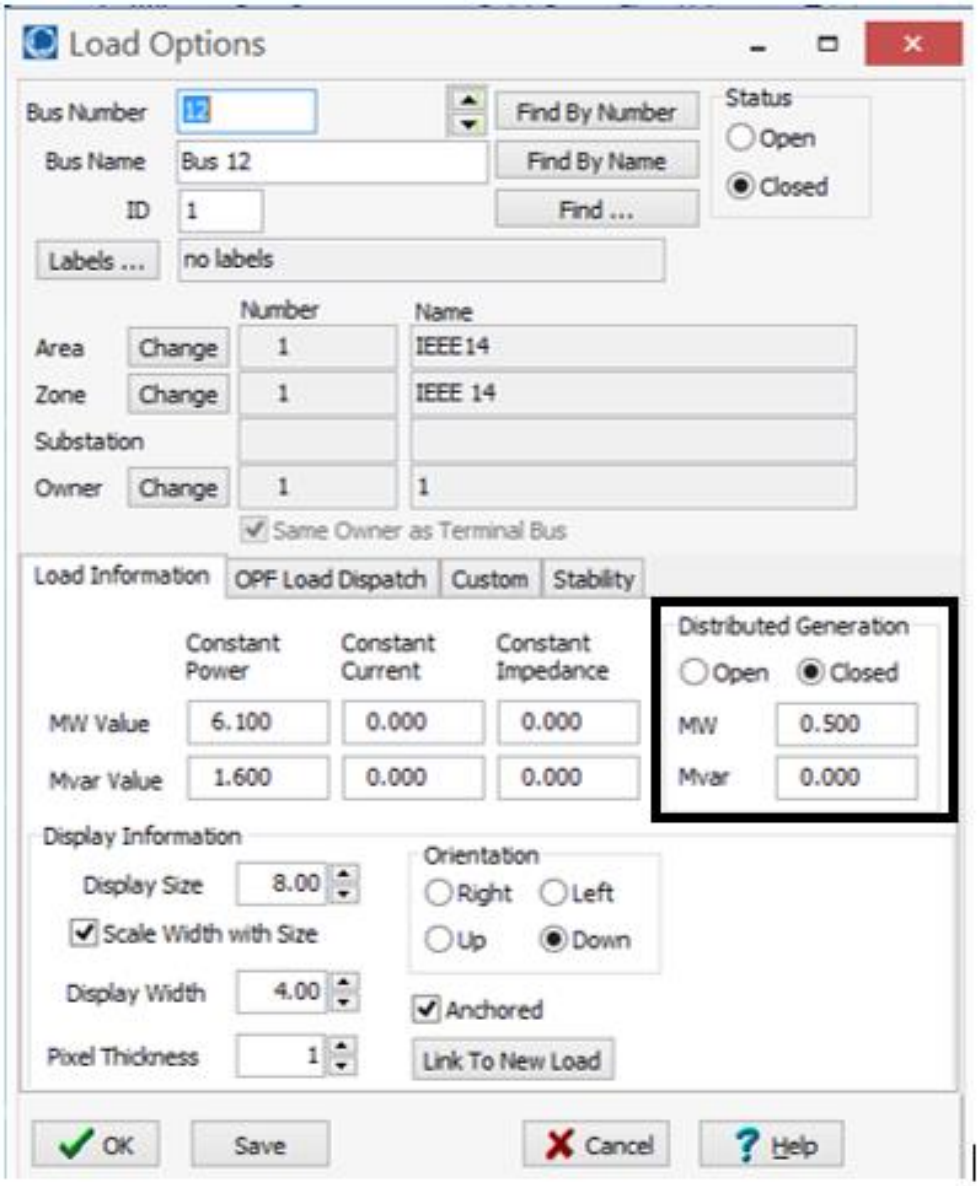

Figure A. 17 Selecting DISTRIBUTED GENERATION for LOAD model

APPENDIX B

STEPS REQUIRED TO APPLY TRANSIENT STABILITY

PowerWorld has the functionality to apply test system stability during and after the fault state. As an instance, for the below system a fault arises between bus-1 to bus-5 for a duration of 1 sec. Following steps are followed to apply this condition.

1. Select Transient Stability as shown in the figure below.
2. A window comes up showing SELECT STEP window on the extreme left and its selected option at the middle. Select Simulation from select step window.
3. Under transient contingency elements window select insert.
4. Transient stability contingency dialog box will open, select branch since we are testing fault between bus-1 and bus-5. Select bus-1 and choose bus-5 from circuit window.
5. Insert time for the fault as 1 sec. Under the type, section choose to apply fault.
6. Choose balance 3 phase fault as fault time and select solid in the fault across the field. Press Ok.
7. Apply steps 3-6 to clear the fault at 1.5 sec. In the type section select clear fault.
8. Now select options from select step window.
9. In the power system values section insert nominal and initial frequency as 50 Hz for Australian power systems.
10. Click Run Transition Stability located above the select step window.

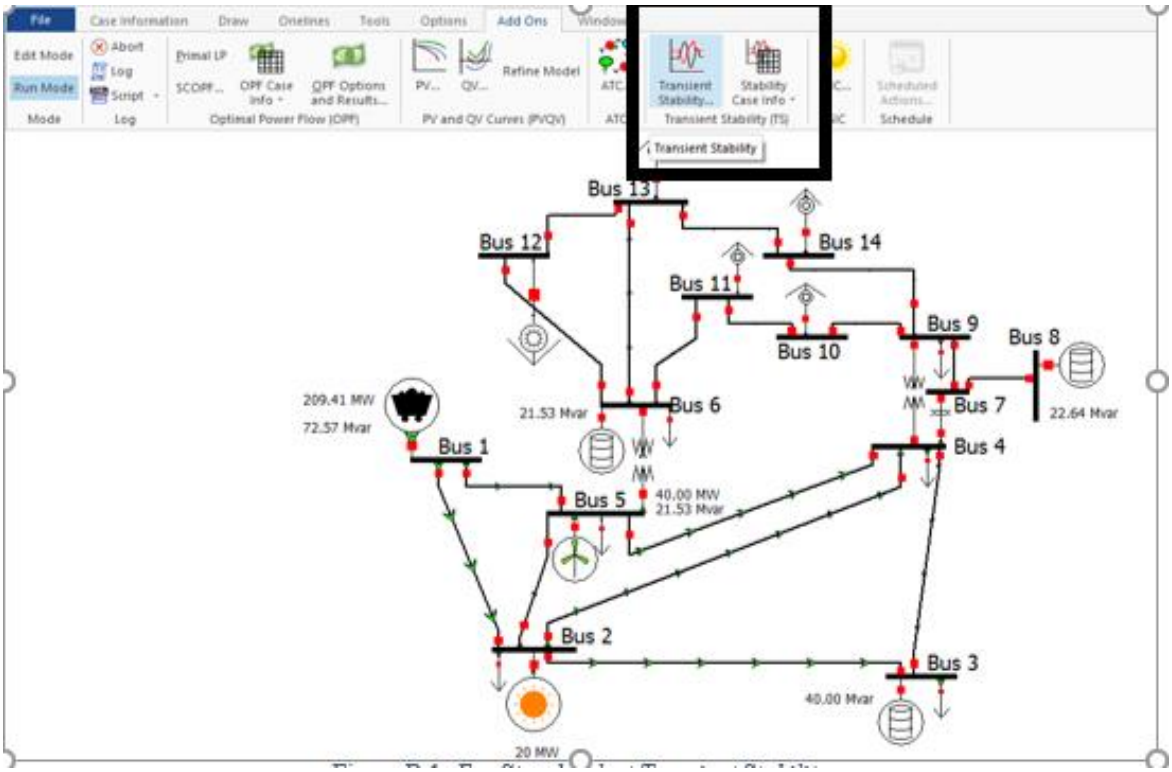

Figure B. 1 For Step-1 Select Transient Stability

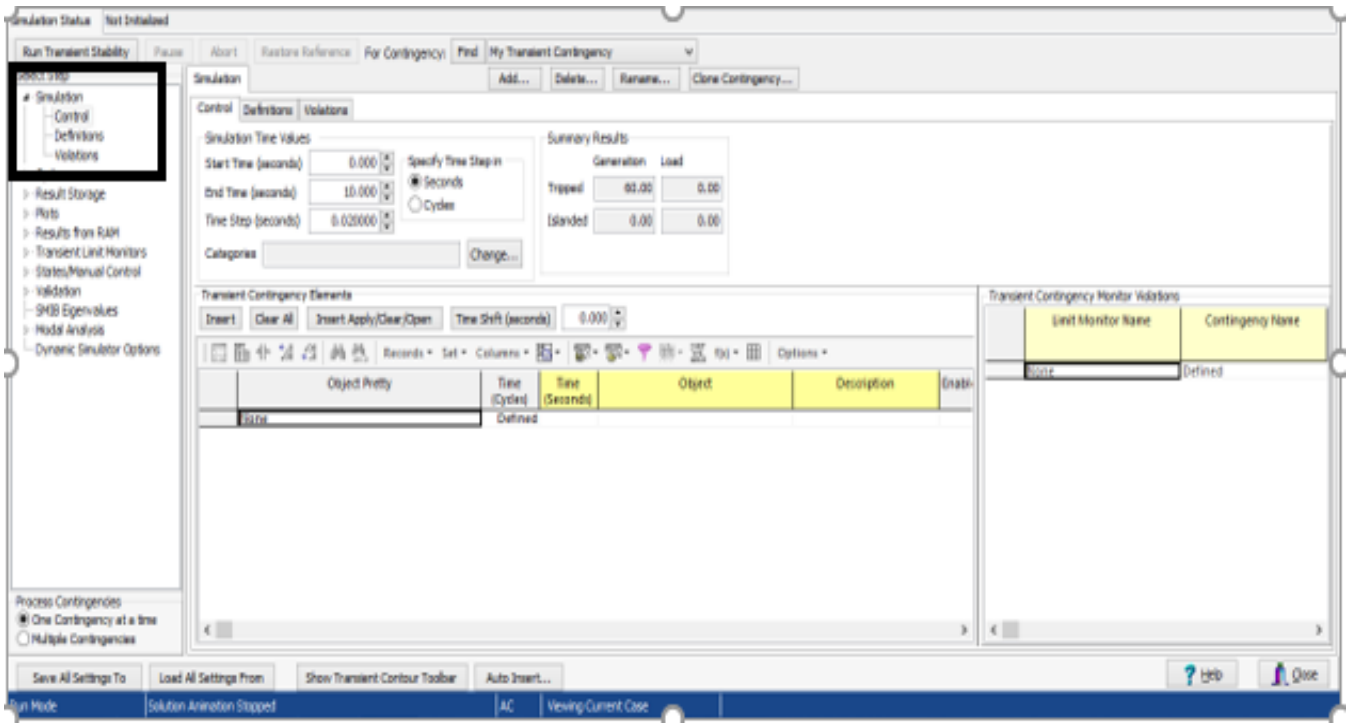

Figure B. 2 For Step-2 and 3 (Select Simulation and insert Transient Contingency Elements)

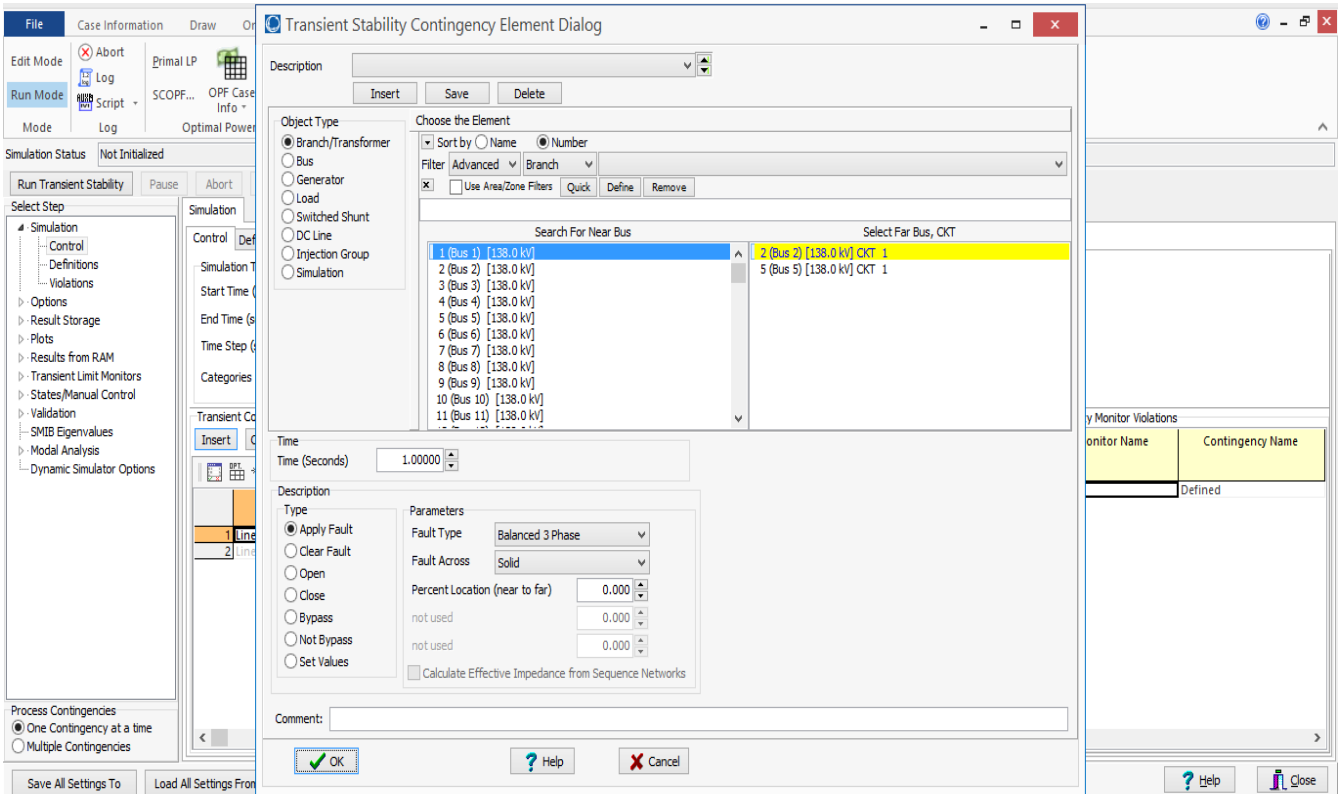

Figure B.3 For step 4,5 and 6 (To insert fault scenario either apply or clear the fault)

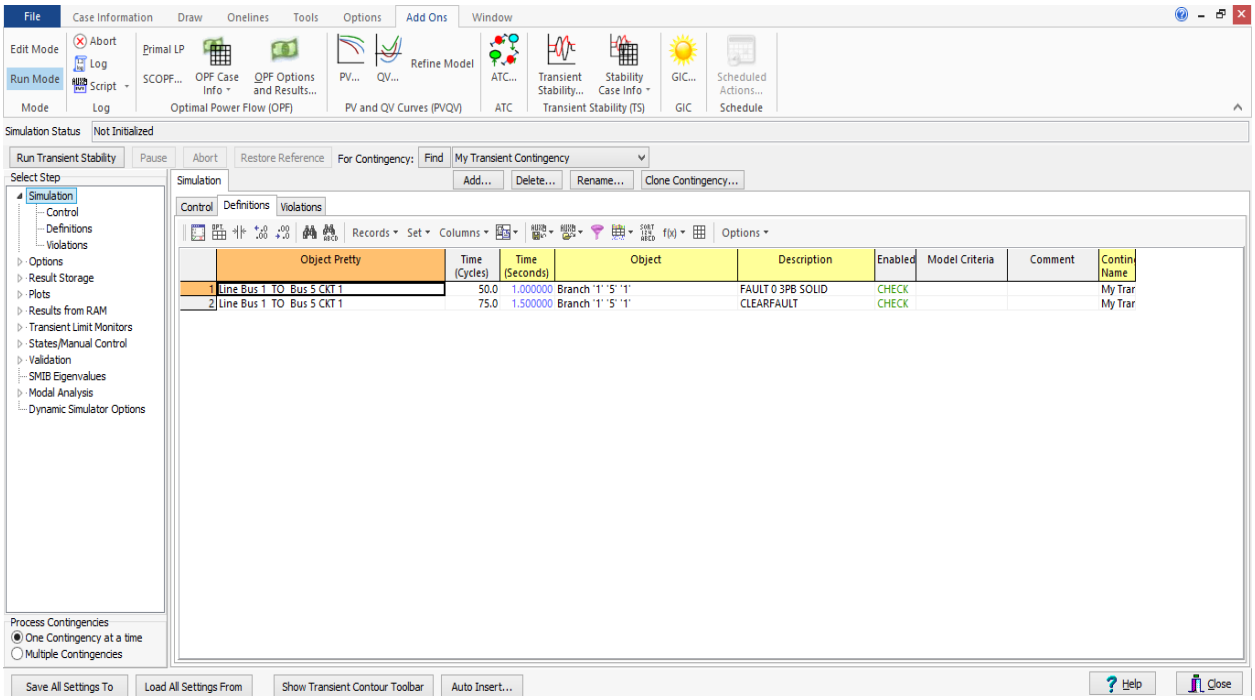

Figure B. 4 After following step 1-7

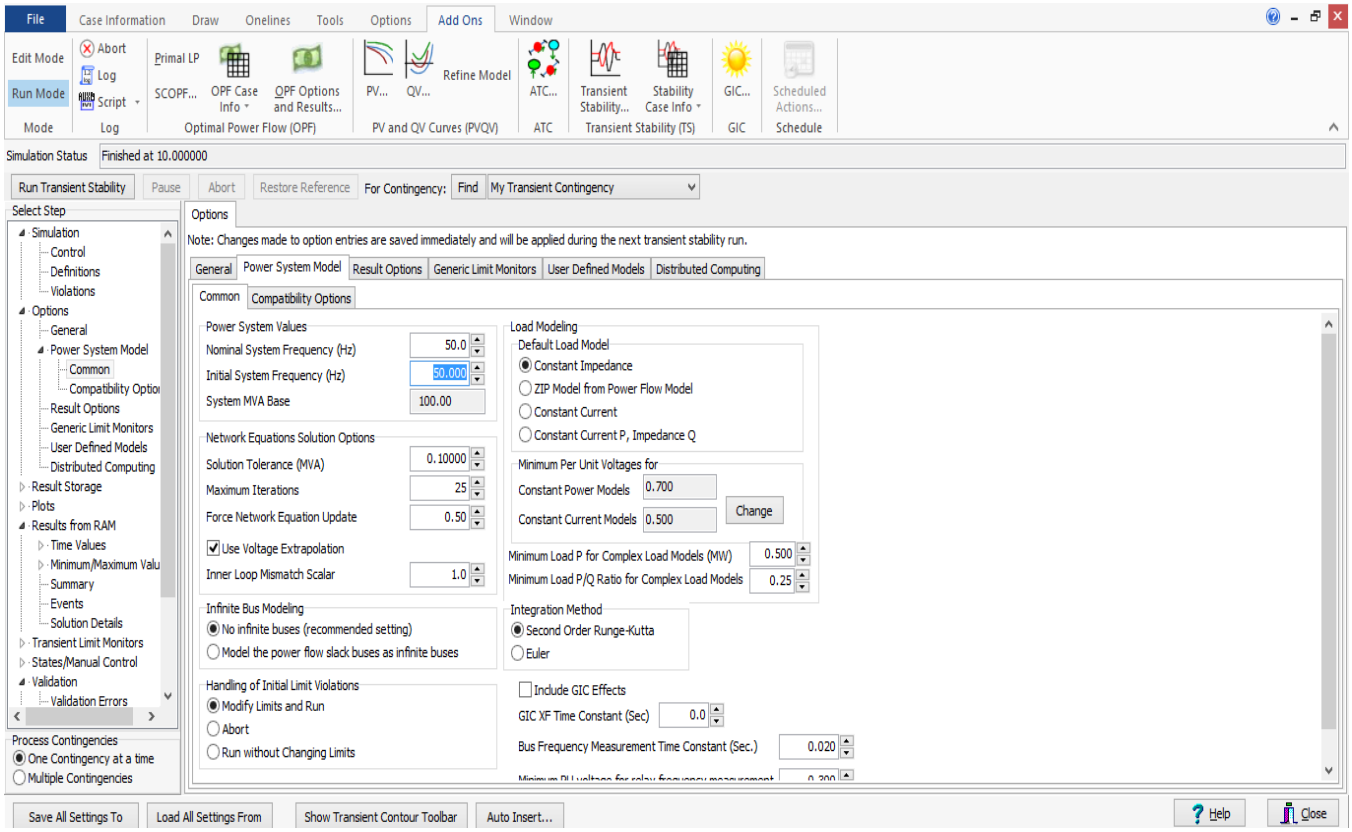

Figure B. 5 For step 8,9 and 10 (Run transient stability)

APPENDIX C

Research Paper

Effect of Line Outages on Cyber Physical Power System

Hafiz Saleem, Prof. Akhtar Kalam, Asif Gulraiz
Victoria University, Australia, Victoria University Australia, DHA University, Pakistan
hafiz.saleem@live.vu.edu.au, akhtar.kalam@vu.edu.au, asif.gulraiz@dsu.edu.pk

Abstract*—An uninterruptible supply of energy is the biggest challenge faced by power engineers. Due to the involvement of information and communication technology (ICT), the behavior of the power grid has transformed completely in recent years. The evolution of the existing grid system has resulted in bidirectional power flow. The grid is made up of micro grids, which in turn is the combination of different generators that are mostly installed at the consumer end to generate electrical power for consumers' own use, while the additional power can be sent to the grid. In order to manage such power systems where we have micro grids and bidirectional power flow, Smart Grid (SG) is developed to efficiently manage the bulk power system across the network. SG will expand the existing capabilities of grid generation, distribution and transmission to provide a system capable of handling future requirements for renewable energy generation, electric vehicles and the demand side management of electricity. SG is based on the cyber physical power system (CPPS), which is vulnerable to cyber-attacks, where an intruder can easily change the information sent or received from the grid. In this paper, the effect of line outages on SG is discussed when there is an attack from any hacker that altered the information of phasor measurement unit (PMU). The IEEE 13-Bus and 39-Bus systems are used, having renewable energy generators to test the SG after line outage. In addition, two different line outage detection techniques are implemented to find pre-outage power flow and transmission line failure.

***Index Terms*—current distortion; distortion factor; filters; harmonics; nonlinear loads; power factor; reactive power**

I. INTRODUCTION

Today's power grid is not only dependent on pure electrical components; it is equipped with sensors to provide measurement at highest data rate and resolution. Due to the addition of a large number of sensor measurements, which added complexity in the power networks, there is a need for CPPS, which can provide simulations and modeling for assessing the characteristics of selective networks fabrics.

A growing demand for a dependable source of energy and other technological developments have inspired the design of an SG. This electrical grid will improve the existing capabilities of the grid's generation, transmission, and distribution to offer a system that is able to handle upcoming requirements for distributed generation, electric vehicles, renewable energy sources and the consumer side management of electricity [1]. In order to attain such objectives, wide area measurement and management systems, automated substation and Advanced Metering Infrastructure (AMI) are being deployed [2]. Increased use of ICT to achieve the required aims and objectives of SG is giving growth to CPPS. However, it is difficult to understand the dependencies between cyber and power domains as well as the impact of cyber issues on the power system.

While studying cyber physical systems (CPS), certain key issues emerge in so-called general-purpose computing. In any software, the time required to perform a specific task could be an issue of performance, not accuracy. It is not wrong to take a longer time to finish any task; it is simply less appropriate, hence less appreciable. However, in CPPS, performing a task, for example, fault detection and its immediate remediation, is time critical. Minor delay or less accurate fault detection may lead to a catastrophic state of failures throughout the system [3]. Risks arising from the cyber system as well as conventional and non-conventional physical system possibilities start to contribute in the overall security of the grid. Research on the behavior of power systems with cyber components is still in its early stages and material on the interrelationship of physical and cyber components is almost non-existent [4].

CPSs are quite common in power systems, and these systems must operate reliably in case of catastrophic failures and other external threats to the power network.

Today's power grid, which has traditional power components linked with advanced communications and control systems and data processing units, is rapidly becoming one of the most complex and largest CPSs. This kind of complex system, which is being developed to attain advanced levels of flexibility, effectiveness and fault resistance, may become the origin of complicated catastrophes too, and this can really diminish constancy [4].

Therefore, robust fault detection, isolation and rectification have become one of the biggest challenges today to fulfill the promises of SG. The aim of the study is to discuss the techniques for fault detection, which will be one step closer to the self-healing SG.

In order to design a reliable SG, there is a need to address all the potential issues, including protection from cyber-attacks. Assessing the possible attack effect on the system requires an assessment of the grid's reliability on the cyber infrastructure and its capability to resist major failures [17]. In addition to that, much detailed analysis of cyber-physical relationship within the grid is necessary to determine the requirement of cybersecurity efforts [1].

The aim of the study is to test different algorithms on a power network model for detection of different faults in order to enable efficient operation of SG. Since robust fault detection, isolation and rectification have become one of the biggest challenges today, this study will contribute to following aspects of SG:

- Secure operation of SG
- Fault identification
- Accuracy in determining fault location
- Reliable data and information network
- Enabling of efficient generation and distribution using renewable sources
- Security of supply

II. LITERATURE REVIEW

Various methods have been implemented with reference to fault detection, power grid weak point prediction and fault rectification. When it comes to identifying a fault, a scheme is developed to identify outage in transmission lines [3], which is based on measurements of phasor angle information. In addition [4], this method is also designed for more than one line failure identification. A method is developed to forecast the fragile power system areas using linear optimization and worst configuration prediction [5]. Another study was done on fault identification using a four feature selection criteria method. The features include i) stepwise regression, ii) testing hypothesis, iii) selection using Akaike's information criterion (AIC) [7]. An approach to identify and detect faults is suggested using Petri net i.e. by obtaining protection system modelling specifics of the grid [7]. The matching pursuit (MP) approach is adopted [7] to measure the stability of transient voltage and voltage sags; this approach uses a sinusoid dictionary for identification of fault values.

Once the process of identification and detection is completed, it is time to find the exact location and region of concussion. An approach that uses wavelet coefficients (WC), is employed to find the location of fault, and this approach uses the WCs of voltage and frequency fault signals [11] [12]. The before and after values of WCs are compared to precisely estimate the location of fault [13]. The Gaussian Markov Random Field (GMRF) method is proposed to find fault location by measuring the phasor angles [14] [15].

III. LINE OUTAGE SCENERIO IN SMART GRID

Consider a hypothetical case on IEEE 14-bus system and suppose there is a requirement of extra power at bus-13 from 13.5 MW to 18 MW. A message will be sent from bus-13 to the supervisory control and data acquisition (SCADA) system for a request of extra power but some hackers took that information and tempered it to a different value: from 18 MW to 70 MW. Due to this change in information, the generator will supply more power as required, which will result in exceeding the branch flow ratings as shown in fig. 1. It can be seen clearly that a fabricated message violated the total power flow limit condition across different branches (i.e. Bus 1-2, 1-5 and 6-13).

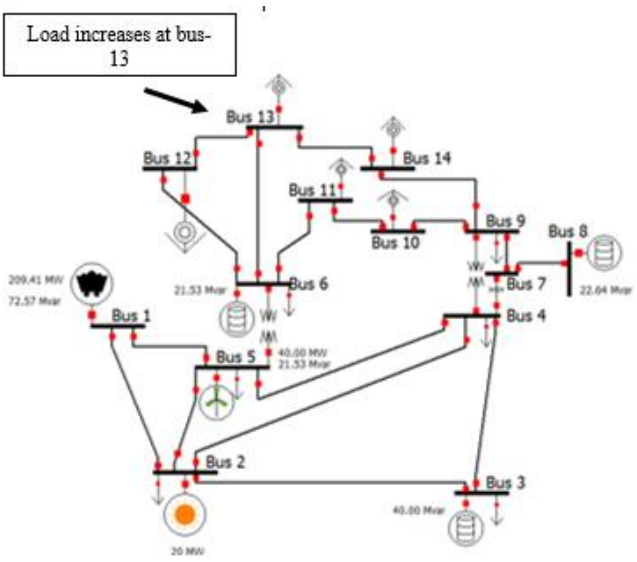

Fig. 1. IEEE 14-bus modified system

Such incidents clearly show that there is a need for SG security to make the system less vulnerable, and a security check will be needed in order to predict the correct power flow before and after the load change.

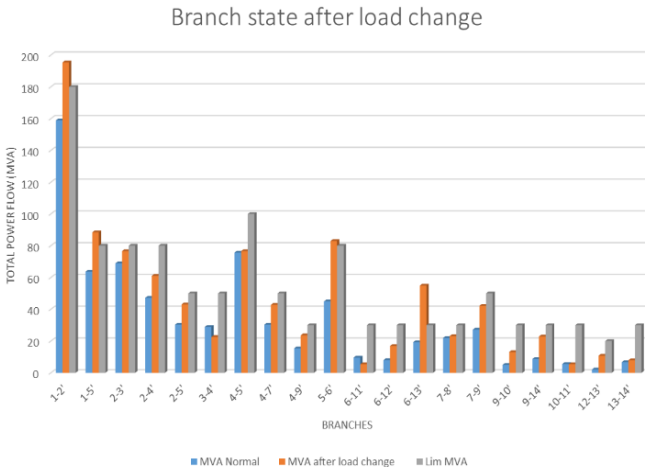

Fig. 2. Power flow before and after load change

IV. METHODS USED FOR LINE OUTAGE DETECTION

A. Single Line Detection Using PMU Data

In this algorithm, detection of system events is done using PMU data, such as the phasor angles from the transmission lines and information on interconnections of the system [5]. The fast oscillation in phasor angles is not being evaluated and it is assumed that only quasi-steady state values of the measured phasor angles before and after the disruption are compared [5]. Change in phasor angle is Δθ, while K is the number of phasor angles detectable at PMU [5].

$$E^* = \arg\min || \Delta\theta_{observed} - f(E)|| \quad (1)$$

Where E = set of events to be monitored, f (E) relates to an event E as a function to the changes in angle due to the event that occurred.

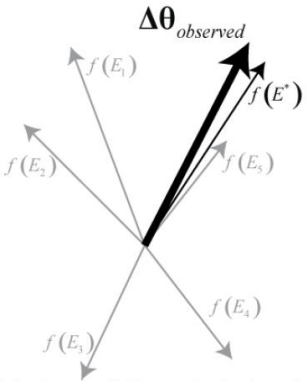

Fig. 3. Resolving phasor angles to determine the event that matches the angle changes [7]

Fig. 3 shows a visual illustration of the above equation but it is limited to two-dimensional array, while equation (1) works for K-dimensional array for phasor angles. According to the above figure, f (E1-5) are least matched events and are colored gray, whereas f(E*) event is best matched.

This method is for single line detection. It uses PMU measurements and information from transmission lines and transformers to find the accurate node where outage takes place. In addition, this method focuses on the pre-outage flow values of the faulty system. A method of edge detection technique was also used to estimate the occurrence of events;to achieve that , it is first necessary to measure the change in angles at the quasi-stable state. Any rapid oscillation in the phase angle needs to be filtered out so that only the original signal is extracted; low pass filters are used for this purpose.

B. Multiple Scattered Line Outage Detection

The main purpose of this algorithm is to design a multiple scattered line outage scheme where the outage is on more than two lines in different geographical locations. This technique, which is employed to detect multiple outages, is called the wide area measurement system (WAMS) [16]. A basic WAMS architecture is shown in fig. 4. In a WAMS, PMUs are installed on the buses, which

measure voltage and current phasors. This information is then passed on to the phasor data concentrator (PDC). The algorithm is then applied to the data of each PDC separately to detect line outage. This information is then transferred to WAMS and is again passed on to the SCADA system to enable it to take appropriate action [16].

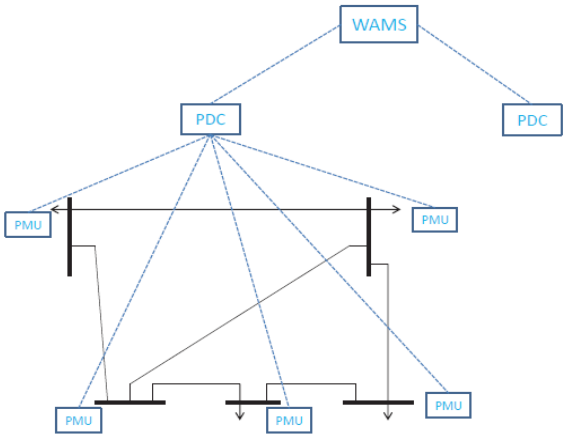

Fig. 4. Basis WAMS architecture [16]

For a typical transmission system, phasor measurement information is expressed in terms of rectangular components of a vector; and $\bar{Y}_n$ can be expressed as the following linear equation [16].

$$\bar{Y}_n = \overline{H_n x} + \overline{g_n} \qquad (2)$$

Where x = State of the system having all line currents

$\overline{H_n} \in R^{Mn\ x\ 2Ni}$ is the measurement matrix,

Mn = Number of measurements within n-th PDC area.

Nl = Number of lines in the whole system

$\overline{g_n}$ = Additive Guassian noise vector

In this scheme, in order to perform line outage detection, measurement and prior information of the states are combined [16]. The statistics of previously stored data of line current is denoted by $\bar{x}$, which have normal distribution having mean vector xp and covariance matrix Λp. An assumption was made that state variables are independent, which indicates Λp is diagonal. At this point, let us assume one central control center processes the measurements to detect line outage and employ li-norm approximation, leading to the convex optimization criterion below.

$$\min_{\mathbf{x}} \frac{1}{2}\|\mathbf{y}-\mathbf{H}\mathbf{x}\|_2^2 + \lambda\left\|\mathbf{\Lambda}_{\mathbf{p}}^{-1/2}(\mathbf{x}-\mathbf{x}_{\mathbf{p}})\right\|_1 . \qquad (3)$$

If the above equation is decomposed into N PDC areas, then the above equation can be expressed as

$$\min_{\mathbf{x_n}} \sum_{\mathbf{n}=1}^{N} f_{\mathbf{n}}(\mathbf{x_n}) \quad . \qquad (4)$$

According to the ”cost function” for each PDC is

$$f_{\mathbf{n}}(\mathbf{x_n}) = \frac{1}{2}\|\mathbf{y_n}-\mathbf{H_n}\mathbf{x_n}\|_2^2 + \lambda\left\|\mathbf{\Lambda}_{\mathbf{pn}}^{-1/2}(\mathbf{x_n}-\mathbf{x_{pn}})\right\|_1 . \qquad (5)$$

where Xn, Hn, Λn and Xpn are the states involved in n-th PDC. Now, derivation to solve the optimization problem in equation 4 is done in a distributed manner. Take xn as the subset of x, which has the states for n-th PDC and also consider xnm as the value for sharing different states among neighboring n-th and m-th PDC. Equation 3 can be rewritten as

$$\underset{\mathbf{x_n}}{\text{minimize}} \quad \sum_{\mathbf{n}=1}^{N} f_{\mathbf{n}}(\mathbf{x_n}) \qquad (6)$$

Now we can apply alternating direction method of multiplier (ADMM) [16] from equation 1 to solve the line outage detection problem derived in equation 6 having a distributed mechanism. Xnm and Zn are introduced as auxiliary variables in order to be considered for ADMM framework. Equation 6 can be expressed as

$$\begin{aligned} \underset{\mathbf{x_n},\vartheta_{\mathbf{nm}},\mathbf{z_n}}{\text{minimize}} \quad & \sum_{\mathbf{n}=1}^{N} f_{\mathbf{n}}(\mathbf{x_n}) \\ \text{subject to} \quad & \mathbf{x_{nm}} = \vartheta_{\mathbf{nm}},\ \mathbf{m} \in \mathcal{N}_{\mathbf{n}};\ \mathbf{n},\mathbf{m} \in P \\ & \mathbf{x_n} - \mathbf{x_{pn}} = \mathbf{z_n} \end{aligned} \qquad (7)$$

This method is used for the same purpose of transmission line outage detection. However, it followed a different procedure since the convex relaxation technique is applied to find out line failures using the same scenario as in the single line detection technique, where numbers of PMU are limited. This paper also applied ADMM to avoid complex computation as in other PMU-based outage detection methods using the 9-bus system as a model shown in fig. 5. Although all these methods take raw data that may encounter security issues as well, this method has a limited number of PMU data and there is no use of raw data in order to calculate outage line detection. They use the network of WAMS, in which each area has a number of PMUs installed at the buses to measure bus voltage phasors and branch current phasors that are applied on certain buses. It also uses the phasor data concentrator (PDC), which takes data from the PMU in its area. After that, a line detection algorithm is applied, but only the calculations after fault detection are sent to WAMS.

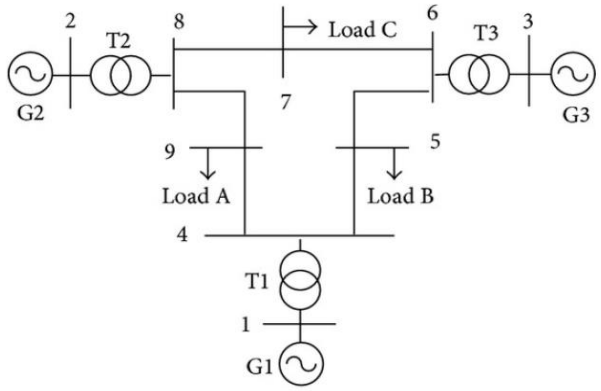

Fig. 5. The 9-bus test system

v. SIMULATIONS

Consider a 14-bus network and apply a line outage at different branches.

A. Simulated Outage at Branch 2-3

A fault is applied at branch 2-3; the fault will occur after 0.5 seconds of simulation started. There will be an outage between the transmission line of bus 2 and 3. Once the fault is applied, power flow will be different at all buses, so PMUs are installed at different buses to keep a record of these changes in the network.

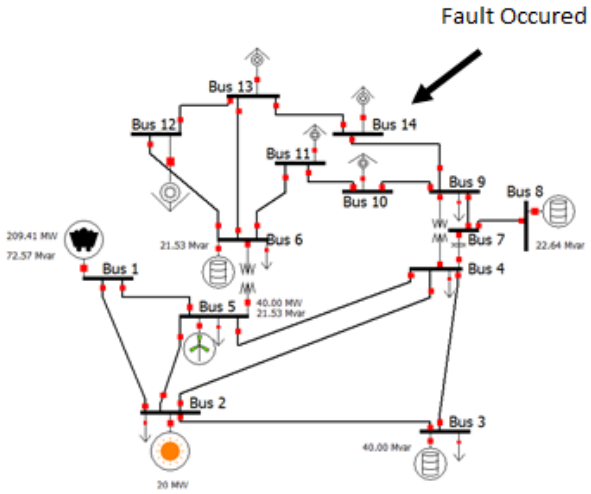

Fig. 6. Fault location at 14-bus network

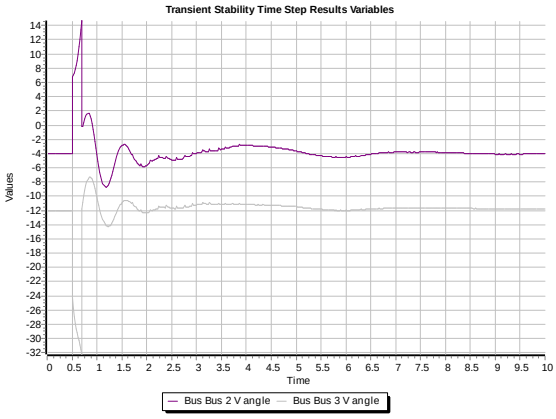

Fig. 7. Voltage angles at bus 2 and 3 after the fault

From the graph of fig. 7, when the fault occurred, instability took place at bus 2 and 3, which causes continuous change in angles. It settled down after a certain interval.

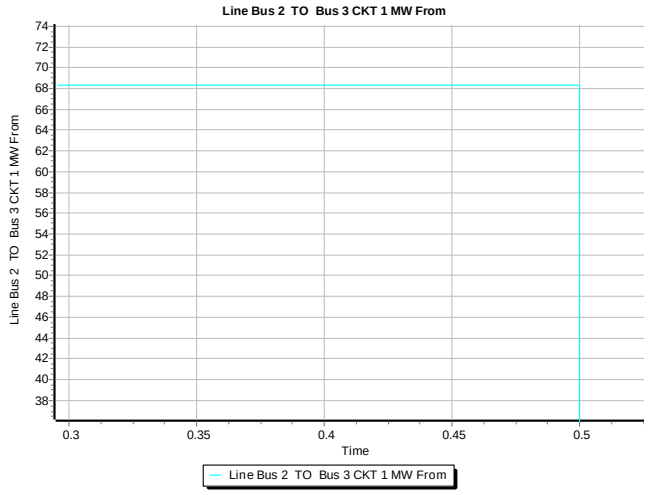

Fig. 8. Pre-outage flow (Bus 2 – Bus 3

Fig. 8 clearly shows the pre outage flow between bus 2 and 3, these values need to be find out using the selected algorithms. Since fault occurred at 0.5 second selected transmission lines are disconnected from the system. During the same time when line outage occurred other lines will get overloaded since the power taken from the faulty line will be transmitted through other lines.

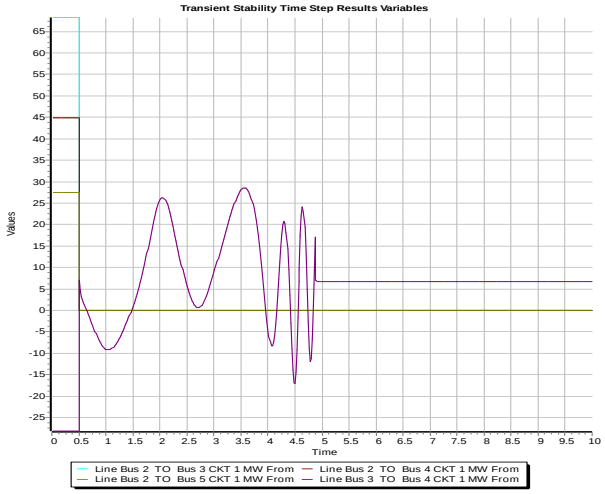

Fig. 9. Power Flow between bus 2 – 3 and adjacent buses

Since outage at line 2 to 3 created an instability throughout the system, it is evident from the above fig. 9 also. Power flow between bus 3 and 4 also disturbed after the fault.

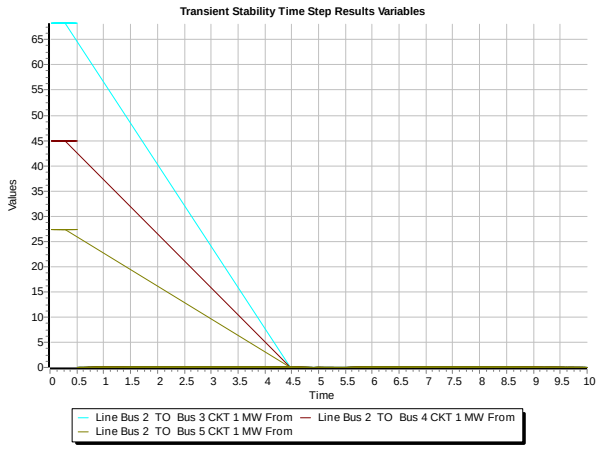

Fig. 10. Outage occurred at other branches also

In fig 10, Outage lines are shown. It is interesting to see how other branches reacted after the fault. Since fault took place at branch 2-3 it is disconnected but due to this line other two lines are also removed from the system.

B. Results from phasor angle measurement algorithm:

Outage at bus 2-3:

TABLE I. PHASOR ANGLE MEASUREMENT RESULTS FOR OUTAGE AT BUS 2-3

	Bus 2 TO Bus 3 (MW)	Bus 2 TO Bus 4 (MW)	Bus 2 TO Bus 5 (MW)
Pre-Outage Flow (MW)	*68.272*	*44.9459*	*27.4206*
NAD	*0.05*	*0.026*	*0.027*

C. Results from alternating direction method for multipliers algorithm:

Outage at bus 2-3:

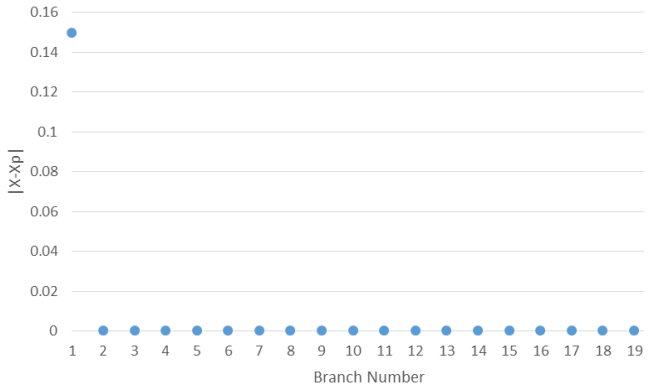

Fig. 11. Alternating direction method for multipliers results for outage at bus 2-3

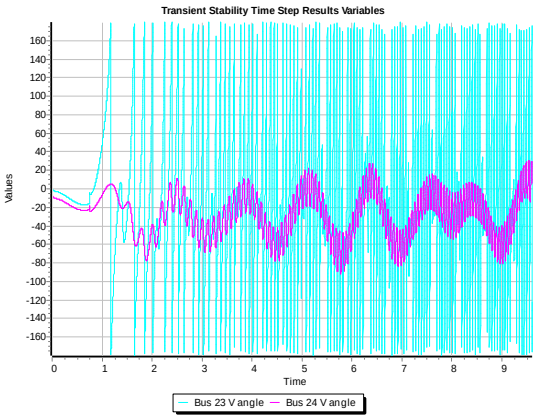

Fig. 13. Voltage angles at bus 23 and 24 after the fault

Now consider 39-bus network and apply outage at two different branches.

D. Outage at Bus 23-24

Now the fault occurred at branch 23-24 at 0.75 seconds, and outage has taken place across these lines. Power flow at nearby buses will also be affected after the fault occurred; there is a change in voltage angles and amplitude at nearby buses. PMUs, which are installed at different buses, are keeping the record of all these changes.

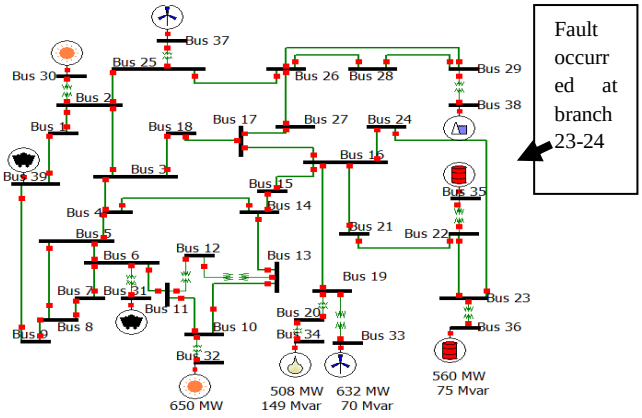

Fig. 12. Fault state at bus 23-24

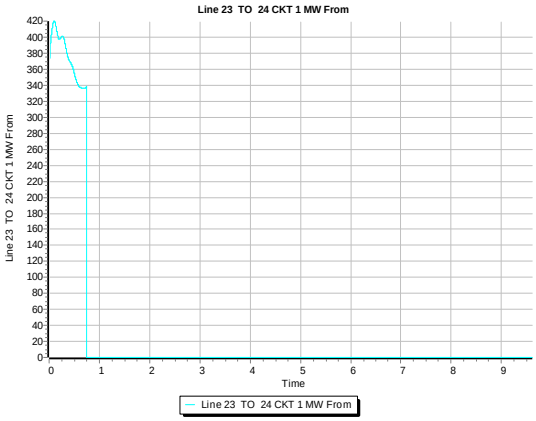

Fig. 14. Outage at bus 23-24

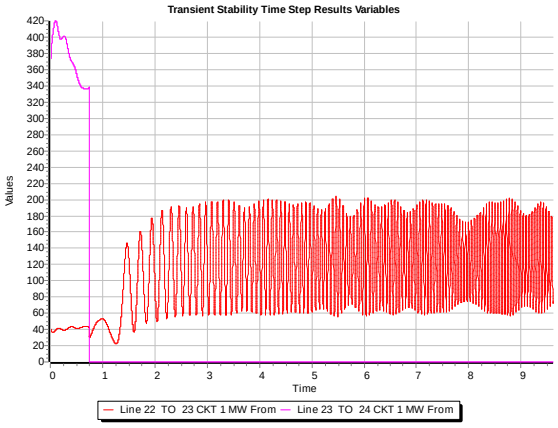

Fig. 15. Affected line due to outage at bus 23-24

E. Phasor Angle Measurement Algorithm Results

Outage at bus 23-24:

TABLE II. PHASOR ANGLE MEASUREMENT RESULTS FOR OUTAGE AT BUS 23-24

	Bus 23 to Bus 24 (MW)	Bus 22 to Bus 23 (MW)
Pre-Outage Flow (MW)	339	40
NAD	0.09	0.026

Fig. 16. Alternating direction method for multiplier results for outage at bus 23-24

When the phasor angle measurement algorithm is applied on a 39-bus system, different results have been obtained in comparison with a 14-bus system but still the outage branch can be detected. In table 12, normalized angle distance (NAD) values indicate the outage line in the system. In addition, it also shows the pre-outage values of the system before the outage occurred, which is nearly equal to the values we have from Powerworld simulations.

Fig. 16 shows the outage line when the distributed line change detection algorithm is applied. This algorithm identifies the branch number having an outage, and from the above fig. 11, the difference of |x-xp| clearly shows that branch 3 (bus 2-3) has an outage.

VI. CONCLUSION

Since SG is equipped with sensors such as PMUs to measure voltage and phase at different buses, these sensors provide continuous measurement of data across the power network. A small alteration in the measurement of phase and voltage at different buses could result in power system instability, so it is necessary to monitor PMU data closely. In order to secure SG from intruders, there is a need for CPS, which can ensure the accuracy of data from different PMUs. Different algorithms have already been designed to predict pre-outage flow and identify the correct outage line, but all these algorithms have some limitations. For example, some work for single line fault detection, while others only detect double line faults.

The aim of this study is to discover the best algorithm out of all the available algorithms designed by different researchers. Selection criteria for choosing any algorithm is that it should be less complex and require a smaller amount of time to process as there are algorithms that are very accurate but take a longer time for computation due to algorithm complexity.

PMU measurement based method is considered to be the most effective way to find line outage in the power system. Current PMU-based methods for line outage detection require information from internal and external network models of the whole power system to identify the line outages using PMU-based measurements. Single line outage detection using phasor angle measurements method is one of those methods used in this thesis for line outage detection, but it involves a long searching process to obtain information about the outage line, and it only

works for single line outage problems. However, the above method was improved [6] to detect double line outage as well, yet it still requires many more iterations to achieve the required result.

In another research named “Monitoring for Power-line Change and Outage Detection in SG via the Alternating Direction Method of Multipliers” [16] WAMS containing PMUs are deployed at various locations in the buses. PMUs are responsible for the measurement of phasor and voltage at the buses. PDCs are used at higher levels to collect data from PMUs in the defined region. After that, the method given in this paper for line outage detection is implemented, and these results will then be transmitted to WAMS to send the collected information to system operators. This method features low complexity distributed processing, which can enhance the efficiency, security and privacy level in SG monitoring.

Both algorithms have successfully identified the outage line for 14-bus and 39-bus systems, but line detection using the PMU data algorithm uses the internal-external network model for the whole interconnected system, in which the goal is to locate external line outages using only data within the internal system [5]. Single line outage detection using PMU data follows a complex searching process to find the outage line but it can only handle the single line outage scenario. In contrast, ADMM methods [16] are less complex compared to single line outage detection, which can increase the efficiency of security in SG monitoring.

References

[1] U.S. Department of Energy (DOE), 2007, A Systems View of the Modern Grid, National Energy Technology Laboratory (NETL).

[2] National Institute for Standards and Technology, Aug. 2010, NISTIR 7628: Guidelines for Smart Grid Cyber Security.

[3] Chen, P., Yang, S. and McCann, J. (2015). Distributed Real-Time Anomaly Detection in Networked Industrial Sensing Systems. IEEE Trans. Ind. Electron., 62(6), pp.3832-3842.

[4] Singh, C. and Sprintson, A. (2010). Reliability assurance of cyber-physical power systems. IEEE PES General Meeting.

[5] Tate, J. and Overbye, T. (2008). Line Outage Detection Using Phasor Angle Measurements. IEEE Trans. Power Syst., 23(4), pp.1644-1652.

[6] Tate, J. and Overbye, T. (2009). Double line outage detection using phasor angle measurements. 2009 IEEE Power & Energy Society General Meeting.

[7] Chertkov, M., Pan, F. and Stepanov, M. (2011). Predicting Failures in Power Grids: The Case of Static Overloads. IEEE Trans. Smart Grid, 2(1), pp.162-172.

[8] Cai, Y., Chow, M., Lu, W. and Li, L. (2010). Statistical Feature Selection From Massive Data in Distribution Fault Diagnosis. IEEE Trans. Power Syst., 25(2), pp.642-648.

[9] Calderaro, V., Hadjicostis, C., Piccolo, A. and Siano, P. (2011). Failure Identification in Smart Grids Based on Petri Net Modeling. IEEE Trans. Ind. Electron., 58(10), pp.4613-4623.

[10] Ruiz-Reyes, N., Vera-Candeas, P. and Jurado, F. (2005). Discrimination Between Transient Voltage Stability and Voltage Sag Using Damped Sinusoids-Based Transient Modeling. IEEE Transactions on Power Delivery, 20(4), pp.2644-2650.

[11] Gao, W. and Ning, J. (2011). Wavelet-Based Disturbance Analysis for Power System Wide-Area Monitoring. IEEE Trans. Smart Grid, 2(1), pp.121-130.

[12] Ning, J., Wang, J., Gao, W. and Liu, C. (2011). A Wavelet-Based Data Compression Technique for Smart Grid. IEEE Trans. Smart Grid, 2(1), pp.212-218.

[13] Jiang, H., Zhang, J., Gao, W. and Wu, Z. (2014). Fault Detection, Identification, and Location in Smart Grid Based on Data-Driven Computational Methods. IEEE Trans. Smart Grid, 5(6), pp.2947-

[14] He, M. and Zhang, J. (2010). Fault Detection and Localization in Smart Grid: A Probabilistic Dependence Graph Approach. 2010 First IEEE International Conference on Smart Grid Communications.

[15] He, M. and Zhang, J. (2011). A Dependency Graph Approach for Fault Detection and Localization towards Secure Smart Grid. IEEE Trans. Smart Grid, 2(2), pp.342-351.

[16] Zhao, Liang, Wen-Zhan Song, Lang Tong, and Yuan Wu. (2014) "Monitoring for Power-Line Change and Outage Detection in Smart Grid via the Alternating Direction Method of Multipliers", 28th International Conference on Advanced Information Networking and Applications Workshops, 2014.

He, M. and Zhang, J. (2011). A Dependency Graph Approach for Fault Detection and Localization towards Secure Smart Grid. IEEE Trans. Smart Grid, 2(2), pp.342-351.

Zhao, Liang, Wen-Zhan Song, Lang Tong, and Yuan Wu. (2014) "Monitoring for Power-Line Change and Outage Detection in Smart Grid via the Alternating Direction Method of Multipliers", 28th International Conference on Advanced Information Networking and Applications Workshops, 2014.

REFERENCES

1. New.abb.com, (2015). Why smart grids | ABB. [online] Available at: http://new.abb.com/smartgrids/why-smart-grids [Accessed 10 Nov. 2015].
2. A Systems View of the Modern Grid, National Energy Technology Laboratory (NETL), U.S. Department of Energy (DOE), 2007, (2015).
3. NISTIR 7628: Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology, Aug. 2010, (2015).
4. https://www.csiac.org/journal_article/efficacy-and-challenges-scada-and-smart-grid-integration, (2015). [image].
5. Chen, P., Yang, S. and McCann, J. (2015). Distributed Real-Time Anomaly Detection in Networked Industrial Sensing Systems. *IEEE Trans. Ind. Electron.*, 62(6), pp.3832-3842.
6. Singh, C. and Sprintson, A. (2010). Reliability assurance of cyber-physical power systems. *IEEE PES General Meeting*.
7. Tate, J. and Overbye, T. (2008). Line Outage Detection Using Phasor Angle Measurements. *IEEE Trans. Power Syst.*, 23(4), pp.1644-1652.
8. Tate, J. and Overbye, T. (2009). Double line outage detection using phasor angle measurements. *2009 IEEE Power & Energy Society General Meeting*.
9. Chertkov, M., Pan, F. and Stepanov, M. (2011). Predicting Failures in Power Grids: The Case of Static Overloads. *IEEE Trans. Smart Grid*, 2(1), pp.162-172.
10. Cai, Y., Chow, M., Lu, W. and Li, L. (2010). Statistical Feature Selection From Massive Data in Distribution Fault Diagnosis. *IEEE Trans. Power Syst.*, 25(2), pp.642-648.
11. Calderaro, V., Hadjicostis, C., Piccolo, A. and Siano, P. (2011). Failure Identification in Smart Grids Based on Petri Net Modeling. *IEEE Trans. Ind. Electron.*, 58(10), pp.4613-4623.
12. Ruiz-Reyes, N., Vera-Candeas, P. and Jurado, F. (2005). Discrimination Between Transient Voltage Stability and Voltage Sag Using Damped Sinusoids-Based Transient Modeling. *IEEE Transactions on Power Delivery*, 20(4), pp.2644-2650.
13. He, M. and Zhang, J. (2010). Fault Detection and Localization in Smart Grid: A Probabilistic Dependence Graph Approach. *2010 First IEEE International Conference on Smart Grid Communications*.

14. He, M. and Zhang, J. (2011). A Dependency Graph Approach for Fault Detection and Localization Towards Secure Smart Grid. *IEEE Trans. Smart Grid*, 2(2), pp.342-351.
15. Gao, W. and Ning, J. (2011). Wavelet-Based Disturbance Analysis for Power System Wide-Area Monitoring. *IEEE Trans. Smart Grid*, 2(1), pp.121-130.
16. Ning, J., Wang, J., Gao, W. and Liu, C. (2011). A Wavelet-Based Data Compression Technique for Smart Grid. *IEEE Trans. Smart Grid*, 2(1), pp.212-218.
17. Jiang, H., Zhang, J., Gao, W. and Wu, Z. (2014). Fault Detection, Identification, and Location in Smart Grid Based on Data-Driven Computational Methods. *IEEE Trans. Smart Grid*, 5(6), pp.2947-2956.
18. Zhao, Liang, Wen-Zhan Song, Lang Tong, and Yuan Wu. "Monitoring for Power-Line Change and Outage Detection in Smart Grid via the Alternating Direction Method of Multipliers", 2014 28th International Conference on Advanced Information Networking and Applications Workshops, 2014.
19. smart-grid tech (2012). *Smart grid vision*. [image] Available at: https://smartgridtech.files.wordpress.com/2012/05/sg-nature.jpg [Accessed 16 Apr. 2016].
20. Nature.com (2012). *Overview of smart grid architecture*. [image] Available at: Nature, “Overview of the smart grid architecture,” http://www.nature.com/nature/journal/v499/n7457/images/499145a-i2.0.jpg [Accessed 16 Apr. 2016].
21. MDPI-Journal0of-Applied science (2012). *Power flow layer*. [image] Available at: http://www.mdpi.com/applsci/applsci-0500706/article_deploy/html/images/applsci-05-00706-g001-1024.png [Accessed 16 Apr. 2016].
22. Dovepress (2013). *Cyber Infrastructure*. [image] Available at: https://www.dovepress.com/cr_data/article_fulltext/s48000/48124/img/fig4.jpg [Accessed 16 Apr. 2016].
23. GE-Grid-Solutions (2012). *Substation Automation*. [image] Available at: http://www.gegridsolutions.com/images/Automation/Application.jpg [Accessed 16 Apr. 2016].
24. Uluski, R. (2015). *Typical Distribution Automation System*. [image] Available at: http://www.elp.com/content/dam/pg/print-articles/2013/06/uluski01-1306pg.jpg [Accessed 16 Apr. 2016].
25. Media.Licdn (2012). *Advanced Metering Infrastructure Systems*. [image] Available at: https://media.licdn.com/mpr/mpr/p/7/005/0a8/13d/3695233.jpg [Accessed 16 Apr. 2016].

26. Xanthus-Consulting (2013). *Cyber Security Objectives Requirement*. [image] Available at: http://xanthus consulting.com/images/Security_Requirements.jpg [Accessed 16 Apr. 2016].
27. LinkedinLearning (2012). *Smart Grid And Security*. [image] Available at: 27. http://image.slidesharecdn.com/securingindustrialandsmartgriddevicesinaconnectedworldwebinarfinal-121030154014-phpapp02/95/securing-industrial-and-smart-grid-devices-in-a-connected-world-webinar-final-10-638.jpg?cb=1351611735 [Accessed 16 Apr. 2016].
28. University of Arizona (2014). *Challenges for Smart Grid*. [image] Available at: http://sgc2013.arizona.edu/images/smart_grid_1_v1.jpg [Accessed 16 Apr. 2016].
29. LaMonica, M. (2014). *Smart Grid Model*. [image] Available at: https://www.cnet.com/news/utilities-try-to-get-smarter-about-selling-smart-grid/ [Accessed 16 Apr. 2016].
30. LBx Journal (2013). *Smart Grid Model*. [image] Available at: http://www.lbxjournal.com/files/u12/figure1_PSG.jpg [Accessed 16 Apr. 2016].
31. Powercybersec.ece.iastate.edu. (2016). *PowerCyber Labs - Iowa State University*. [online] Available at: http://powercybersec.ece.iastate.edu/powercyber/powersystems.php [Accessed 8 Sep. 2016].
32. Hicks, C. (2012). *THE SMART GRID*. Where We Are Today and What the Future Holds. [online] ERB Institute -University of Michigan. Available at: http://erblegacy.snre.umich.edu/Research/InstituteReports/11-12/Hicks-Smart-Grid.pdf [Accessed 8 Sep. 2016].
33. Icseg.iti.illinois.edu. (2013). *IEEE 14-Bus System - Illinois Center for a Smarter Electric Grid (ICSEG)*. [online] Available at: http://icseg.iti.illinois.edu/ieee-14-bus-system/ [Accessed 4 Nov. 2016].
34. Wang, W. and Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, [online] 57(5), pp.1344-1371. Available at: https://research.ece.ncsu.edu/netwis/papers/12WL-COMNET.pdf [Accessed 4 Nov. 2016].
35. Jiang, H., Zhang, J., Gao, W. and Wu, Z. (2014). Fault Detection, Identification, and Location in Smart Grid Based on Data-Driven Computational Methods. *IEEE Transactions on Smart Grid*, [online] 5(6), pp.2947-2956. Available at: http://ieeexplore.ieee.org/document/6850055/ [Accessed 5 Nov. 2016].

References

36. Sridhar, S., Hahn, A. and Govindarasu, M. (2012). Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, 100(1), pp.210-224.
37. Razmi, H., Shayanfar, H. and Teshnehlab, M. (2012). Steady state voltage stability with AVR voltage constraints. *International Journal of Electrical Power & Energy Systems*, [online] 43(1), pp.650-659. Available at: http://www.sciencedirect.com/science/journal/01420615/43?sdc=1.
38. Shah, Y. (n.d.). *Energy and fuel systems integration*. CRC Press 2015, pp.353–410.
39. F. Blaabjorg. "Probabilistic capacity of a grid-connected wind farm", 32nd Annual Conference of IEEE Industrial Electronics Society 2005 IECON 2005, 2005
40. Yan, Guangwei, and Peipei Wu. "Robust Data Transmission upon Compressive Sensing for Smart Grid", Electric Power Components and Systems, 2014
41. Xu, Wilson, and Julio Garc√≠a-Mayordomo. "Three-Phase Power Flow and Harmonic Analysis" , Electric Power Engineering Series, 2008.
42. Zhao, Liang, and Wen-Zhan Song. "Distributed Power-Line Outage Detection Based on Wide Area Measurement System", Sensors, 2014.
43. Mirzaei, Maryam, Jasronita Jasni, Hashim Hizam, Noor Izzri Abdul Wahab, and Ehsan Moazami. "Static voltage stability analysis using generalized regression neural network", 2013 IEEE 7th International Power Engineering and Optimization Conference (PEOCO), 2013.
44. "2011 Index IEEE Transactions on Smart Grid Vol. 2", IEEE Transactions on Smart Grid, 2011.
45. López, Gregorio, Pedro Moura, José Moreno, and José Camacho. "Multi-Faceted Assessment of a Wireless Communications Infrastructure for the Green Neighborhoods of the Smart Grid", Energies, 2014.
46. Bolognani, Saverio, Ruggero Carli, Guido Cavraro, and Sandro Zampieri. "A distributed control strategy for optimal reactive power flow with power constraints", 52nd IEEE Conference on Decision and Control, 2013.
47. "Advances in Neural Networks – ISNN 2009", Springer Nature, 2009
48. Cavraro, Guido, Ruggero Carli, and Sandro Zampieri. "A distributed control algorithm for the minimization of the power generation cost in smart micro-grid", 53rd IEEE Conference on Decision and Control, 2014.
49. Haidar, A.M.A.. "Transient stability evaluation of electrical power system using generalized regression neural networks" , Applied Soft Computing Journal, 201106

References

50. Jaya Bharata Reddy, M., D. Venkata Rajesh, and D.K. Mohanta. "Robust transmission line fault classification using wavelet multiresolution analysis", Computers & Electrical Engineering, 2013.
51. Ho, Quang-Dung, and Tho Le-Ngoc. "Smart Grid Communications Networks: Wireless Technologies, Protocols, Issues, and Standards", Handbook of Green Information and Communication Systems, 2013.
52. Xie, Jing, Chen-Ching Liu, Marino Sforna, Martin Bilek, and Radek Hamza. "Threat assessment and response for physical security of power substations", IEEE PES Innovative Smart Grid Technologies Europe, 2014.
53. Rana, Md, and Li Li. "An Overview of Distributed Microgrid State Estimation and Control for Smart Grids", Sensors, 2015.
54. Fang, Xi, Satyajayant Misra, Guoliang Xue, and Dejun Yang. "Smart Grid — The New and Improved Power Grid: A Survey", IEEE Communications Surveys & Tutorials, 2011.
55. Cavraro, G., R. Arghandeh, G. Barchi, and A. von Meier. "Distribution network topology detection with time-series measurements", 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015.
56. ITOH, MAKOTO, and LEON O. CHUA. "DUALITY OF MEMRISTOR CIRCUITS", International Journal of Bifurcation and Chaos, 2013.
57. Cavraro, G. (2013). *Smart Grid distribution model*. [image] Available at: http://automatica.dei.unipd.it/tl_files/pubblicazioni/PhDThesis/CavraroGuido_PhD_presentation.pdf [Accessed 16 Sep. 2016].