ANALYSIS OF CYBER SECURITY IN SMART GRID SYSTEMS

by

James Masonganye

Submitted in partial fulfilment of the requirements for the degree
Master of Engineering (Electronic Engineering)

in the

Department of Electrical, Electronic and Computer Engineering
Faculty of Engineering, Built Environment and Information Technology

UNIVERSITY OF PRETORIA

June 2017

SUMMARY

ANALYSIS OF CYBER SECURITY IN SMART GRID SYSTEMS

by

James Masonganye

Supervisor: Prof. G.P. Hancke

Department: Electrical, Electronic and Computer Engineering

University: University of Pretoria

Degree: Master of Engineering (Electronic Engineering)

Keywords: Cyber Security, smart grid, SCADA, National Institute of Standard (NIST)

Cyber security is a major concern due to global incidents of intrusion. The impact of the attacks on the electricity grid can be significant, resulting in the collapsing of the national economy. Electricity network is needed by banks, government security agencies, hospitals and telecommunication operators.

The purpose of this research is to investigate the various types of cyber security threats, including ICT technologies required for safe operation of the smart grid to protect and mitigate the impact of cyber security. The modelling of cyber security using the Matlab/SimPowerSystem simulates the City of Tshwane power system. Eskom components used to produce energy, interconnect to the City of Tshwane power distribution substations and simulated using Simulink SimPowerSystem.

DECLARATION

I declare that this dissertation is my own work. The dissertation is being submitted as partial fulfilment of the requirements of the Master degree in Electronic Engineering at the Department of Electrical, Electronic and Computer Engineering, University of Pretoria. It has not been submitted before for any degree or examination in any other University.

James Masonganye

June 2017

ACKNOWLEDGEMENTS

I would like to extend my sincere gratitude to the following individuals:

- To my supervisor Prof. G P Hancke, for his support, encouragement and guidance on this dissertation. I am exceptionally thankful for his assistance for constantly providing technical guidance.

- My son James Junior Vutlhari Masonganye, and my daughter Mikateko Masonganye for their support and understanding throughout my research. They have given me strength whenever I needed it.

- To all my friends and family for their understanding and motivation.

- To my editor, Ms Liza Marx from APES (Academic and Professional Editing Services) for copy-editing, proofreading and formatting my dissertation.

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
APES	Academic and Professional Editing Services
CB	Circuit Breaker
CIKR	Critical Infrastructure and Key Resources
CoT	City of Tshwane
DoS	Denial of Service
ELC	Expected Load Curtailment
EMS	Energy Management Systems
EPRI	Electric Power Research Institute
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GOOSE	Generic Object-Oriented Substation Events
HDSL	High Bit Rate Digital Subscriber Line
HMI	Human Machine Interface
HV	High-voltage
ICT	Information Communication Technology
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IP	Internet Protocol
ISGT	Innovative smart grid Technologies
LAA	Load Altering Attacks
LAN	Local Area Network

MVAr	Mega Volts Amps (Reactive)
NAT	Network Address Translation
NERC	North American Electricity Corporation
NIST	National Institute of Standard
PDC	Phase data concentrator
PMU	Phasor Measurement Unit
RTU	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SFCL	Superconducting Fault Current Limiter
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	Service Oriented Architecture
TLS	Transport Layer Security
AC	Alternating Current
ARP	Address Resolution Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server
DSL	Digital Subscriber Line
DSO	Digital Subscriber 0
EOC	Embedded Operations Channel
FEP	Front End Processor
HOR	Type HCB Pilot Wire Relaying System
MAC	Medium Access Control
UNEM	Universal Network Manager

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 PROBLEM STATEMENT

1.1.1 Context of the problem

This research focuses on identifying an inclusive physical smart grid cyber security challenge and security needs at multiple levels of the electric power grid with specific focus on Advanced Metering Infrastructure (AMI) security. The topic will further identify the role of cyber security research, going beyond the traditional information technology security environment. The Phase 1 implementation of the City of Tshwane AMI programme forms the basis of this research. Applying cyber security through a combination of analytical and simulation tools on a "live" AMI infrastructure, (like the one at the City of Tshwane), will evaluate the effectiveness of risk mitigation under the sophisticated smart grid physical cyber-attack scenario.

The rollout of AMI or smart grid systems, also globally, is a new technology with limited application in South Africa. An increasing use of information communication technology based electrical reticulation networks though, increases cyber security weaknesses, influencing the smart grid cyber-attacks. This research will discuss smart grid security, including areas of vulnerability, cyber assets protection, the layered approach to security, data management and privacy concerns.

The economy and the environment require substantial changes, ensuring the efficient operation of the smart grid system. Companies globally, continue modernising their power

systems [1]. The modernisation of the electric grid will ensure reliability, stability and manageability of the power system, providing interruptible power supply to the end users. The power system security in the smart grid remains a challenge, as the system is susceptible to hacking of the computer systems, as technology is deployed and the grid modernised. Hackers can access the utility computer network from the electrical substation local area network environment.

The research represents the work in progress towards the reduction and prevention of cyber-attacks on the smart grid system.

The dissertation investigates modelling the interaction of cyber security and smart grid, using the Matlab/Simulink tool. Matlab/Simulink demonstrates how a cyber-attack will result in electrical power network disruption.

1.1.2 Research gap

The research gaps that should be attended to in conclusion of the study, is to combine the co-simulation of the power system and telecommunications network devices. The task is difficult as the models should integrate.

Various SCADA installations globally, were victims of cyber-attacks. The most prominent attack launched on the SCADA system was in July 2010. The *Stuxnet* worm malware attacked a Siemens SCADA, Microsoft windows operating system, with programmable logic controllers [2]. The scope of this dissertation is to study the impact of cyber-attacks on smart grid systems and simulate the behaviour of the grid when exposed to various attacks.

1.2 RESEARCH OBJECTIVE AND QUESTIONS

Wireless networks based on IEEE 802.11 and GSM standards are one of the key communication technologies used to realise smart grid networks, and they can be easily

manipulated by intruders to launch a DoS attack by attacking a smart grid network. The wireless networks are susceptible to jamming by the intruders due to their openness and non-security [3]. To countermeasure the influence of the denial of service attacks, proper design of the network is required for the grid to be more resilient. Designing an effective counter measure, play a critical role to countermeasure the impact of the denial service attacks.

- How a cyber-attack launched on smart grid can disrupt a power delivery?
- How cyber-attack expected load reduction is simulated using SimPowerSystems?
- What are the impacts of DoS attacks on smart grid Infrastructure networks?

1.3 APPROACH

The research aims to assist smart grid operators to improve cyber security and to introduce more resilience in the infrastructure, with a set of minimum-security measures. The outcome will be, gaining more knowledge on cyber security in smart grid to eliminate DoS and other threats by cryptographic methods.

The research approach is based on implementing the SimPowerSystems in a real-time simulation environment. The simulation will enable the interaction with real-time Matlab library components inter-connected, forming a smart grid system. The combination of the Matlab Simulink package and mathematical models will be used to simulate the cyber-attacks. From a technical point of view of the operating power grid system in reality, the time time-domain analysis capabilities are the initial requirement. The Matlab SimPowerSystems program will be used for its simplicity and it is easy to assemble the model [4]. The approach will be to execute the Simulink models from the Matlab environment in real-time.

To achieve the objectives of this study, the following approach will be followed:

- A desktop research on standards and practices related to cyber security.
- A detailed research in governmental agencies and academic institutions providing information regarding defence against cyber threats.

- Read findings from an expert group on the security of communication networks for smart grids.
- The Simulink models will be executed in real-time using the Matlab package.
- SimPowerSystem will be used to perform dynamic analysis of electric power system.
- A scenario will be implemented in which the assailant increased the load on an electrical grid and an attack will be initiated through the communication network. The attack will be similar to the DoS attack and once started, it will damage the electrical grid.
- The City of Tshwane AMI programme will be used as a case study and Matlab Simulink models will be used as a test bed for the smart grid cyber security study and the lesson learned applied in this research.
- Document and report on the communication infrastructure used by the City of Tshwane and running the simulation using network monitoring tools on the Tshwane smart grid infrastructure.

1.4 RESEARCH GOALS

The main goal of this research is to analyse and simulate the impact of cyber-attacks, using Simulink SimPowerSystems. The threats, vulnerabilities and cyber-attack security challenges will be analysed. Subsequent paragraphs provide the load points in Mega Watts (MW), measurements from various substations, addressing the controls, to mitigate the risks posed by cyber-attacks and countermeasures. Best standard practices will be suggested, applicable to the industry. Matlab simulation of the cyber-attacks will need to be addressed to assist in solving these challenges.

1.5 RESEARCH CONTRIBUTION

The research provides a practical overview of smart grid cyber security in the power system environment. Launching a DoS in the power system can be achieved by hacking the electricity communication data protection and communication network. Groups such as the National Institute of Standard (NIST) dealing with cyber security are responsible for

implementing the cyber security standard in smart grid. The NIST research, IEEE journals and magazines, indicates that numerous cyber security issues need to be addressed in smart grid.

During the deployment of the City of Tshwane AMI infrastructure, the system required adhering to the security requirement of the CoT prior to the system deployed in the environment.

The research comprises these sections:

Chapter 1 describes the problem statement, including the research methodology used to achieve the study outcomes. The status quo concerning the network being studied, is also described in Chapter 1. An overview of the electricity protection network and the intelligent protection relays in the electricity data protection network, is also described. Each network component and the system parameters are specified.

In using a network with various components in the substations, the cyber-attack is stimulated, indicating how a failure in a device, such as opening and closing of a circuit break can result in load reduction. This technique in simulating a cyber-attack, results in the collapse of the power grid.

Chapter 2 discusses the literature study with case studies and security threats for the smart grid system. The section provides the description of how the smart grid can be initiated by the intruder into the power grid or distribution network. Some of the grid entry points are described, such as substation LAN posing risks of possible cyber-attacks.

Chapter 3 indicates how the system responds to various attack scenarios. Various cyber-attacks scenarios are validated, using SimPowerSystems modules to measure voltages and currents. The results of the simulation signals passing through the block built in SimPowerSystem, resemble the power grid cyber-attacks.

.

Chapter 4 discusses the summary of the simulation results of the power grid network, affected by the variation of the substation transformer frequency for both primary and in-feed substations. The insight of the security architecture required is described, to implement a secured remote access of the SCADA.

Chapter 5 provides an overview of the work and the relevance of this study to the cyber-attacks occurring in other parts of the world.

Chapter 6 provides proposals for further research in the similar field. The research concludes with a list of references.

1.5.1 DNP Protocol SCADA system implementation in the City of Tshwane

The City of Tshwane SCADA front-interface, devises a version of DNP3 Level 3 (L3) implemented by Siemens. The version of the SCADA system is spectrum power 3 (operating as a master). It is normal practice globally to connect a master with DNP L3 to n slave with DNP L2 or even to L1. In the City of Tshwane's case, the protocol changes when the FEP is implemented.

Access to the spectrum power services are offered under the existing service level agreement with Siemens. The condition of this agreement is that the hardware and software installation of a VPN (ISDN or DSL) is performed by the City of Tshwane. Siemens engineers provide remote support through the VPN (ISDN or DSL) router.

The VPN (ISDN or DSL) connection with local providers and the LAN connection to the network control system, is the responsibility of the City of Tshwane. It is possible for an experienced hacker, to alter the parameters of the sensing SCADA devices, if tight security mechanisms are not implemented on the system. Password control is therefore highly secured and connection is not utilised for any additional connection, for security reasons.

Writing any values to the system, can result in the amendment of the data sets [5] - [6]. The assailant can access the PowerMap server in the control centre to retrieve data and grid plans from the server database. By retrieving the substations line diagram from the PowerMap server, the hacker can study the diagrams and intelligently hack into the SCADA sensors or related instruments interfacing with the utility communication networks. The effective authentication and encryption of the utility grid plans is described in [7], its criticality is confirmed in the risk based analysis of the study.

Remote opening of a Circuit Breaker (CB) for the substations feeding critical supply load within the grid by using SCADA HMI, causes load shedding at that supply point or the grid

network. The results of this research indicate that by simulating such an attack in Matlab, the substation can trip, resulting in a total loss of power supply. It is also possible to log into the substation LAN environment and switch the relays “OFF” or “ON”. Most relays comply with IEC61850 standards enabling remote access.

IEC61850 relays deployed by the Electricity Department of the City of Tshwane, are the next generation of relays for substation communication networks. The intelligent relays are used for the reliability of the substation protection system. As indicated in Figure 1.1, most of the electricity IED relays are intelligent. The security protocol including rules should always be adhered to when working on these devices. The relays are designed to operate in the optical fibre communication medium, allowing fast substation tripping and clearing of faults in the grid network. Maintenance and remote settings of relays is possible, assisting engineers performing this function without visiting the substations.

1.5.2 Advantages of RED670 IEC618050 relays

The main advantages of the intelligent RED670 relays compared to traditional copper based relays are:

- The communication of the 615 multiplexers provides redundancy in the event of link failure.
- Data communication is continuously monitored with alarms.
- When one feeder cable fails due to a cable feeder fault, the zone protection is activated, isolating the faulty cable instead of tripping the entire substation.
- Relays are equipped with recorders for analysis, done remotely.
- The system is integrated to the SCADA for remote operation.
- Settings and programming of relays are done remotely.

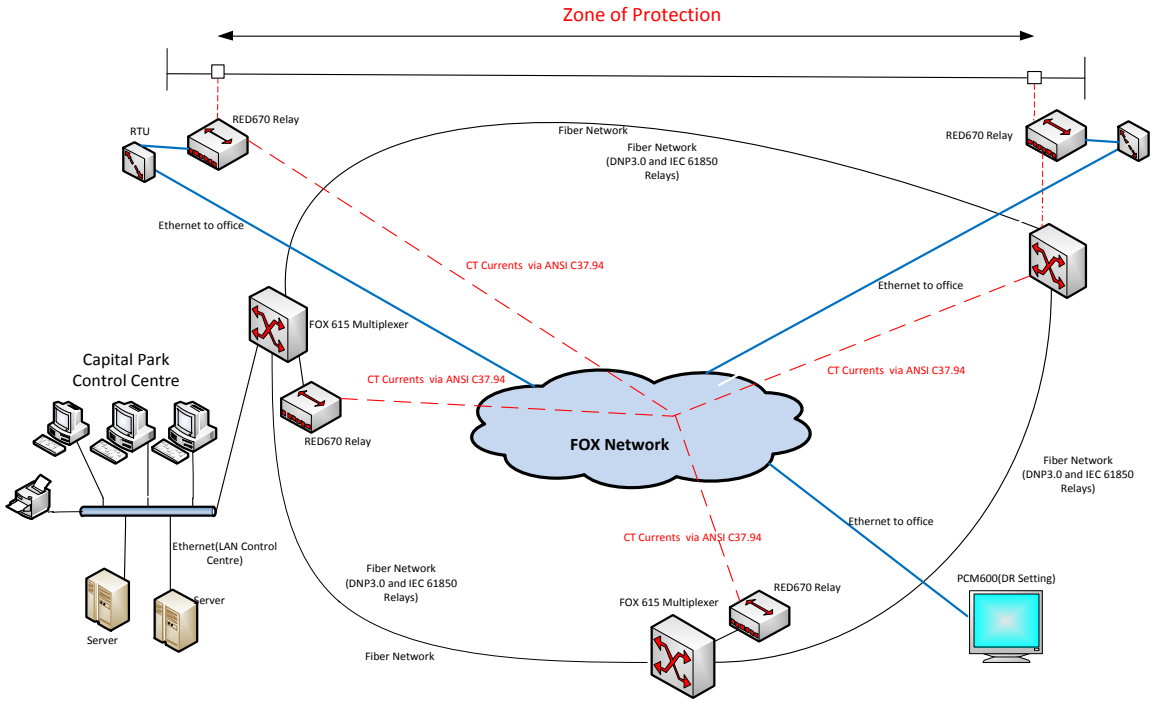

Figure 1.1. IEC 61850 substation LAN RED 670 relays

In Figure 1.1, the RTU communicates through the data protection FOX based SDH network, using the IEC61850 protocol with the RED670 intelligent relays. The transmission medium is fibre optic cable. The information on tripping, link status, currents and CB status is available in the PCM600 disturbance recordings for the team responsible for protection network monitoring the network status. The above information is available to the control centre team at Capital Park, using the DNP3.0 protocol through the FOX to FOX network. The optical Ethernet port is available to interconnect with multiplexer for communication with the fox network.

The equipment is mounted in the substation switchgear inside the substations. The remote settings and uploading of the disturbance recordings from the RED670 relays is done from the central location. Section 4.3 defines the description, architectural design; including configuration of the system against cyber-attacks. The combined test bed simulation implementation of the diagram in Figure 1.1 is beyond the scope of this work. The construction of the communication and power system simulation tools is an expensive and

time-consuming exercise. Cyber-Attack analysis is simulated in Matlab/Simulink and the simulation results indicate the method of destroying the power system.

1.6 RESEARCH OUTPUTS

Table 1.0 (Appendix A), lists research outputs published in international journals, web access and conferences, used to conduct the research.

1.7 OVERVIEW OF STUDY

The chapter provides an overview of the study network. The research comprises the background and theoretical perspective of the smart grid system. It also presents an overview of simulation of the power system, using Matlab/SimPowerSystems. The City of Tshwane power system is modelled as a smart grid system, using Matlab/Simulink.

Eskom supply the City of Tshwane with electricity. The city is one of Eskom's largest consumer of electricity in South Africa. Four in-feed supply points from Eskom to Tshwane exist. These are Kwagga, Njala, Rietvlei and Buffel stations. The sub-transmission network from Njala in-feed power station is used for the research. Control, monitoring and supervision of the City of Tshwane electrical network occurs remotely from a central location at the Capital Park network control centre depot.

The City of Tshwane Electricity network comprises various substation configurations. The most prominent substation configuration in the City of Tshwane network, is known as the redundant ring transformer configuration, recognised for its redundant line feeders for back-feeding consumers in the event of faulty feeders, ensuring continuous electricity supply. The Njala supply line was chosen in this research for simulation, using Matlab/SimPowerSystem. For simulation purposes, it is assumed that in the event of faults in the network, there is no high-voltage (HV) separation point to isolate the substation in case a feeder fault or transformer fault occurs in the network.

The substation load points included in the simulation model are indicated in Table 1.1.

Table 1.1. City of Tshwane electricity substation load points

Substation(s)	**Load(MW)**	**Transformer (MVA)**
Njala	700 MW	4 x 250 MVA
Wingate	49.6 MW	5 x 35 MVA
Watloo	49.6 MW	6 x 35 MVA
Wapadrand	38.6 MW	4 x 35 MVA
Mamelodi 1	57.8 MW	4 x 35 MVA

In designing the smart grid network, the substation loads measured in MW (from Table 1.1) were input to the model in Figure 1.2. The following assumptions were made in the design and simulation of the model:

- The machine-initiated generator represents the Kendal Eskom generation power station.
- Power to the City of Tshwane's five substations are supplied by the Eskom generation substation.
- The electricity data protection communication network integrates into the SimPowerSystems model.
- The ABB FOX to FOX multiplexers, RED670 IED relays are incorporated into the model.
- Monitoring and control of the model are coordinated from the Capital Park network control centre.

An underlying reason for the assumption made above is because no software is available to simulate both the power system and the communication network simultaneously [8].

The SimPowerSystems tools do not include libraries or tools required for the advanced smart grid systems.

In this simulation, the Eskom Kendal power generation station is used to power up all the substations through the 400KV line to the City of Tshwane Njala in-feed substation. The 132KV substations are energised from Njala in-feed where the voltage is stepped down from 400KV to 275KV. The total power black-out on the network is initiated by opening the circuit breaker CB1, CB2 and CB3 are resulting with the disruption or shutdown of the power supply.

The remote SCADA HMI control centre at Capital Park receives tripping information through the FOX communication network. The cyber-attack is launched when the intruder accesses the electricity communication network, and the commands reaches the Remote Terminal Units (RTU) and IED devices that will transmit to the actuators.

The Matlab simulation file depicting the smart grid model was designed using Matlab release R2015b. Figure 1.2 indicates the configuration of the network. The substations load points were drawn using the blocks from the SimPowerSystem library. The sub-transmission network is inter-connected with the distribution line parameters. The MatlabR2015b simulation results are shown in Figure 3.1 to Figure 3.9 and the load current represented responses to cyber-attacks. Figure 3.3 shows that initiating a cyber-attack by opening all the CB's, results with the straight-line load current, showing "zero" or no current flowing into the grid.

1.7.1 Simulation methodology of the normal operation of the grid under no cyber-attack is described

- Kendal power station on full load.
- Supply auxiliaries to Eskom Kendal Unit 1.
- Energise the Kendal 400KV line to Njala.
- All CBs CB1, CB2 and CB3 closed.
- Pick up City of Tshwane substation load through Njala in-feed substation.
- All substation transformer frequencies set at 50 Hz.

The above steps indicate that the power system operates under normal conditions without intruders attacking the grid. The simulation results of the network operating without being cyber-attack (when the CB1 is closed) is indicated in Figure 3.7.

The simulation above can be applied in the steps described in [9], of the study of security analysis considering cascading outages. The simulation steps are as follows:

- Initialisation: The power system is initialised to N-1 secure with an AC load flow calculated under specific operating conditions.
- N-K contingency application: K represents the electrical components failing to operate in the transmission network. This is also referred to as branched outages.
- Power System Security Estimation: This occurs when the transmission network operates in an insecure grid status, due to voltage collapse and load imbalance. The system bus voltage needs to be maintained to operate in a specific range.

Comparing the similarities of the Monte Carlo simulation used in the above steps with the Simulink SimPowerSystems simulation in this work, it is shown that the approach in this study attains greater potential in practical application.

1.7.2 Methodology of the simulation steps after launching a cyber-attack

- Kendal Power Station on full load.
- Supply auxiliaries to Eskom Kendal Unit 1.
- Energise the Kendal 400KV line to Njala 275 KV.
- Circuit breaker CB1, CB2 or CB3 opened.
- Pick up City of Tshwane substation load through Njala in-feed substation.
- All substations transformer frequencies still set at 50 Hz.
- Pick up load by opening CB’s CB1, CB2 or CB3.
- Triggering of the above CB by opening.
- Current Iabc at load in Figure 3.9.

These steps indicate the load current after a cyber-attack, indicating how the system responds with the three-phase load current indicating the three-phase current at no load, a cyber-attack or no cyber-attack, respectively. The simulation result shows the CB triggering and changing the transformer frequency to model a cyber-attack.

1.7.3 Methodology of the simulation of cyber-attack by transformer frequency variation

- Kendal power station on full load.
- Supply auxiliaries to Eskom Kendal Unit 1.
- Energise the Kendal 400KV line to Njala 275 KV.
- Shut download by frequency variation.
- Pick up City of Tshwane substation load through Njala in-feed substation.
- All substation transformer frequencies set at 40 Hz.
- Pick up load by opening CB's CB1, CB2 or CB3.
- Triggering of the above CB by opening.
- Current Iabc at Load for BUS1 in Figure 4.4.

1.7.4 Power system outages resulting in cyber-attacks

The following paragraph provides the breakdown of power outages, resulting attacks on BUS 1, BUS 2 and BUS 3 of the model. The network is designed such that the system implementation in Figure 3.4 indicates three different buses. The in-feed substation at Njala 275 KV connects directly to BUS1. The substation load for the various primary substations are connected to the various buses with each BUS associated to each substation load as below. The dialogue box block in the model provides for entering the parameters, measuring current and voltage outputs at various substation load buses.

- Mooikloof 132 KV substation load point ~ 46 MW (BUS1)

Another assumption made in the type of the sub-transmission network supplying power to various 132 KV is using a radial sub-transmission network. To ensure the reliability factor, power from the 275 KV Njala to the 132 KV substations, uses two 132 KV pylon routes. Alternate supply is made in the event of the failure of the sub-transmission line. The monitoring of the three-phase voltages and current for BUS1 (B1) at Mooikloof is as follows:

- Voltage Measurement ~ “Phase to ground”.
- SetLabel IV_ “Vabc_B1”.
- Vpu _“On”.
- Current Measurement _ “Yes”.
- Ipu _ “On”.
- Powerbase _100e6.
- Vbase _132e3.

Wapadrand 132 KV substation Load point ~ 49.6 MW (BUS1)

Three-phase voltage and current load measurement for BUS1 (B1) at Wapadrand substation ~ 49.6 MW.

- Voltage Measurement ~ “Phase to ground”.
- SetLabel IV _“Vabc_B1”.
- Vpu _“On”.
- Current Measurement _ “Yes”.
- Ipu _ “On”.
- Powerbase _100e6.
- Vbase _132e3.

Watloo 132 KV substation Load point ~ 38.6 MW (BUS2)

Three-phase voltage and current load measurement for BS2 (B2) at Watloo substation ~ 38.6 MW.

- Voltage Measurement _ “Phase to ground”.
- SetLabel IV _ “Vabc_B2”.
- Vpu _ “On”.
- Current Measurement_ “Yes”.
- Ipu _ “On”.
- Powerbase _ 100e6.
- Vbase _132e3.

Mamelodi 1 132 KV substation load point ~ 57.8 MW (BUS3)

Three-phase voltage and current load measurement for BUS3 (B3) at Mamelodi 1 substation ~ 57.8 MW.

- Voltage Measurement _ “Phase to ground”.
- SetLabel IV _ “Vabc_B3”.
- Vpu _ “On”.
- Current Measurement _ “Yes”.
- Ipu _ “On”.
- Powerbase _ 100e6.
- Vbase _132e3.

The simulation results show the response of the system in the event of cyber-attack. Several load point simulations were performed, analysing and evaluating the system performance in response to the load shed by the grid after the cyber -attack. The voltage base for all the buses in the smart grid network is set at 132KV and a reference voltage of 132KV was used. The reference power base was set at 100e3MVA. The power of the Eskom Kendal generation power station was set at 700MVA. This is connected to the City of Tshwane grid. The

Matlab/Power system time step was set at 0.2 seconds to run the simulation. The frequency was set at 50 Hz to allow for the stable operation of the power system. The nominal frequency used in South Africa is 50Hz and all electricity from Eskom generation power stations to the national power grid including Municipalities is always set on 50Hz.

1.7.5 The City of Tshwane electricity data communication and protection network

The data protection network of the City of Tshwane is based on an optical fibre network. The network services the entire 132KV and more than 206 11KV electricity satellite substations. The central management of this network is remotely done with a UNEM/CST system operated from Electronic Services in Riviera, Pretoria. All stations are configured to report through an EOC channel connected through one of the sifox and X21 channels and SNMP through the Ethernet LAN portions of the network. Paragraph below provides the basis for applying the cyber-attack since the substation LAN can be used to launch a cyber-attack to the electricity grid if an intruder plugs a PC on a substation LAN environment.

1.7.6 Services using the network

The following specific services use this network:

- Emergency telephone services between the control centre at Capital Park and all the substations.
- SCADA system communication in the substations.
- This system is based on defined 64kbps data channels through SIFOX cards.

1.7.7 Network configuration

Revision and upgrade of portions of the network is required to improve the operation of the system and to provide the users with a modern extended data network. The critical links between the primary and secondary substations stations are provided with new optic fibre communication units with a maximum speed of STM-1 or 155Mbps and STM- 4 or

622Mbps. Communication between the primary and secondary substations are provided using copper pilot cables and the links are established with HDSL technology.

1.7.8 Network components

The following networking components are deployed on the network:

- Routers.
- Ethernet hubs and switches.

All networking components are compatible with the arrangement that is in use on the City of Tshwane's corporate IT department network. The routers are compatible with the existing Cisco system. All routers have fractional E1 WAN capacity with a 10/100 baseT Ethernet port. Two types of Ethernet switches are installed on the network.

1.7.9 Transmission network

The transmission network of the CoT is based on SDH transmission facilities. The network speeds are selected, providing the best possible service to the users. The main backbone rings are used to set up as many DS-0 channels as can be made available. The system commences with 20 channels combined into the fractional E1 links.

Each substation is provided with a local area network based on 10base –t Ethernet. Most applications that run on the network are installed as fixed applications, requiring communication from various offices to the respective suspension for load, quality and demand monitoring. Communication for the SCADA system runs from the electricity network control centre. All data connections between the corporate network and electricity network are routed through the firewall connection at Capital Park. An intruder can launch a cyber-attack by plugging into the LAN infrastructure at the substation.

Communication for the Micro-SCADA system occurs through network adapter cards. The network is available for communication and transfer of files between PC's plugged into the substation LANs and the main data system at the CR de WET building. Intruders can use a complex attack such as Main, in the middle attacks in the substation to tamper the information inside the LAN with ARP trusting protocol [10].

With ARP protocol, an attack is launched by sending an ARP reply to the protocol gateway SCADA HMI with a specific IP and MAC address. Unawareness of the protocol gateway will update the ARP cache table, paired between the SCADA HMI and protocol gateway address. The attacker impersonates the SCADA HMI for the protocol gateway to send IP packets to the HMI [11]. The attacker can use the intercepted information afterwards to launch severe attacks on the grid.

1.7.10 Network protocols

The protocol was designed to be compatible with the existing transmission system. The data communication equipment in conjunction with the transmission equipment ensures that all point–to point links are configured according to the following protocols:

- Data-link protocols: PPP, FRL, X-25.
- Network protocols; IP, IPX, SNA.
- Routing protocols: ICMP, SNMP, TCP, UDP, DNS, FTP, TFTP, RADIUS, TACARS, PAP, CHAP.

All protocols comply with the applicable standards issued by the IEEE, RFC and ITU.

1.7.11 Network interface

Two types of network interfaces are used between the routers and the FOX systems for the wide area network and fractional E1/T1 for the high-speed backbone. Initially the ports are set up for DSO channels. The interface is complete with the required DSU/CSU units. These units are supplied as part of the WAN card on the router, or as part of the interface card of the FOX system.

Serial interface, X-21/V.24, running at 64kbps, for interfacing to FOX6+ through N3BS cards and FOX U through SIFOX cards. The fox network is designed to transmit high capacity data networks, such as video surveillance for substation security. This can be achieved by deploying an interface card into the FOX system to carry video data and provide monitoring and security for the electricity substations.

Various network interfaces and can be used to segment the network traffic from each other, but using VLAN is not a permanent solution addressing cyber security attacks. Mitigation and measures should be implemented to address the vulnerabilities in the electricity smart grid.

1.8 DNP3 CHARACTERISTICS USED FOR THE CYBER SECURITY [12]

1.8.1 TCP/IP interface

In cyber security, the authentication and confidentiality of the network operation uses TLS and IPSec protocols. The assumption is that cyber security is only concerned with data transmission, even though network connections may seem legitimate to TLS and IPSec. The cyber-assailant can manipulate the destination device by changing the router IP address if the cyber security standard and protocol described in this study is not used. The altering of the substation operations may be compromised and cannot transmit the control commands.

The master only assesses the monitoring devices in the smart grid, network, and the nature of the security of the DNP3 SCADA protocol can be manipulated and attacked. The cyber security operations are not concerned with authentication or confidentiality since TLS or IPsec are used for the connection security. The cyber security therefore assumes that the connection is legitimate and is only concerned with the DNP3 data.

Although the connection may be legitimate to TLS or IPsec, the source device may have been compromised by a cyber-assailant allowing the cyber-assailant to manipulate the destination device if the cyber security in this study is not used. Without the cyber security proposed, a master (which typically only accesses monitoring data) may be compromised to transmit control commands, altering the substation operations.

1.8.2 Data-link layer protocol

The data-link layer header in the cyber security applies the following rules in implementing the protocol network:

- The system address.
- Data-link destination address.
- Data function.

The link status information between the substation devices in the data-link layer functional code can share information such as link commands. The reset link button on the devices restarts the devices in the event of a link failure between the FOX to FOX switches. This is a important feature used by technicians to troubleshoot a fault in link failure.

Although the UNEM management system is designed to monitor whether the link is down or up, certain instances occur where the SCADA services remain off-line even though the FOX system reported otherwise. This is because the RTU input module for the SCADA interconnecting with the FOX inside a substation, is not visible on the management system. The smart grid cyber security ensures that only valid function codes are used in the devices to protect the network from cyber-attacks. Introducing smart grid increases the risk of cyber-attacks due to the communication layer incorporated on the power grid, and the risk mitigation can be improved if the correct communication equipment is accurately implemented to protect grid. This can be achieved by using valid function codes.

The data-link layer function code can be used to indicate link status information between devices and to pass link commands, such as reset link. Consequently, a cyber-assailant can alter the function code value for attacks in expectation of exposing vulnerabilities that may not have been handled by the device programmer (trying different header combinations to cause state errors). The cyber security must therefore ensure that a device is used with valid function codes.

Introducing smart grid solutions imposes that cyber security and power system communication systems must be dealt with extensively. These parts together are essential to ensure the proper electricity transmission, in which the information infrastructure forms a critical part [13].

The extensive fibre based communication network for the City of Tshwane, established with the SDH/PDH technology, enables the power system to be operated as smart grid. It was therefore possible to design and model the City's power system using SimPowerSystem as indicated in Figure 1.2 to test and verify the designed power modelled.

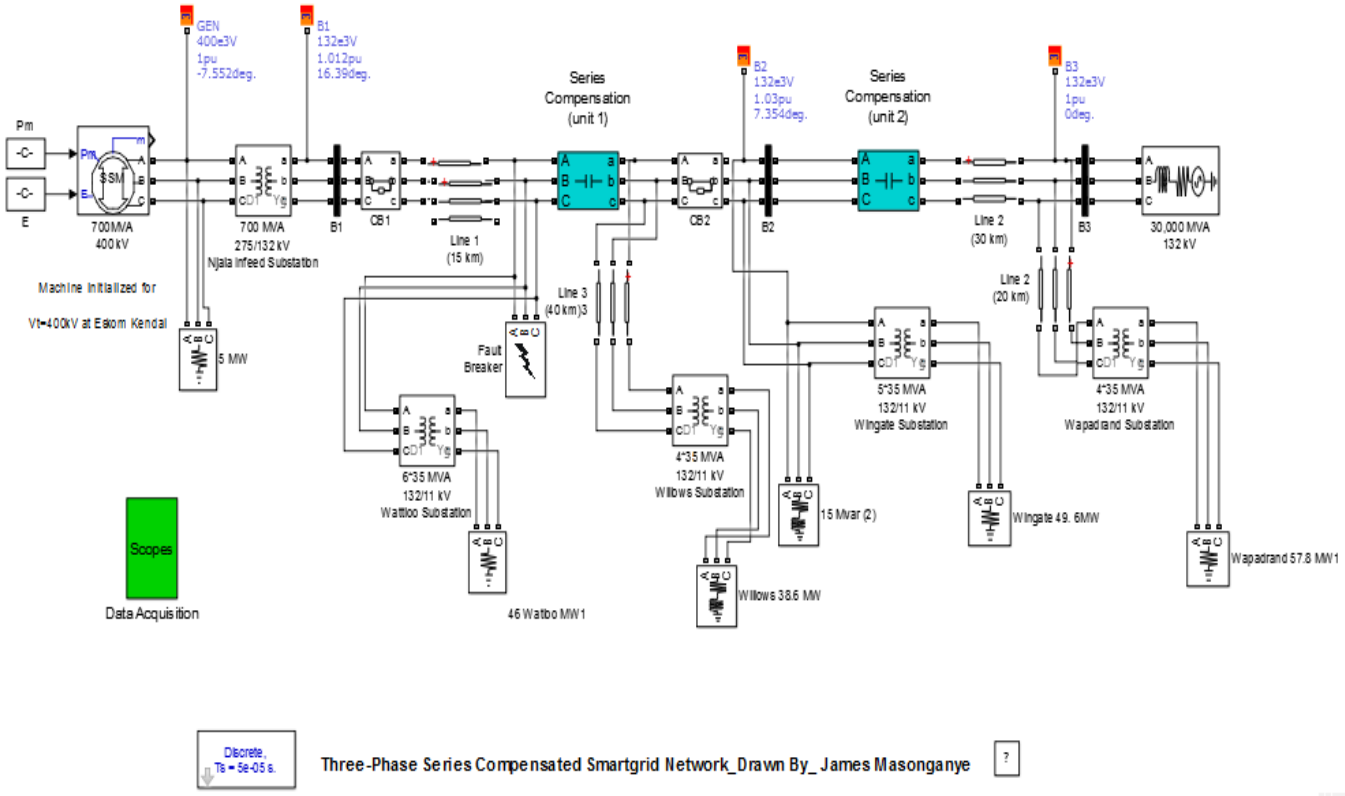

Figure 1.2. Simulink/SimPowerSystem block diagram

The power system comprises a 630MVA, 400 KV line supplied from Kendal to the Tshwane in-feed substation. Njala is one of the City of Tshwane points of supply from Eskom. From Eskom Kendal conventional power plant in Emalahleni/Witbank, a 150 km transmission line, is connected through a step-down transformer at Njala through Apollo inverter switch yard substation. At the Njala substation, the transformer voltage is stepped down to 132kV from 400kV. The HV industrial load providing power to the business industrial areas and low power residential loads, are supplied by the same Line 1 distribution network from (B1) indicated. The other satellite substations also directly connect with the same network Line 1 from branch network B2 and provide power to the industrial and residential customers.

The substation battery charger and substation racks are fed from the power AC Busbar, converted to the 32 V DC. The electrical substation bus scheme supplies the maximum of

six x DC circuits [14], The maintenance team can also react to a flat substation battery, monitored separately through a GPRS network. The GPRS network monitoring the battered substation, do not pose any cyber security risk since the network is separate from the electrical protection and data protection network operating through the substations fibre optic networks.

Figure 1.3 presents the diagram indicates a high-level design of the inter-connection of the City of Tshwane grid with the Eskom national network from the Njala in-feed substation. These are separate networks and it is not possible for the assailant to launch and cyber - attack from the City's electrical infrastructure causing outages to the Eskom National electricity grid. It is possible to cause a power outage to the City if the attack is launched from the Eskom side of the grid since the power to the City is supplied by Eskom.

The Kendal, Apollo substations are Eskom owned and the inter-connection between the City and Eskom is at 275 KV Njala in-feed substations.

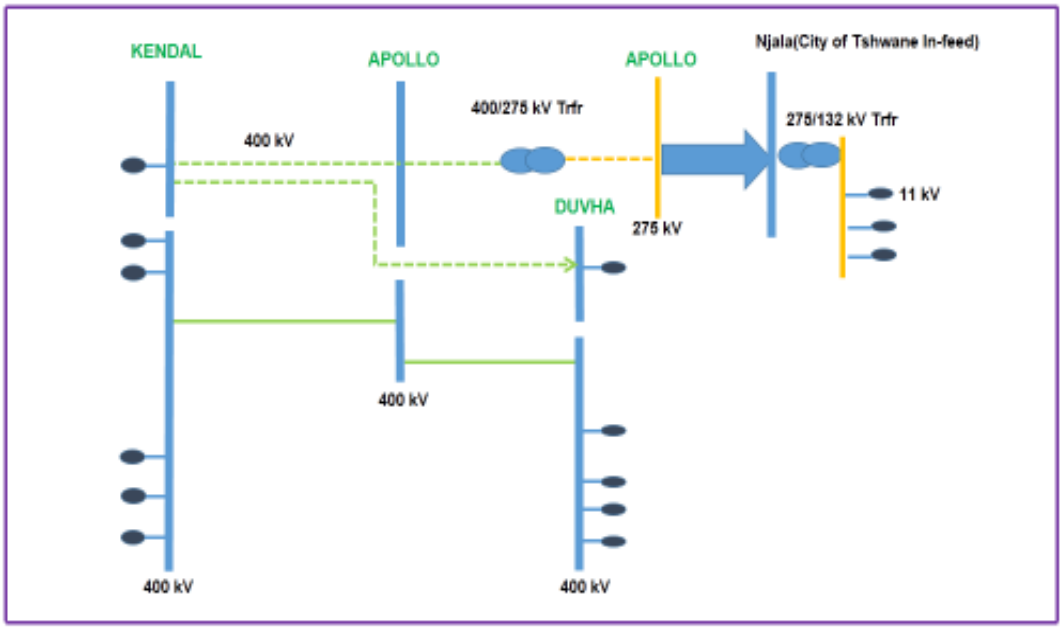

Figure 1.3. Eskom/Kendal to Tshwane transmission configuration

Eskom built, operates and maintain most of its telecommunication national network services. This national private telecommunications infrastructure is used for its internal control and operations of the power grid. The network comprises a microwave backbone with management from its national network management centre.

As discussed, the Eskom national power telecommunication network is physically separated from the Metro power grid, making it impossible to launch a cyber-attack from the Eskom into the municipality power network. Physically separation implies that the communication infrastructures of Metros and Eskom are not linked to each other.

1.8.3 Attack scenarios

The cyber-attack of an electricity grid can be initiated by tripping the substation transformer if the substation communication infrastructure is penetrated. The intruder can access the infrastructure kilometres away or from anywhere globally, if the utility communication network is connected to the public internet network. Architectural design of mitigating an attack from the public network is described in Paragraph 4.2. Such attacks can cause a long-lasting outage that can be catastrophic to the national economy and can cause possible loss of life since critical loads such as hospital, and other institutions depend on electricity to operate.

In the simulation of the attack, a Matlab SimPowerSystem is used by accessing the LAN infrastructure and open the circuit break 1 (CB1) on the SCADA HMI. If the attack opens a breaker in Line 1 of the model, a maximum load of 190MW of power required to operate Wattloo, Willows, Wingate and Wapadrand substations will result in load shedding with a loss of electricity supply to the suburbs supplied from the above-mentioned substations. Although the protection of customer homes is vital since any attacks can affect the grid robustness [11] cyber security efforts are more focussed on sub-transmission of the utility grid, since this is the area where cyber-attacks are likely to occur.

The design of the power line ratings should be able to withstand the 190MW of power ratings. The power flow, being more than the ratings margins, could also result in damaging the HV feeder cable or sub-transmission line. The design of the network is such that the intelligent electronic devices protection relays can sense the power flow in the power system sub-transmission lines. Should the power ratings exceed the design level of the HV voltage line, the tele-protection tripping signals will be activated and will send the high-speed data to open CB1 to prevent damaging the high-voltage line.

Depending on the protection scheme implemented for the line, an automatic line opening would be delayed and an alarm transmits to the control centre through the RED670 relays, or directly to the SCADA system. The system operator at the network control centre in

Capital Park, would selectively shed the load at one of the transformer to protect the line from possible damaged.

The other possible scenario is that a power level higher than a line's rating would not be permitted to flow through the line; a protection relay along the line would sense the power level jump, immediately opening a circuit breaker CB1, preventing damage to the line. Another possible scenario is the automatic line opening would be delayed, requiring the system operator at Capital Park network control centre to intelligently shed load from the grid.

In this attacked scenario, it should be noted that the delay in the automatic line opening depends on the setting on RED670 Intelligent Electronic Device (IED) relays. The RED670 fibre based communication relays comprise in-built time services with self-support supervision and version handling of the events are also incorporated in the relays. This function is internally designed and implemented in the IED software installed inside the relays. The local protection scheme in the FOX network are supported with the Simple Network Time Protocol (SNTP) were the networks of IED require timings for the entire substations multiplexing protection schemes.

In the 132KV substations indicated in Figure 1.4 time-transfer messages in the region of milliseconds (ms), programmed into the relays depending on the critical nature of the grid. Any delays in the operation of the fault protection by the relays can lead to the damage of the transmission Line 1. Failure or the delay in the breaker opening during a fault can damage the HV line completely or cause destroying the substation by fire. Figure 1.5 indicates the grid artificial fault and locations of SFCL simulation results.

In smart grid systems, intelligent relays are used to stabilise the grid. The fibre protection relays offer these advantages:

- The relays communicate over an SDH/PDH multiplexer network where there is redundancy in the event of link failure.

- Communication is continuously monitored with alarming features.
- Cable zone differential protection isolating cable faults, preventing the tripping of the entire substation.
- Fault recorder for post analysis of the fault after major problems occurs remotely with remote downloading of data.
- Interfacing with the SCADA network through the DNP3.0 protocol for remote operation.
- Remote setting changes and data download can be implemented.

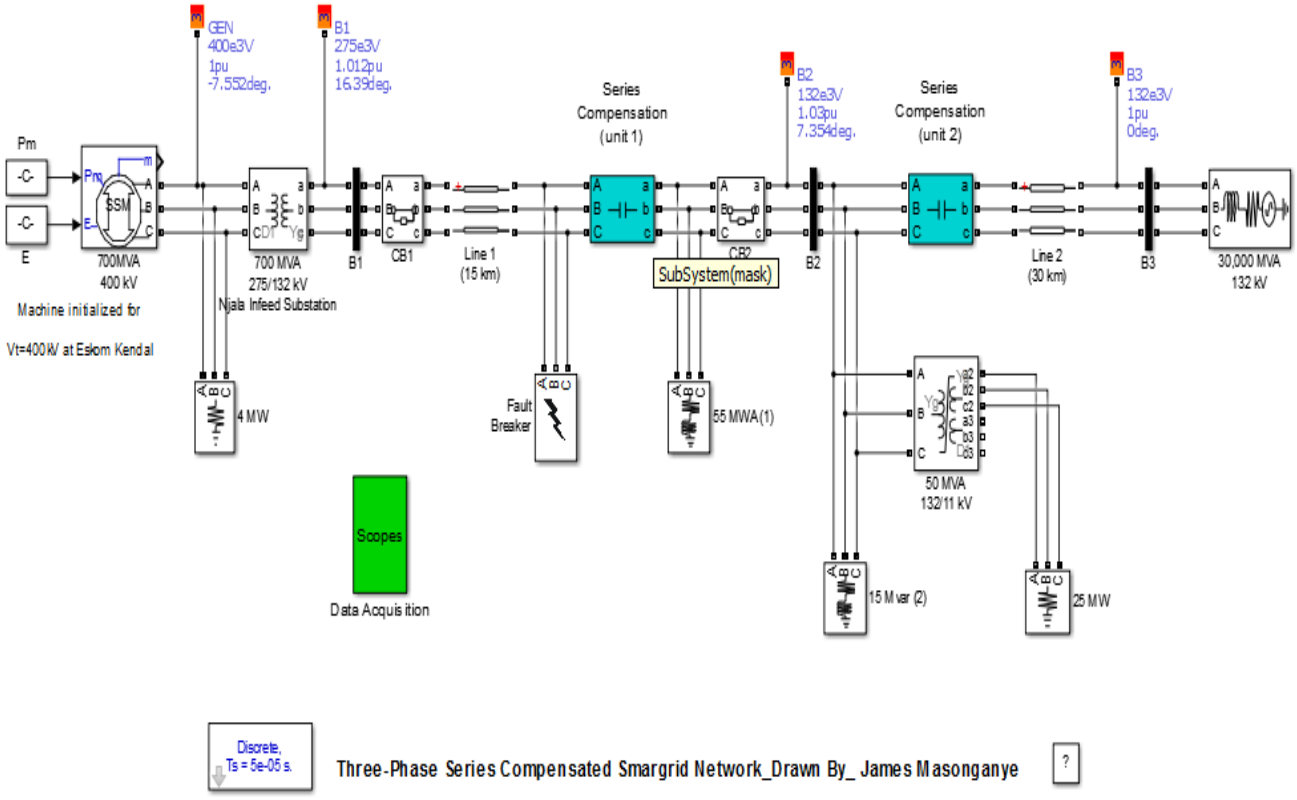

Figure 1.4. City of Tshwane smart grid design diagram

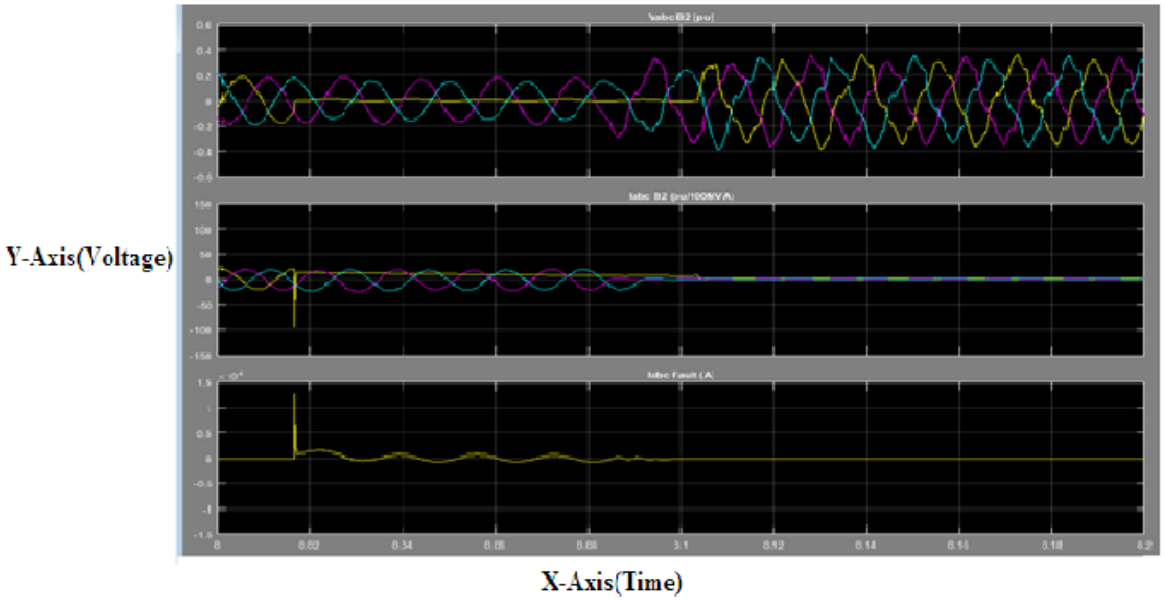

Fig 1.5. The smart grid artificial fault and locations of SFCL simulation

1.8.4 Simulation description

At the Njala in-feed substation both lines are shunt capacitor compensated by a 15 MVAr bank of capacitors reactance. The shunt capacitors and series compensation equipment are located at the B2 Wingate substation where a 300 MVA 275/132 kV transformer with an 11KV tertiary feeds the industrial MW load.

The simulation results in Figure 1.5 reveal the system with a response time delay of 0.02 seconds. Increasing the power generated to exceed the design for Line 1, will cause an increase in the fault current level. At 0.02 s the CB1 can trip by line over current protection relay, the relay response time can cause the fault current to pass through prior to activation. This feature is implemented at most substations. The City of Tshwane FOX to FOX communication network has an interface card called the Tebit card, designed to handle high-speed mission critical communication.

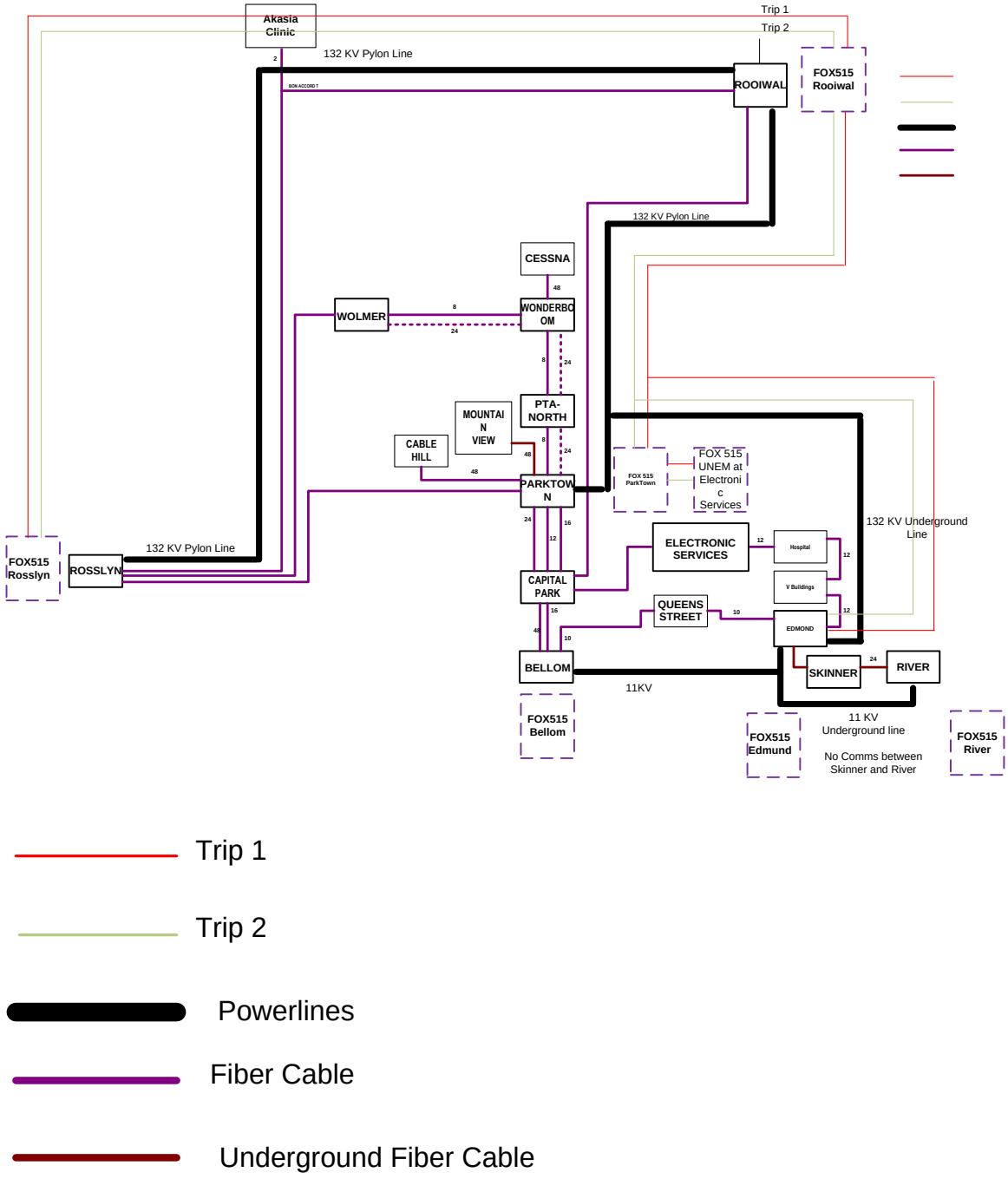

Figure 1.6. Data protection communication network of the City of Tshwane Electricity Department

The digital multiplex FOX -FOX network in Figure 1.6 is designed to operate in electrical HV network and installations are done at substations. The equipment can deal with harsh substation environments, including the electromagnetic interference. It is also reliable, providing secure communications for real-time signals such as voice, SCADA, tele-protection, data including IP/Ethernet and status/control signals.

Interfaces for optical transmission on PDH/SDH 8Mbit/s, STM-1 155Mbit/s and STM-4 622Mbit/s are available. Additionally, the intelligent RED670 relays are also interfaced with the fox network. The UNEM management of the fox network proceeds at Riviera, Electronic Services in Pretoria, as indicated in the diagram above. The feature implemented in the substation protection does not address cyber security for the substation. Only security concerning operation and configuration is addressed.

CHAPTER 2 LITERATURE STUDY

2.1 CHAPTER OBJECTIVES

The national infrastructure plan of the United States of America is collaborating to enhance the protection of the electrical grid against cyber-attacks. Critical Infrastructure and Key Resources (CIKR) focusses on threats and hazards such as terrorist attacks, accidents, natural disasters, and other emergencies under the National Infrastructure Protection Plan (NIPP) [15].

The research reveals the possibility to launch a cyber-attack on the electricity grid if security mitigations are not implemented. The security threats posed by cyber-attacks on the network are discussed in this chapter.

2.2 FIRST THEME OF LITERATURE STUDY

IP address schemes utilised in the City of Tshwane electricity network are highly confidential and the information on IP address cannot be disseminated to third parties to safeguard the network against possible cyber-attacks.

Security threats and flaws are some of the valid concerns in the electricity network. In the South African context, most security threats associated with the power system network are classified as vandalism and copper cable theft.

2.2.1 Security threats [16]

Cyber security threats to the smart grid are revealed and described as follows:

- Malware - Malware are vulnerable to viruses, spyware and trojans and this security threats are deployable to the SCADA server systems. The network connectivity provides a great deal of opportunities for the infection with malware.
- Hackers - These are individuals, including groups with the technical capabilities to gain access to the utility or Industrial SCADA networks. Network data flow can be disrupted with the intention of taking over the control of the system. The results of the disruption could be power systems and other installations.
- Insider-– An employee with access to the employer password to gain access to the network. The employee with knowledge of the company physical assets can disrupt the company computer networks.

The 2015 report published by the Industrial Control System, cyber emergency response team indicate that of all the economic sectors which was attacked in 2015, the electricity sector remains the most attacked sector [17]. Various layers in the SCADA system are used as defencing mechanism to protect the system against malicious attack.

2.2.2 Cyber security threats

Network security for the DNP3 is handled by the lower layer security protocol such as TLS or IPsec. The TCP/IP views the DNP3 address as its user data. The assailant masquerading as another device on the network cyber security, matches the IP address of the pair addressing the DNS. It is not for the assailant to manipulate the system DNS addresses and operate without being detected.

Security for the DNP3 network addresses is not handled by the lower layer security, such as TLS or IPsec, since the DNP3 addresses appear as user data to TCP/IP. A cyber-assailant could manipulate the DNP3 addresses and not be detected by TLS or IPsec if the data

transmission was from a legitimate but compromised device. Consequently, an assailant could disguise as another device if the cyber security does not confirm that the source IP address matches the source DNP3 address pairing.

2.2.3 Application layer security

The smart grid security rule proposed for implementation of the DNP3.0 at the start of the application layer message use the following rules for implementation of network:

- Qualifier.
- Indexes.
- Functional code.

Data communication commands and requests to the primary substation master respond to the satellite substation through the main master. Start, stop and reconfiguring of a device are used to attack a DNP3.0 device handled by the cyber security layer. The challenges in this application layer are the security rules too large to define the data security rules.

A master station can write a certain point such as binary output and input. The network header and data objects may be used to define security rules in the power system transmission network.

2.2.4 Operating cyber security

Cyber security operates in three states being the idle, frame and data security. The operation is in the idle state when data is not transmitted. Data is processed in the frame state and the processing of data occurs in the application where data security is included. If the transmission does not conform to the system usage, cyber security is used to discard the data.

In the frame state, a look-up table apply cyber security rules with few values in the control field. The controlled values are implemented in the cyber security look-up table. The look-up table destination IP address are combined with the DNP3 addresses to find the data transmitted to the DNP3 devices. The data security state uses a single device to create an IP address and discard data transmissions that does not match the rules.

2.3 THE SECOND THEME OF THE LITERATURE STUDY

World leaders recognise the importance of sustainable development with smart grid deployment as top priority. The key to this is the threats that are associated with cyber-attacks to the global grid infrastructure. Smart grid comprises the existing power network and information technology communication network. The leaders are aware of the security threats caused by cyber-attacks on the electricity infrastructure. The resilience and efficiency of the energy network need to be maximised [18]

2.3.1 Risk mitigations strategies in the protection and control of the grid

Deploying the ICT infrastructure of the power systems, resulted in more communication channels parting the substations. Before introducing IED electronic relays in the power systems, the HOR relays operating on the pilot cabling network provided inter-tripping and signalling for the substations. This was achieved using pilot based differential protection schemes. All overhead line and cable circuits were relying on the pilot communication cable protection schemes to balance the current and voltages.

The pilot cable protection circuits are still in use in most substations globally. The City of Tshwane still occupy this type of equipment in its 11KV distribution network. Although all the primary 132KV substations use optical fibre networks, most 11KV satellite substations rely on the pilot cable protection scheme for substation-to-substation tele-protection and communication.

The newer multiplexing technologies deployed in the pilot cable communication networks, operates using the HDSL. The fox system has an interface card specifically designed to carry HDSL traffic, and the maximum speed that can be transmitted in the HDSL is 2Mbps. The major challenge with this technology is the high failure rate of the pilot cable wires directly buried underground, causing the power grid to become a "time-bomb" during the operational life of the substations. The costs associated with the repairing of the pilot cabling network are also high.

The challenge with the pilot translay protection is that when the pilot cable becomes faulty, the substation protection is achieved with the installation of shunt resistance. Faults on the substation pilot do not result in the interruption of power supply. The major challenge occurs when one of the feeder cables supplying power to the 11KV substations becomes faulty; the whole 11KV substation could trip on translay protection. It is impossible to use the GPRS/3G/4G cellular networks for the substation-to-substation protection scheme environment due to the time critical nature of the protection required for the substations which is in the region of milliseconds (ms).

The only services that can be operated on the power system networks are SCADA, used for control and monitoring. Automating the substations through cellular networks concern its own challenges. The cost of data payable to the service providers and security for cellular networks is an impending factor. Joining the public networks, results in the communication security of the substations to be out of the utilities control representing a security risk.

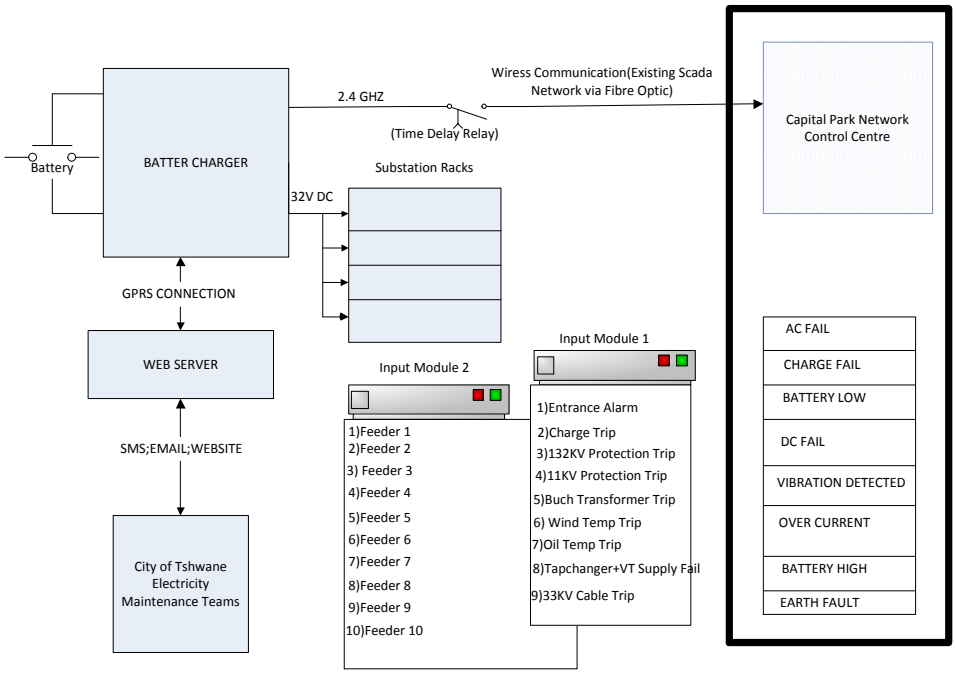

Figure 2.1. City of Tshwane Mini-SCADA implementation for DC battery monitoring

The GPRS implementation of the mini-SCADA system described in Figure 2.1 is used for substation DC batteries and charger monitoring. The input/output expansion collaborate with 12 relay modules. The system is configured to send SMS and email notifications regarding the fault conditions of the substations.

The real-time information from the sensors and batteries is retrieved using the webserver, specifically designed to register and store controlling information.

The following are the key offerings available on the system:

- DC Protection - The substation DC protection equipment is monitored remotely using the load-testing device. The monitoring of substation DC protection reduces the risk of protection failure, including the substation blowing up.

- Panel Monitoring - This will assist the Capital Park network control centre and switching teams being aware of the exact location to restore power after 11KV tripping.
- Increased maintenance - More maintenance on the power network, with fewer staff members.
- Theft and vandalism – The damage caused by theft and vandalism is detected faster and repaired before any long-term damage occurs in the power grid system.
- Load-testing – Monitoring of AC failure, cable trip, low battery and earth fault.

The intrusion detection algorithm is used to detect intrusion attempts to safeguard the web server from prospective system hackers. The advanced encryptions standard is deployed for secure transmission of DNP3 data used for the SCADA system over the internet. DNP3.0 data routes through the firewall designed in the SCADA security architecture, described in Paragraph 4.2.

2.3.2 Security threats [19]

As indicated above, power system security is a major concern for the power grid. Proper policies and protocol need to be implemented for access control, audit trails and other protection issues in the infrastructure. The infrastructure needs to be secured and protected in real-time to mitigate the risk of cyber-attacks against the following:

Cyber threats in smart grid systems include:

- Failure of the safety measures.
- Failure of tele-protection equipment circuits.
- Giving the system password to intruders and hackers.

Dissatisfied employee with technical knowledge of the system:

- Vandalising the network with the aim of causing power interruptions.
- Hacking into the system databases and computers.
- Implementing viruses.
- Password theft.
- Terrorist attack.

A key factor for the security of the power system operation is to protect the plan from the network hacking and possible cyber-attacks. The IP addresses of the various routers and devices implemented inside the substation, should not be available to the public. The IP address scheme of the electricity network is used for substation monitoring network. The range of the IP network is different from the City of Tshwane Corporate IT network. It would be difficult for the intruder to launch a cyber-attack even with access to the substation LAN network.

Off the shelf software packages can be used to perform traceroutes by connection a PC on the substation LAN to retrieve the IP network connected on each device on the network.

2.3.3 Network security for smart grids purposes

The main aim of the system protection is categorised in various security layers, defined to address the following measures:

- Delaying and avoidance of attacks.
- Delay attacks for enough counter actions to be implemented.
- Determining the severity of the attacks. This is achieved by entering several passwords, attempts to guess the correct one.
- Notify the authorities in time for them to be aware of impending attacks.
- Implementation of actions by the authorities.
- Assessing the attacks to analyse their impact.

2.3.4 Vulnerabilities of smart grid communication architectures [20]

The smart grid threats can be categorised into the following scenarios:

- Data manipulation.
- Network sabotage.
- Espionage.

Manipulation of the network can be achieved at a system level. The network manipulation can be accomplished by accessing the city-wide SAP Billing and metering information and by modifying the software. The utility is required to implement various security layers for the early detection of breaches that could compromise the protection of the grid against cyber-attacks. This could also be achieved by placing software in a smart grid gateway [21]. The assailant needs to gain access into the environment. The main aim is to find the weakness on the network and in the process, gain reasonable control of the network components.

Accidents such as cable damage by the assailant, could lead to significant impacts. Most attacks on the power networks are caused by cable theft. Espionage involves a class of threats in the smart grid system where the assailant assesses information on addresses and lifestyle. Another typical aspect is attacking a low voltage network component of the grid.

2.4 MORE LITERATURE STUDY THEMES

Inside a substation LAN smart grid traffic, need to be totally separated from the operational information of the substation. Data segregation can be achieved by partitioning the traffic into VLAN’s to protect important information such as SCADA traffic, access control and substation protection services. Where utilities fibre optic network is used to carry telecommunication based services for internet and public WiFi, it is highly recommended not to connect all to the same switch. All networking cabling should be connected directly to the patch panel and then routed to a separate switch dedicated for those services.

Operational data, such as Generic Object-Oriented Substation Events (GOOSE) and IED 61850 protection relays should also be separated since this is mission critical data used for the operation and protection of the power system network [22].

Within the City of Tshwane electricity data protection network, the following telecommunication is used for substation-to-substation communications are:

- Optical fibre cabling consisting of aerial cables, optical ground wire and underground fibre.
- UNEM network management systems for FOX management.
- FOX telecoms multiplexer SDH/PDH switches at all in-feed 275 KV, 132 KV and 11KV substations.
- Digital trunked radio communication.
- Radio communication towers at distribution substations.
- DC power systems at substation.
- Load-testing communication equipment.
- RTU, including tele-protection.
- Switching centres linked to the towers at emergency centres through microwave and optical fibre cabling.
- Pilot cable for the tele-protection for line differential protection systems.

The City of Tshwane telecommunication network is designed according to the following network:

- Access network.
- Corporate IT network.
- Intranet.
- Extranet.

The corporate IT network, Intranet and Extranet are the responsibility of the IT department of the City. The development of the access network is part of the electricity department's network deployment.

2.5 REFERENCING

Utility operators take various measures to protect substations automations and the communication networks within the substations against cyber-attacks. Substations are equipped with an anti-virus system, protecting the substations against cyber-attacks. Technology evolves with this factor; more standardised security measures should be implemented to protect the power systems against attacks.

Issues of cyber security in the smart grid system are of high priority since numerous devices are vastly distributed in the Service Oriented Architecture (SOA) - based infrastructure [23].

The SOA is flexible to integrate by their nature of design since they are distributed widely across the web. With the advent of a smart grid, a general increase is extant on the need for systems to be inter-connected. The most severe threats to the infrastructure is cyber-attacks with social engineering with the most severe attacks. Social engineering is conducted by phishing [24]. The assailant can take control ownership of computer system, gain access to email and password login information.

Technical research and journals contain more information on smart grid security. Various challenges are faces impeding on implementing the smart grid security, including:

- Regulation guidelines.
- Only 87% of the utilities are complying with the NERC security rules. This implies that not all of them are aware of the security of the recommended security measures [25].
- Terminology and standardisation.

- The lack of standards to quantify the security required in the grid is one of the impeding factors affecting security requirements for the power grid.
- Research and cyber security in power grid.
- Most electronic devices used in power system relays and software are vulnerable to attacks due to the lack of defined security.
- Collaboration.
- Universities and national labs implemented test beds for testing and measuring but this system is disjointed. The capabilities can be achieved by some level of interconnectivity between these systems.

2.5.1 Substation data security

Substation transmission communication networks are designed with high bandwidth to carry data traffic. Monitoring of substations using the SCADA system from control centres, require constant data transmission to monitor and operate the substation from the remote locations. The multiplexers are installed inside the substations prior to the local area networks.

Because of the smart grid deployments using critical data, both the SCADA systems and the smart grid networks need to be engineered with secure data networks. Cyber security for the substation is of paramount importance for the safe operation of the grid network.

2.5.2 Security inside the substation

Various data segregated needs to be utilised for the operation and control of the substation. Inside the substation SDH/PDH for substation and ATM broadband switches used to carry internet traffic are used for voice over IP services. These two different technologies are separated using VLAN. If the same hardware is used inside the substation, the hardware should maintain segregation with priority given to the SCADA and protection services. The GOOSE and IEC61850 messages are separated using VLAN since data are critical for the

operational requirement of the substations. The data separated using VLAN use the same equipment to maintain the various ports.

The LAN Security using VLAN is achieved between the two substations:

- The VLAN installed substations which are equipped with FOX switch Multiplexer can be at VLAN 2 and the remote substation at another remote substation can be set on VLAN 2.
- The data transmission between the two substations will not be visible to any port on VLAN 2. This configuration of substation switches using VLAN ensuring that the logical separation of traffic for the LAN substations are implemented for data transmission.

2.6 ADDITIONAL CYBER-ATTACKS ON SMART GRID

2.6.1 Cyber switching attacks

Attacks on a smart grid system can be influenced by switching the basic attack rules. Using these attacks, the power system can be destabilised by switching the grid between two systems. This is achieved when a hacker gain access to the power system and estimate the generator speed [26]. The hacker drives the generator and rotor speed to instability, isolating it from the power system. The total black-out of the entire power system can be affected if the critical generator inside the power generation substation, are attacked.

Some of the obstacles that can prevent the hacker from launching the above attacks, include access into the grid cyber layer and estimating the system frequency from which the measurements are estimated. The difficulties in accessing the cyber layer and estimating the frequency of the system, can be overcome by the hacker, resulting the hacker analysing the cyber switching attacks in real-time.

2.7 LEARNING THE CYBER SECURITY TO MITIGATE THE FALSE DATA INJECTION

Data falsely injected into the grid can be demonstrated employing a Matlab/Simulink package software. The effectiveness of using the false data injected is demonstrated by simulating the 39-BUS system to demonstrate the mitigation [27]. A short circuit fault occurring in the middle of a transmission line, is cleared by deploying protection methods capable of learning the malicious attacks.

The phasor measurement units used to measure the stability of the grid, are used for detecting data integrity generated. Deep learning of cyber securities is used to address the threat model against malicious attacks. The true values of the PMU data are validated by verifying the presence of the attacks. The PMU are the devices normally installed in the power grid, capable of enabling the entire grid status to be observed and controlled in real-time [28].
The frequencies, and phase angle strategy proposal of a deep learning based, are described by the threat model below.

Methods for specifying the attack mitigation threat models are:

- Knowledge of the power system.
- Corruption of the Phasor Measurement Unit data.
- Prevention of the phase data concentrator (PDC) against the data compromised.

In the first assumption, the assailant is credited with the topology of the power system and the information regarding the network topology may be obtained by eavesdropping the electricity data communication network. The second assumption executes the attack with minimal cost, if the PMU reading are replaced with the wrong or changed quantities. The last assumption requires the Phasor data concentrator, acquiring an expert attack detection mechanism.

2.7.1 Physical attack in co-ordinated cyber-physical attacks

In paragraph 2.6.1 and 2.7, the switching cyber-attacks and false data injection were discussed. In this section the impact of coordinated cyber-physical attacks on the designed model is investigated. The 132KV substations for the model under study are linked with HV transmission lines, spread over a larger metropolitan area.

Inside the substations there are protection relays, but the transmission lines outside the substations are exposed to physical attacks. Tripping the transmission lines should not disconnect the whole power [28] but only the portion of the network affected by the power outage. Only the actual power flow on each transmission line in the network will be redistributed, based on the power flow after the physical attack on the transmission line.

2.8 CHAPTER SUMMARY

In this chapter, the brief overview of the cyber security threats (including hazards) cyber-attack focus was provided. Section 2.2 offered a detailed overview of Smartgrid security threats, including efforts by the industrial control and emergency response team on security threats.

The chapter described in brief, the operation state of cyber security. The role of the pilot cable protection scheme for the 11KV satellite substations was also covered. Key available features, such as substation DC protection for battery and panel monitory was also addressed. Network vulnerability, security (including the design of the data protection network for the protection of the substation), was addressed in this chapter.

Sections 2.6 and 2.7 concludes with the various types of cyber-attacks, such as cyber switching attacks and learning the cyber security for false data injection. It was found that it is possible for the hacker to destabilise the power grid by launching these attacks.

CHAPTER 3 METHODS

3.1 EXPECTED LOAD CURTAILMENT FOR VARIOUS BUS MODES

Once the system administrators' rights are illegally accessed, the intelligent cyber assailants can easily initiate a cascading failure or a black-out, by sabotaging the secondary electrical components (protection systems). The enhancement of cyber security in power systems must address the coordinated cyber-attacks on ICTs and responses of secondary electrical systems, directly depending on ICT [29].

Suppose that all CB's in the in Fig. 3.1 are closed and the initial settings for the three-phase breaker CB1 initial state "closed", switchA, switchB, switchC "on". The switching times [5/60] bus protection for three-phase voltage and measurements all set phase to ground with base power of 100e3 VA. The initial settings for the transmission line protection from Njala in-feed substation to Mooikloof is described in this paragraph. The ELCs, measuring the cyber-attack risks, are Mooikloof 46MW, Wapadrand 38.6 MW, Wattloo 49.6 MW, and Mamelodi 1 at 57.8 MW. If assailants can attack 10%, 50%, and 90% of parameters, respectively. Figure 3.10 shows the ELC as a function of the number of SimPowerSystem simulations when 90% of the parameters are attacked.

By launching a denial of service attack on the communication network, the assailants can jam the communication channels by attacking the TCP/IP protocol, and this entails flooding the network traffic [30], [31]. By attacking the protocols used in communication networks, the network packets from sensors passing the channels will be lost.

The power system can therefore be modelled as an on or off switch under DoS by simulation the SimPowerSystem in Matlab.

The existence of a DoS in the smart grid network can destabilise the power grid using switched system theories [32]. The DoS attacks are launched by opponents with the main aim of flooding the network and cause the network congestion. All packet data traffic is lost, resulting in the control centre system operators not being able to update the SCADA HMI system. The type of attacked modelled using Matlab/SimPowerSystems is called the Aurora attack since the assumption made was that the test bed was designed using power systems layer.

The communication layer was not integrated to the power system layer and there is no communication to interconnect the data flow between the power system and the communication model. The assumption is, communication data transfer does not pass through the substation in real-time. For the data flow to pass through the communication layer, a communication network simulator should be added to allow data to pass through.

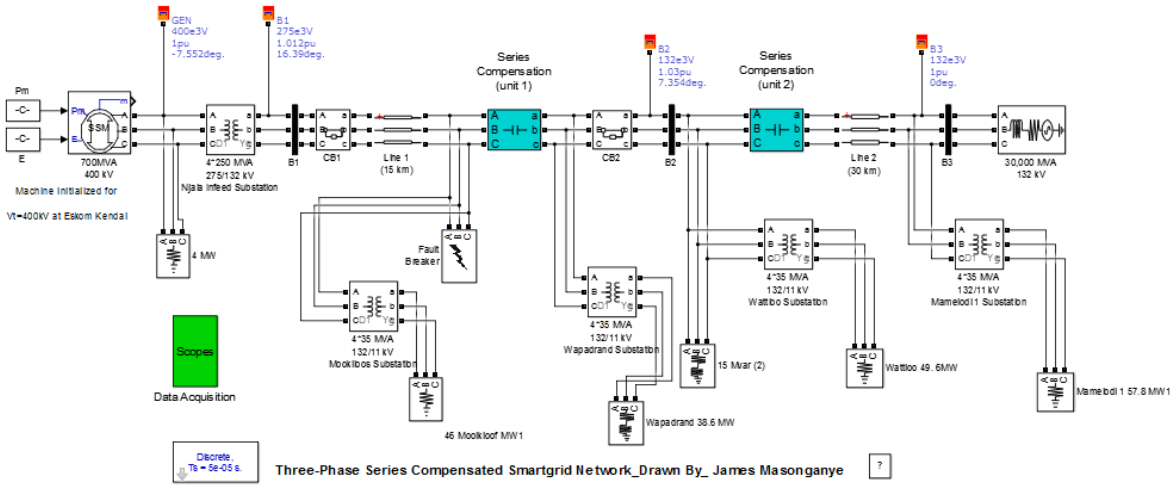

Figure 3.1. City of Tshwane smart grid network simulated model using SimPowerSystem

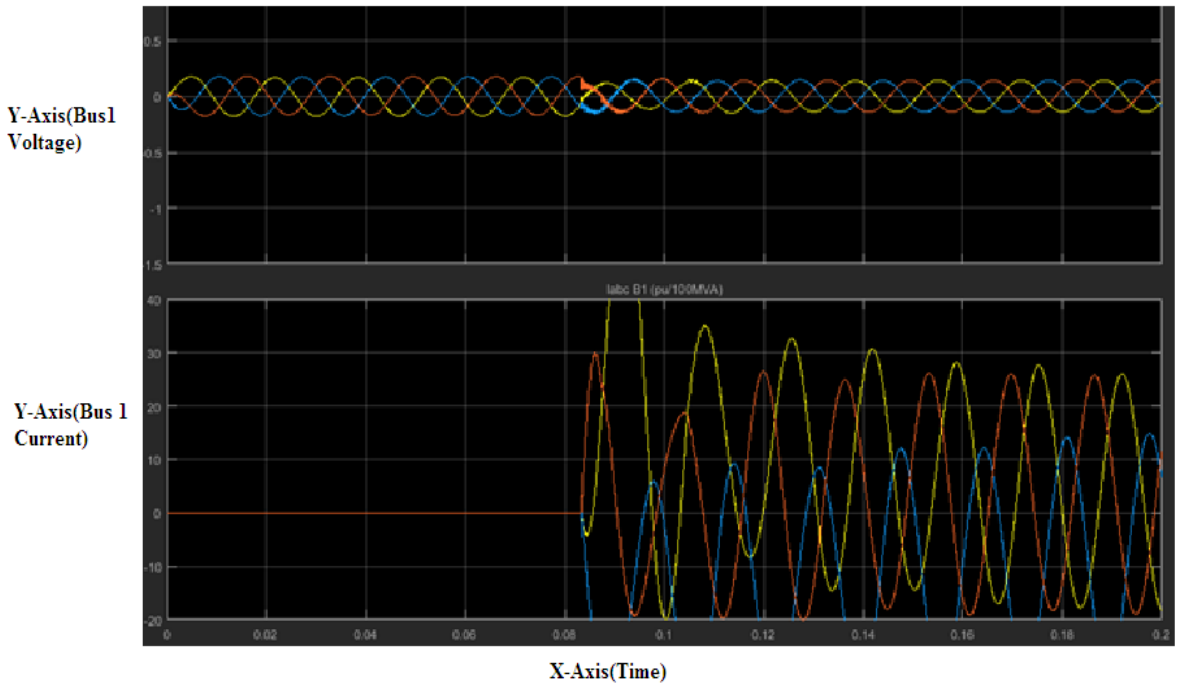

Figure 3.2. Expected load curtailment cyber-attacks

The ELC reaches about 43MW, though with minor variations, after 2000 simulations, based on which the simulation is converged. The convergence of the simulation process is similar in the other two cases.

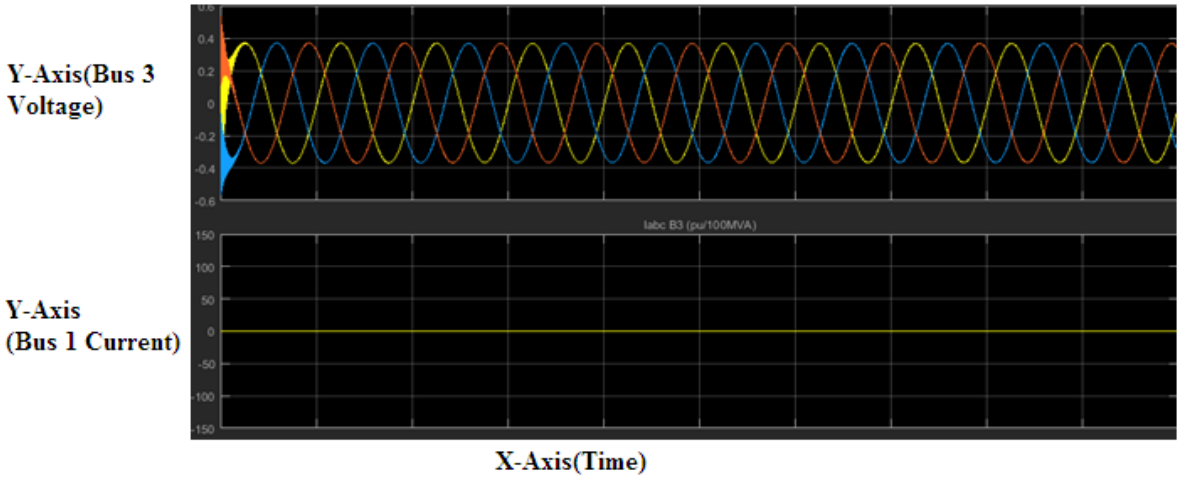

Figure 3.3. Expected load curtailment cyber-attacks

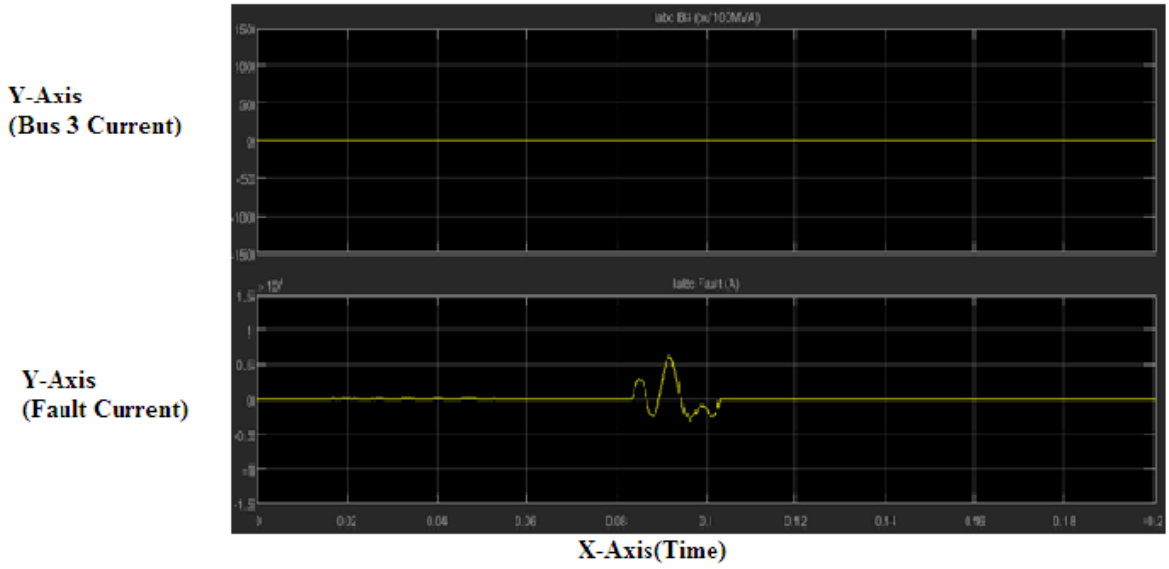

Figure 3.4. Expected load curtailment cyber-attacks with fault current

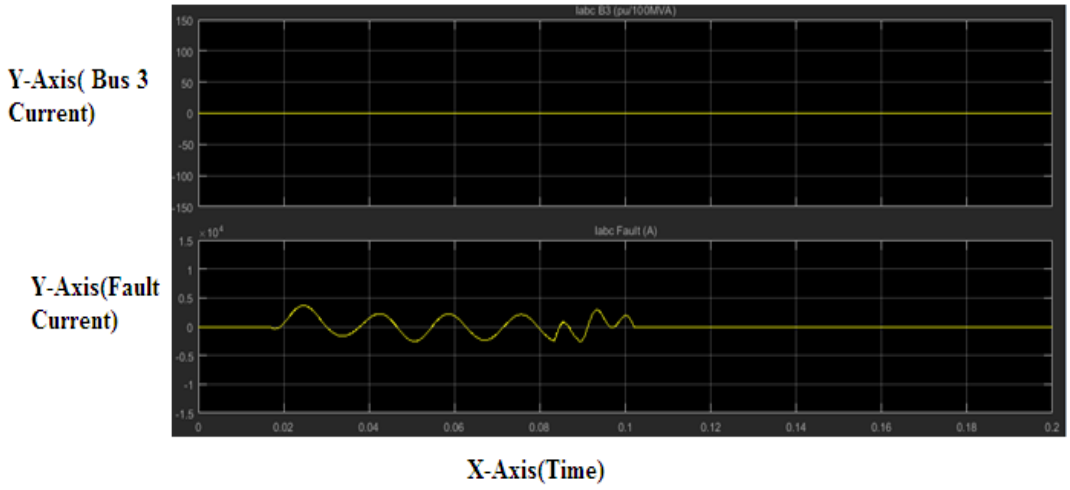

Figure 3.5. Expected load curtailment cyber-attacks

Table 3.1. Expected load curtailment for differential bus operation and cyber-attack

Substation	Load(MW)	50% of Load Reduction(Load)	Transformer (MVA)
% of parameter attacked	0%	50%	
Njala	700 MW	350 MW	4x 250 MVA
Wingate	49.6 MW	24.8 MW	5 x 35 MVA
Watloo	46.7 MW	23.4 MW	6 x 35 MVA
Willows	38.6 MW	19.3 MW	4 x 35 MVA
Wapadrand	57.8 MW	28.9 MW	4 x 35 MVA

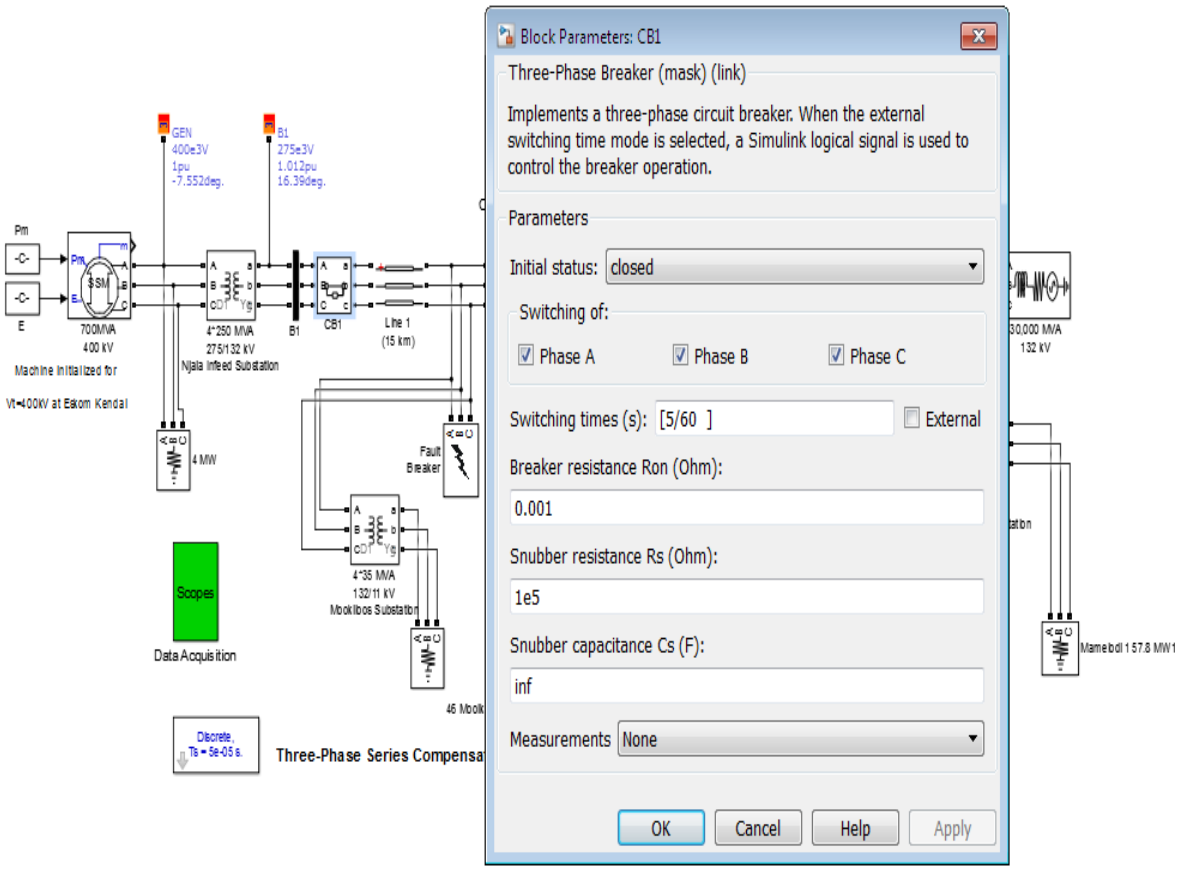

Figure 3.6. The block parameters of the transformer, changed to curtail the load for various substations by 50% to simulate the attacks

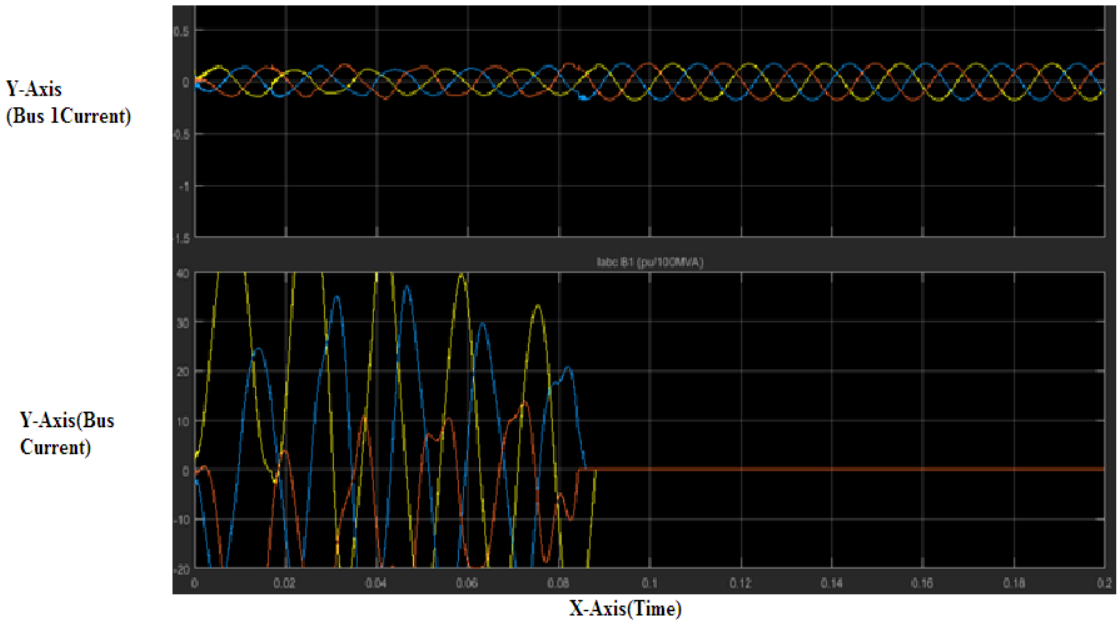

Figure 3.7. ELC CB1 closed

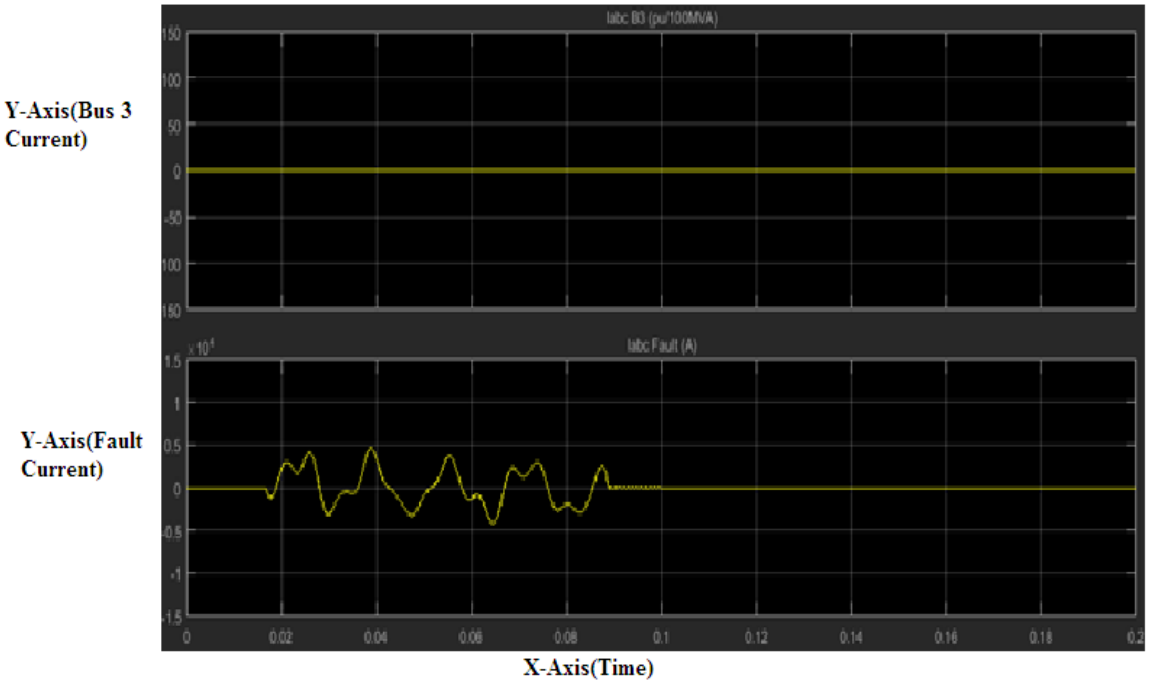

Figure 3.8 ELC CB3 SimPowerSystem when 10% of the parameters are attacked

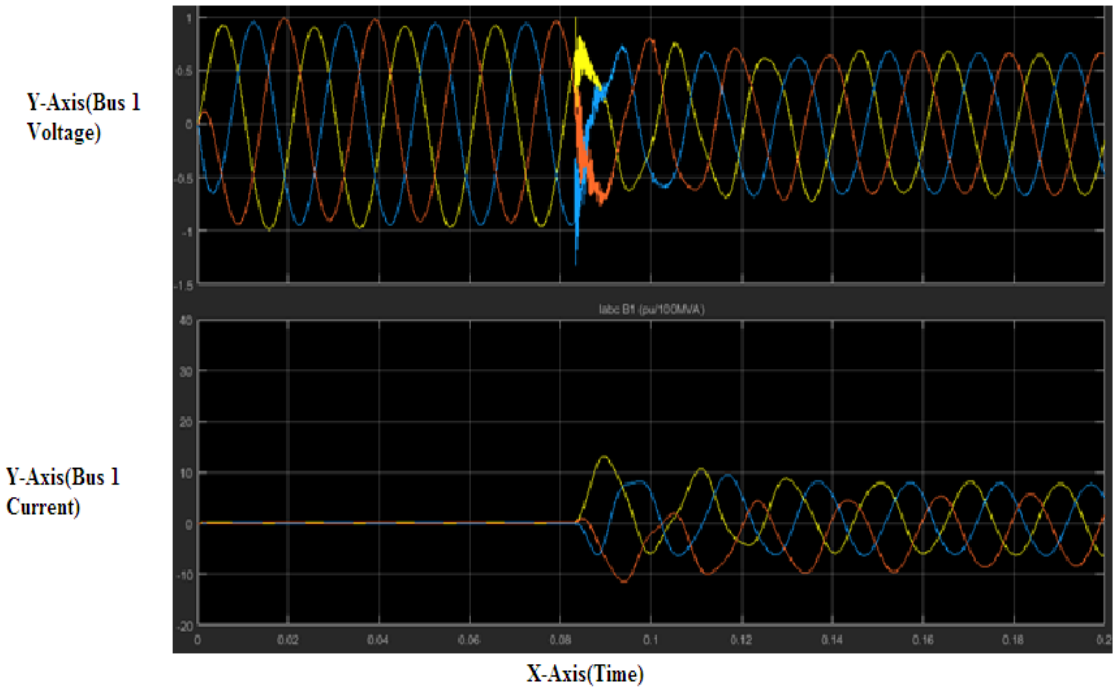

Figure 3.9. CB1. The three-phase circuit breaker (CB1) open at 0.08 seconds

Figure 3.1 to 3.5 also considers Aurora attacks with the power system operating under cyber-attacks on the 132KV side of Njala in-feed substation. The above simulation shows the effects of the Cyber-attack on the power system. The following launching time will show how the system responds. The block parameters of the CB switching times were selected with the breaker open and close at different time intervals as indicated in the Table 3.2.

Table 3.2 describes the simulation result shown in Fig 3.9 to Figure 3.13, including the attack steps. The switching times shows that the assailant launches an attack by opening a breaker's CB1 to CB3, resulting in various load consumptions.

Table 3.2. Three-phase breaker switching times

Breaker Initial Status	Breaker Resistance(Ohm)	Switching times	Switching time (s)
Open	0.001	5/60	0.08
Open	0.001	10/60	0.2
Open	0.001	20/60	0.3
Open	0.001	30/60	0.5
Open	0.001	40/60	0.7
Open	0.001	50/60	0.8
Open	0.001	50/60	1.0

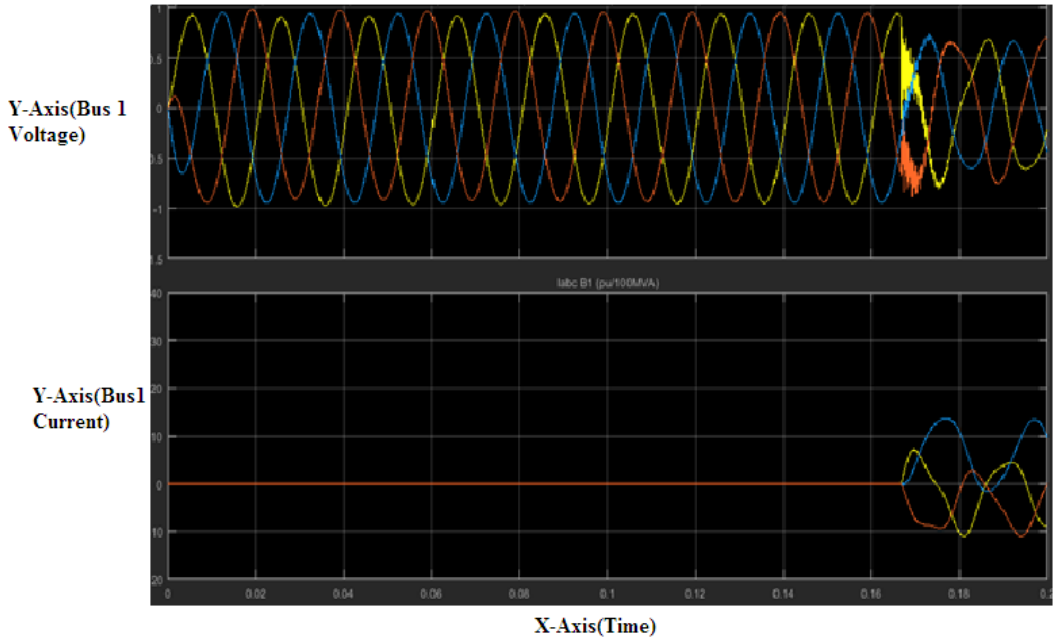

Figure 3.10. Three-phase beaker switching times at 0.2 seconds

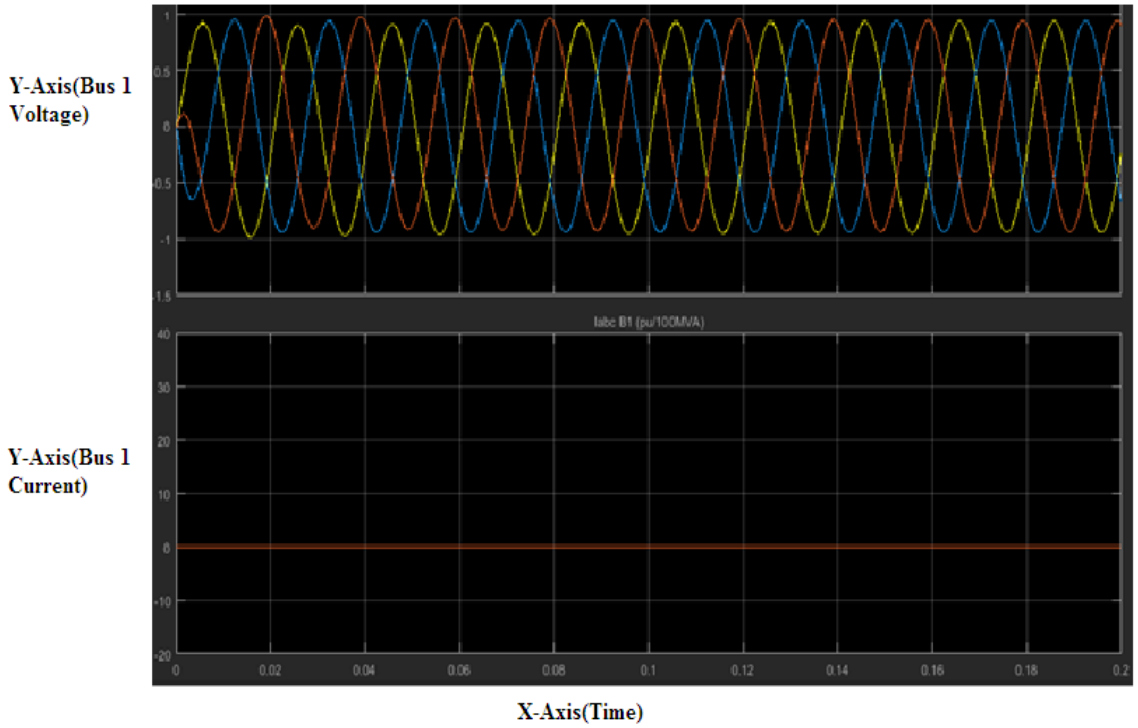

Figure 3.11. Three-phase beaker(CB1) switching times at 0.3 seconds

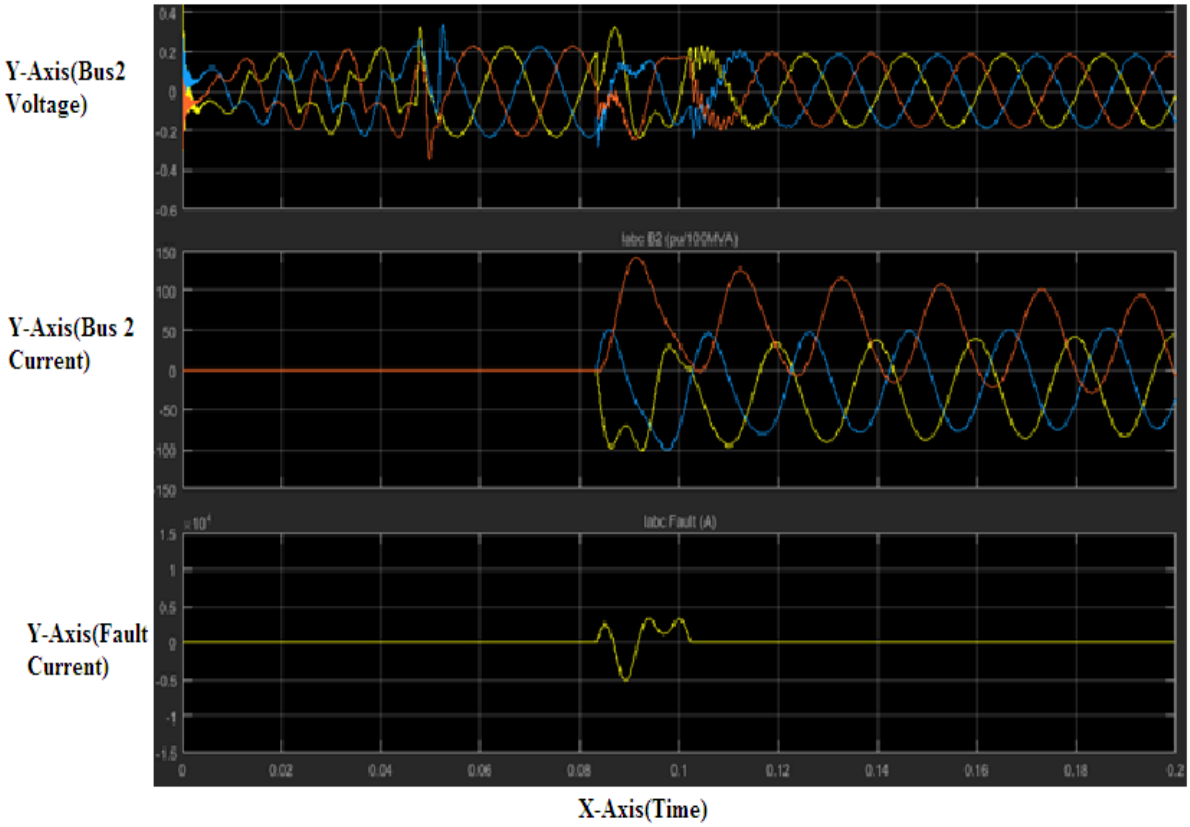

Figure 3.12. Three-phase beaker (CB2) switching times at 0.08 seconds

CB carries the full load current continuously without overheating or damage. Figure 3.13 shows when the circuit breaker (CB2) opens the circuit on no load, it breaks the normal operating current resulting in the disturbance of the power systems. The simulation shows the operating current when the fault occurs.

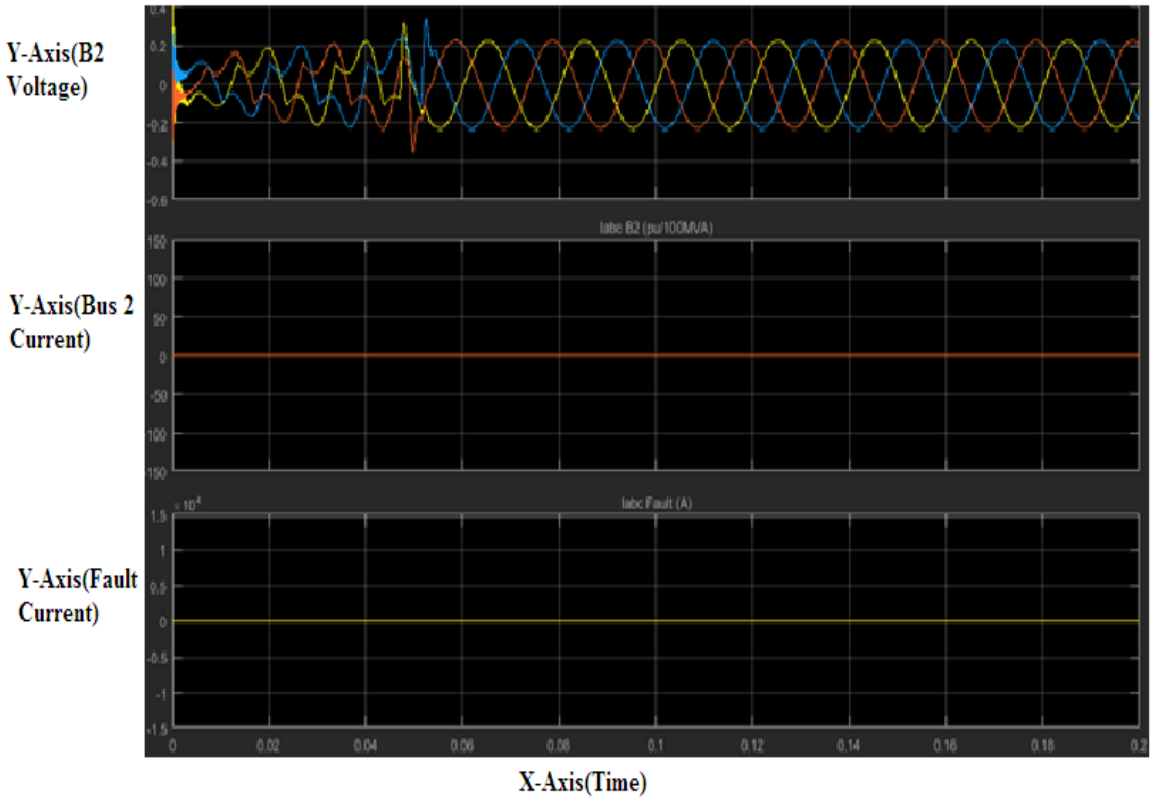

Figure 3.13. Three-phase beaker (CB2) switching times at 0.3 seconds

CHAPTER 4 RESULTS

4.1 RESULTS AND DISCUSSION

The study analysed the impact of cyber-attacks on the power system. The role the communication infrastructure plays in the operation of the modern power grid shows that the grid is more exposed to cyber-attacks. In this paragraph, the results of the cyber-attacks on the power grid, using false data injection and various frequency are analysed.

The substation load points in the Table 4.1 are derived from the transformer reading and input into the simulation model. The response of the system is analysed by varying the frequencies of the simulation model.

Table 4.1. Simulation result

Substation	**Load(MW)**	**Transformer (MVA)**	**Frequencies (Hz)** Minimum	**Frequencies (Hz)** Maximum
Njala	700 MW	4 x 250 MVA	49.90	50.29
Wingate	49.6 MW	5 x 35 MVA	49.72	50.105
Watloo	46.7 MW	6 x 35 MVA	49.81	50.06
Willows	38.6 MW	4 x 35 MVA	49.87	50.06
Wapadrand	57.8 MW	4 x 35 MVA	49.96	50.33

Figure 4.4 indicates the result when a corrupted frequency is injected and detected by the smart grid system. In this simulation, it is shown that varying the transformer frequency

results in a corrupted graph. Changing the frequency results in the transformer tripping and power outage. This is shown by the graph with corrupted lines in Figure 4.4.

The frequency can be corrupted if the assailant plugs the PC into data protection communication LAN infrastructure and gain access into the SCADA system. In a real co-simulation design environment were the power system is integrated with communication network and monitored with a SCADA system, the control bus will appear as in Figure 4.1 and 4.2 from the control centre SCADA system.

To view a load bus in the simulation in real-time as depicted in Figure 4.1 and Figure 4.2, a co-simulation for MatlabR201b and NS3 software package would have to be integrated, used for the communication network

4.2 OVERVIEW OF THE CITY OF TSHWANE SCADA APPLICATION

The City of Tshwane Electricity department uses the Siemens Spectrum Power 3 in controlling and monitoring its electricity grid. The systems comprise software, hardware and interfaces for monitoring and control of its electricity network. The picture of the one- line single diagram of the SCADA system at Capital Network Control is shown in Figure's 4.1 and 4.2.

The one-line diagrams are used to display input and output values of the substations in tabular form. The state of the substations breakers is displayed as single line diagram to provide the following network conditions:

- Computation and checking of the limit in MW, MVAr, KV and MVA.
- Handling of electrical faults.

- Voltage and current flow for the substation BUS.
- Opening and closing of the CBs.
- Transfer of load to the different feeder.
- Detect overload network branch.

Smart grid systems are dependent on reliable SCADA and embedded systems for the grid to be operated efficiently [7]. The level of security provided by most SCADA systems is limited and low. This is due to the challenging nature of security analysis in embedded systems. The SCADA systems requires a high-level of security to be in place for the protection, control and accessing of the database. As a security measure, protecting the system from possible cyber-attack, access to the SCADA system requires a router to be configured to block the hackers.

Access to the SCADA system is granted manually by the system operators, to allow remote access, and a specific user need to be authenticated by the system before being able to switch the system to service mode. The following service tool protocols are used for remote access to service the system:

- Telnet.
- PuTTY.
- NetOp.
- PcAnyware.
- WinVNC.
- TetraTermPro.
- Timbuktu.
- Netmeeting.
- Tarantella.
- Citrix.
- MS Terminal Server.
- SNMP.

The HTTP, Telnet protocols are only allowed to operate outside the zone of the SCADA system due to insecurity associated with these protocols. Blocking of traffic can be furnished by configuring the firewall using firewall management.

Figures 4.1 and 4.2 represents the single line diagram of the SCADA under normal operating conditions with the CBs of the substations closed. The single line diagram depicting a SCADA human machine interface, is simplified indicating relative arrangements inside the substations. The main purpose of representing substations as single line diagram, is to assist the system operators at the control centre with the switching operation, control and monitoring of the substations.

One of the strategies used by the assailants is to study the topology of the power grid to successfully launch an attack on the SCADA, using data injection. In launching a cyber-attack and the control centre exposed to attacks, the data detection scheme can be defended by identifying the source of the tampered data [33]. The mechanism used to analyse the powerflow in the smart grid, is the Matlab simulation tool.

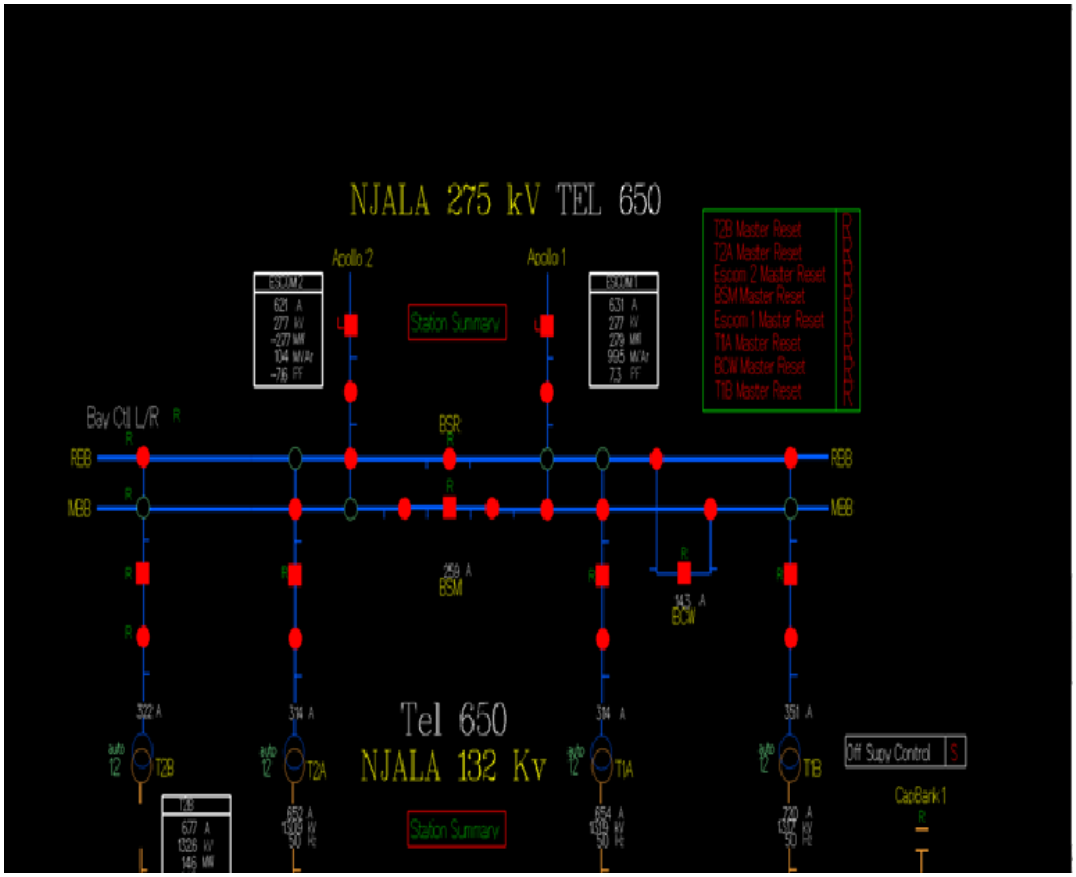

Figure 4.1. Control Centre online display by SCADA before cyber-attack- Njala in-feed substation

The system operator responsible for operating the SCADA system at Capital Park network control centre can make an incorrect decision by the remote opening of a CB on the HMI SCADA.

The real-time bus load for the network in the study was validated from the SCADA system in Capital Park. It was impossible to view the impact of cyber-attack on the online SCADA from control centre since load management and power management is done using the “Live” system.

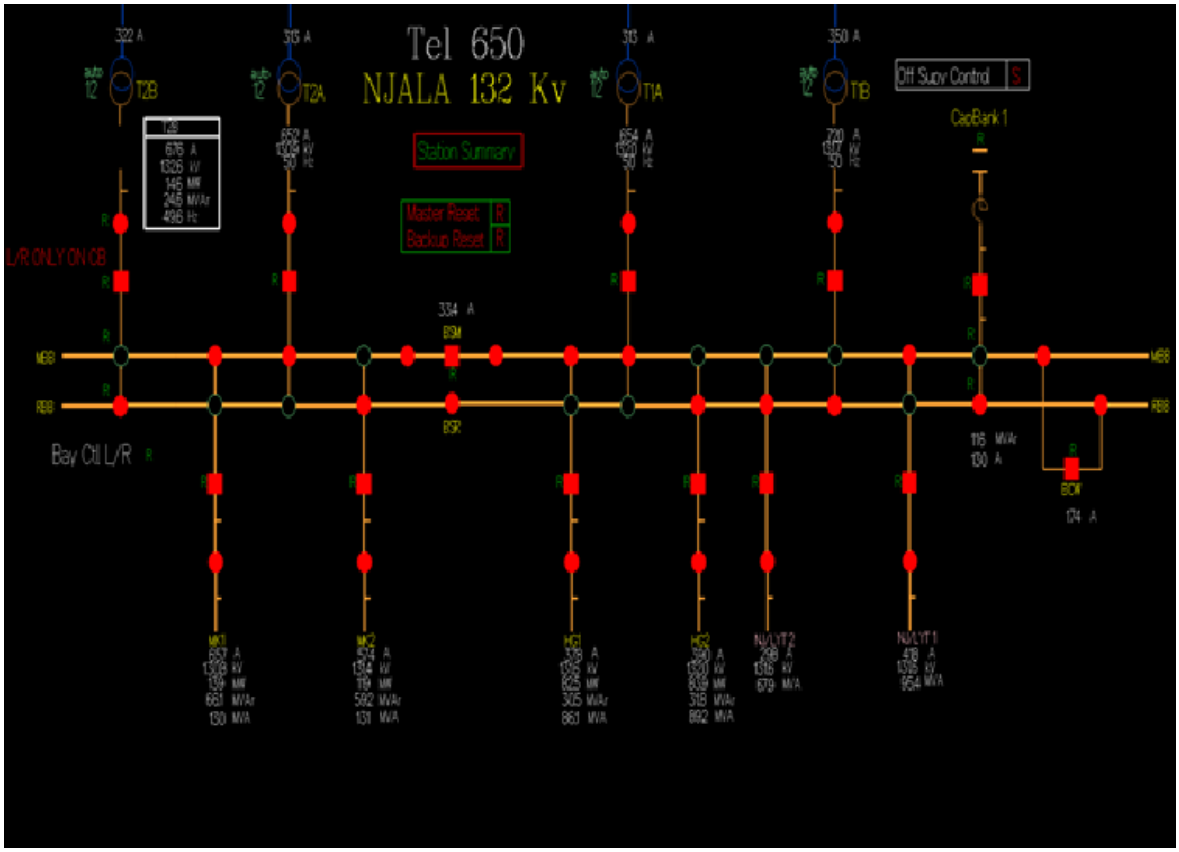

Figure 4.2. Control centre single line diagram by Scada before cyber-attack

At the control centre, sensors installed at the substations to measure the voltages and power flow, monitors the grid. When the measured data is transmitted from substation to the control centre through communication networks, the data can be intercepted and altered by the technique, called false data injection.

As shown in Figure 4.1 of the SCADA single line diagram above, the power flows at Mooikloof (MK1 and MK2) Lines 1 and 2 is 130MVA and 131MVA respectively. The false data can be injected into the power system bus by the assailant, resulting in the system operator at control centre making a uniformed decision by overloading the transmission lines with shifting the load. When the line is overloaded to exceed the threshold of the line the line, the line could be damaged resulting in a major power outage [34].

The attack on the grid protection and control system can also be initiated by launching an Aurora attack [35]. From the SCADA line diagram, a breaker carrying more load, enough to cause a major outage on the grid is opened. Physical access to the RED670 relays requires an assailant to access a communication, not encrypted from substation LAN. By using the protective relay to launch an attack, the hacker needs a good understating of the relay to initiate a fast trip to the CB. The SCADA line diagram at the main control centre and the substation LAN communication, provides a good condition for initiating an attack.

The utility SCADA systems are hosted on secured communication networks, comprising wide area and local area networks. The network sensors are designed to collect voltage and current measurements. The data are relayed to the main control centres, suing RTU located in the main centralised SCADA system. The topology of the dynamic systems is adjusted using the actuators operated by the RTU [36].

Field devices, such as RTU, sensors and actuators are not designed security features to project the grid against cyber-attacks.

4.2.1 Implementing testbed SCADA specific cyber-attacks

The cyber security vulnerability inside the substation can be investigated by simulating the attack in the testbed environment. The testbed design is based on a grid connected photovoltaic SCADA system.

The security focussed testbed simulation architecture of a cyber-attacks inside the substation comprises of following components [2]:

- SCADA human machine Interface.
- Database.
- Intrusion Detection System (IDS) device for monitoring network activity.
- Protocol gateway.
- IED simulation device.
- Router.
- Firewall.

Figure 4.1 and 4.2 indicate the control centre computer as part of the Scada supervisory control software hosting the substation single line diagram.

4.3 TRAFFIC SEGREGATION OF SCADA WITH FIREWALL AGAINST CYBER-ATTACK

As described in Praragraph 4.2 above, the electricity comprises a network address translation called NAT, to control and block the traffic between inside and outside interfaces. This is used to block standard network protocols such as Telnet, HTTP and FTP from entering the SCADA system and databases.Using VLAN to segregate the SCADA and broadband internet traffic, is not recommended in the power system environment.

A maintenance contract for remote access of the mission critical system such as a SCADA system is required to allow regular upgrades of firewall to protect the system againts possible cyber-attacks. Firewalls deployed for the SCADA system are not allowed for years without being maintened. As indicated in Figure 4.3, the public network is utilised to connect to the SCADA system from far remote locations. Traffic between the two sites are controlled by security polices of the two organisations. The type of the Cisco router is provided, using VPN routers from Siemens.

The firewall installed at the City of Tshwane electricity SCADA Ethernet network, is part of the security zone from the site of Siemens, providing remote maintenance support to system. It is possible to block HTTP traffic from the DMZ (demilitarised zone) to the City of Tshwane firewall. This type of security architecture is implemented to protect the SCADA against possible cyber-attacks. The DMZ is a segmentation of the network between the internal network and external network [2]. The current transmission route uses VPN connection to the system through the internet. This type of architectural design has the following benefits:

- The data transmitted on the route entertain a high-level of security.
- High availability high quality of data.
- High-level of security between DMZ and City's intranet network.
- VPN security implemented using IPSec between DMZ and City's intranet network.

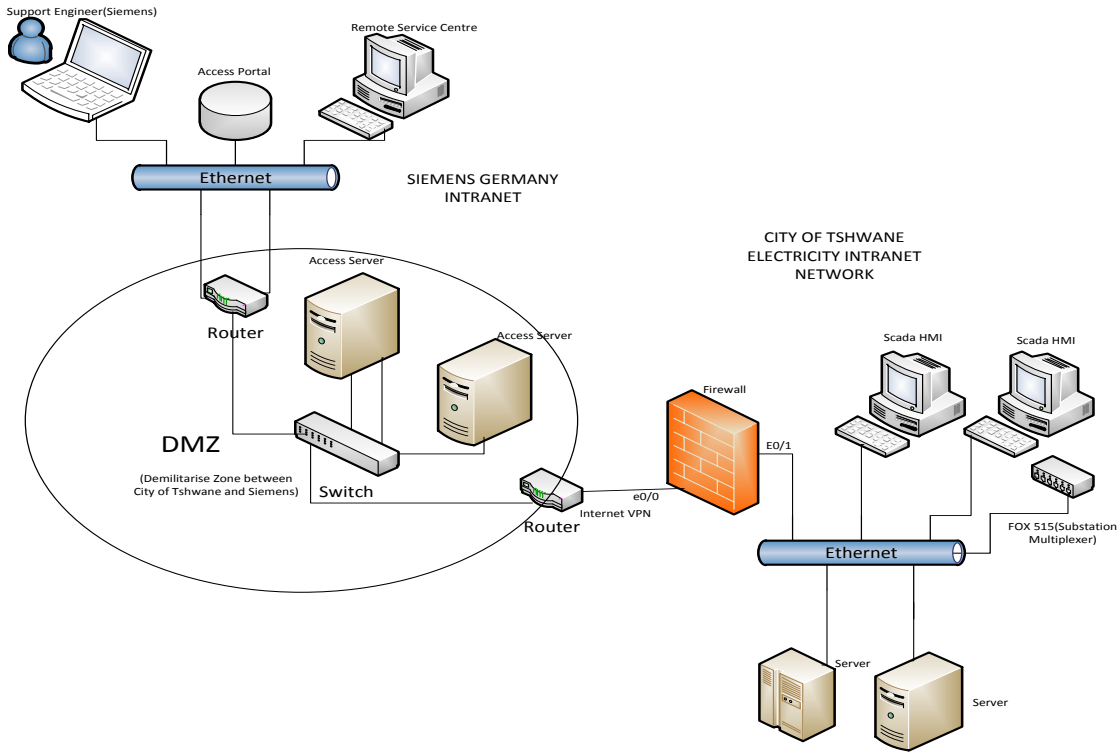

Figure 4.3. Security infrastructure of the SCADA system

The lack of adequate security mechanism such as authentication, can lead to the intruder gaining access to the SCADA system. Once the substation generators deviate from the nominal normal operation of 50Hz, the protection relays send signals to the CBs to open causing damage to the substation equipment, resulting in total power loss.

Simulation results of the intruder gaining access to the SCADA system, opening a substation breaker is shown in the Figure 4.4.

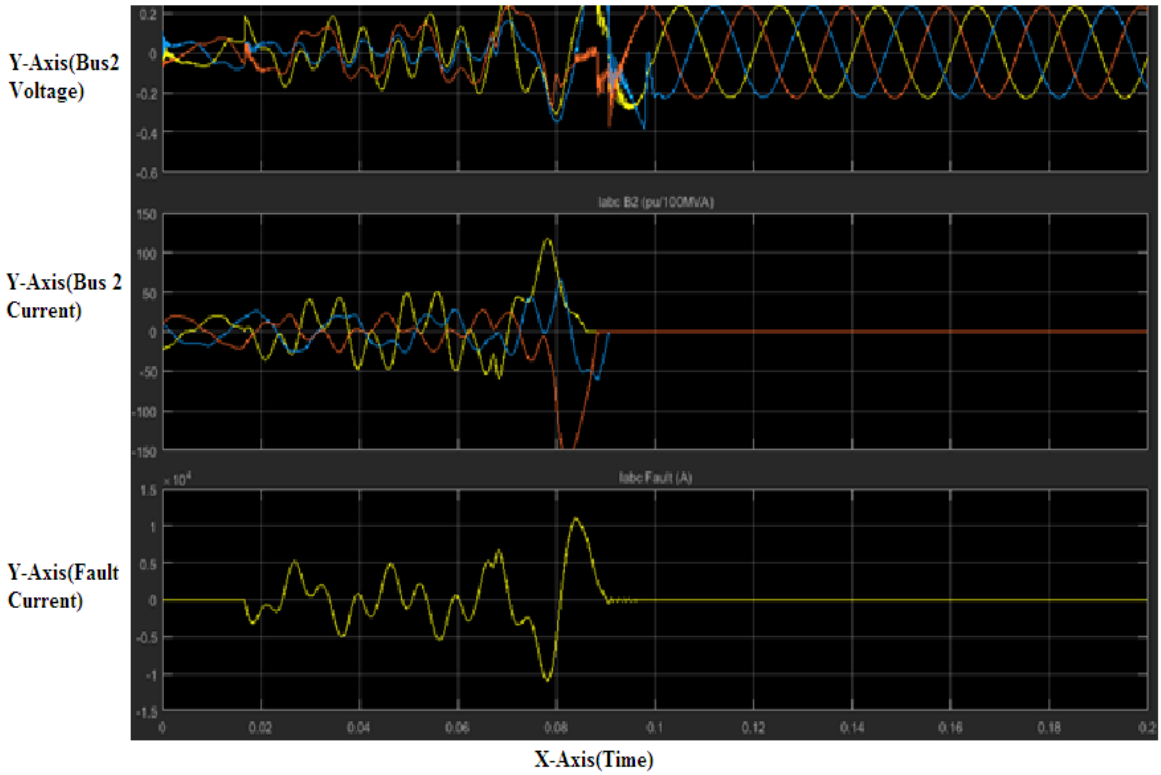

Figure 4.4. Load at B2: Load analysis simulation

The above load analysis above simulation models from the load buses. The minimum and maximum frequencies value on the load buses are indicated in Table 4.

The load at bus B2 is decreased from the initial value 42.3 MW to the maximum 84.6 MW. The graph in Figure 4.2, at load B2 show the corrupted frequencies measured in the Iabc from 0 to 0.08 seconds.

The simulation in Figure 4.5 indicates how the system responds when the load changes resulting an attack. This type of attack is described in paragraph 4.4 and is referred to as the load altering attack. The power grid generators are designed to operate at 50Hz and any

deviation from the nominal frequencies result with the failure of the CBs and protection systems.

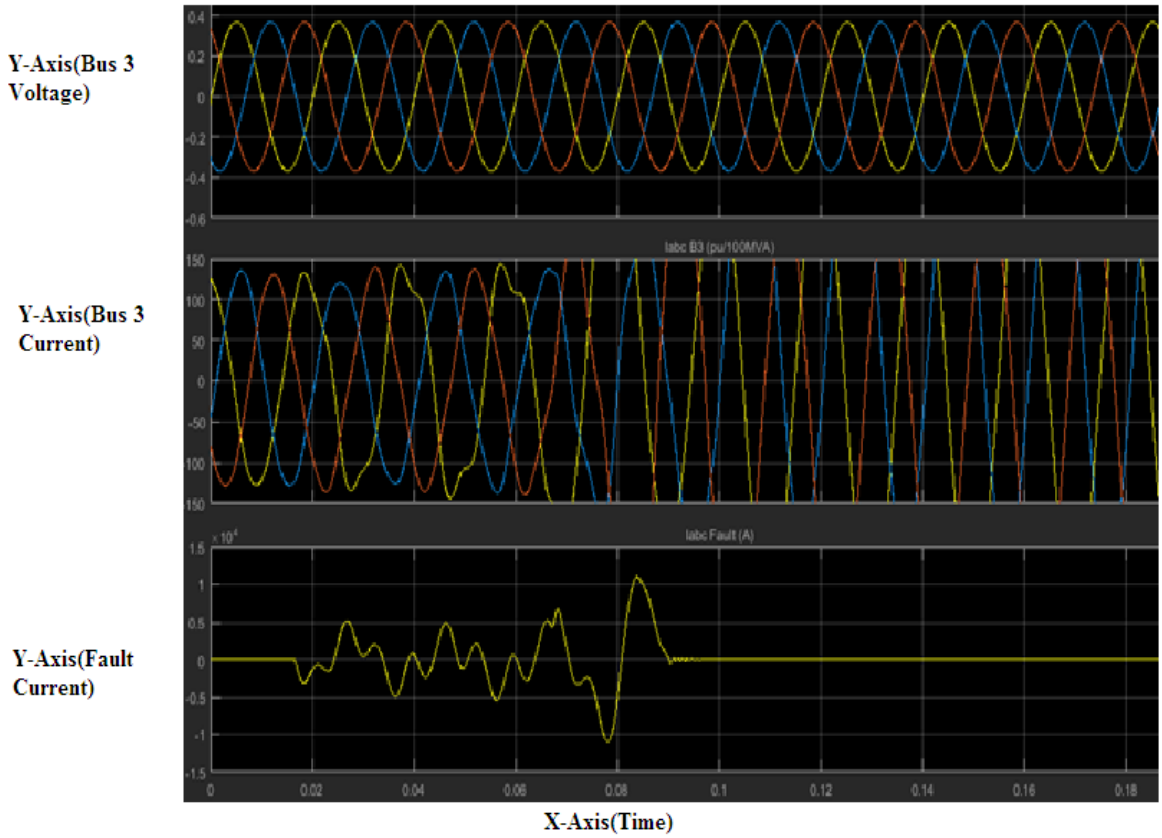

Figure 4.5. Load Analysis at B3 when the circuit breaker is closed

Several quantitative methods on the vulnerability assessment were proposed for the SCADA/EMS system. For instance, in [35], an assessment of the risk is proposed to improve the robustness of the power system against cyber-attacks [37].

4.4 HIGH-LEVEL CYBER SECURITY REQUIREMENT [38]

The main challenges faced by the smart grid deployment according to the Electric Power Research Institute (EPRI) is the cyber security of the grid system, due to the high potential of incidents of attacks against the utility sector.

It is import for the cyber security to address the risk posed by the disgruntled employees and terrorists. Organisations and power system operators need to assess applicable standards and processes within their environment. Numerous technical organisations and societies are working on the development of a standard to address the risk of the cyber-attacks.

Organisations such as the NIST, were specifically established to ensure standardisation in the domain of the smart grid systems. The draft NIST Interagency report (IR-76268) was established by the security work group to consider the requirements of security in the smart grid across all components of the grid.

The deployment cyber security in the smart grid systems requires collaboration between the industry, academia and the power system industry experts [39]. As described in the above paragraph, close collaboration with standard bodies such as NIST are important to coordinate the security of the system. This will depend on the authentication, privacy and authorisation of the private technologies. Federal Information Processing Standard (FIPS), Advanced Encryption Standard (AES), and Triple data Encryption Standard (3DES) provides the grid with high security which is readily available.

The 3DES standard will insure sooner since the lifespan of the power system grid components is prolonged. The AES will likely be the preferred for the new grids components. The IEEE 802.11 networks operating in the unlicensed frequency band and various wireless based protocols, need a varying degree of security, such as 3DES. The security required for the wired system is a firewall, IPsec and virtual private networks. The Secure Shell(SSH) and SSL/TLS operating in the higher layer should also be used to provide security.

This is advised by a synchronous attack launched from multiple locations in the network, to cause a major grid to oscillate [40]. With the development of the information security, more threats were introduced in the networks. Viruses and network threats are not the only security risks posed to the network. Data steal and destruction are the other organised threats to the system. Other types of attacks, include variable structure switching attacks facilitated by cyber-attacks, requiring the attack to have a dynamic state of the network to launch an attack in real-time [41].

The ICT layer resides on top of the smart grid system, capable of controlling smart, intelligent switches appliances, including providing integration of generations. Various system interaction is required between the Energy Management Systems (EMS), and home customers [42].

TCP/IP and Ethernet technologies in the smart grid systems, are adopted at a higher speed with the cost of the system reduced significantly. The drawback of these technologies is that they are susceptible to IP spoofing, TCP SYNC and routing attacks. In the SCADA systems, the deployment of firewalls prevents hacking and cyber intrusion. Inside substations LAN, the network remote access points used for system maintenance, security need to be increased to prevent unauthorised access. The installation of CCTV, including pepper sprayers are some of the physical security measures that can be deployed.

Denial of Service (DoS) attacks. Research work is still ongoing to minimise the impact of unauthorised access [43]. Load Altering Attacks (LAA) are type of attacks attempting to change the load of the grid, damaging the power system through circuit overflow method [44].

There various types of loads can automatically respond to price signals in the controllable scenario [45], [46]. The volume of the load can be changed by statically altering the load were the attack change the volume of the transformer or network load [47]. Segmentation of the network into smaller components could assist with limiting the impacts of malicious attacks on the network. This can prevent the spreading of the attacks on the network and monitoring of the ingress and egress network traffic [48].

CHAPTER 5 DISCUSSION

The 9/11 terrorist attacks on the United Stated, followed by the power black-out in August 2003, led to more focus directed to the NERC CIP (Critical Infrastructure Protection) [49].

The Matlab simulation techniques applied to this research, allows for the proper understanding of the IED's devices prior to their deployment in the network. The end results will be to incorporate new components with the network grows [50].

The electronic embedded devices used in cyber-physical systems and particularly in smart grid applications for monitoring and control purposes, are increasing. Various real-world examples showed that grid systems are exposed to various threats that can lead to serious implications (Stuxnet). Most of the smart grid embedded IEDs run firmware, along with the sophisticated nature of firmware modifications, render firmware attacks one of the most advanced threats on embedded devices [51].

The simulation in this work indicates launching an attack during a different timeslot, resulting load shedding for the specific interval. Load shedding is influenced by initiating an attack on the grid system by opening the power grid CB's. A fault on the power network, at time intervals are removed by the quick operation of the protection system [52].

Compared to the internet based services, strict performance criteria are required in power systems operations. The following are examples of the system reliability requirements:

- The SCADA system for grid control and monitoring (99.99%).
- A redundant grid design will continue to operate during cyber-attack.
- Security systems should be continuously tested to counter the impact of cyber-attacks.
- Testing and security do not easily influence the operations of power systems.

Logical smart grid interfaced cannot be addressed by a single cyber security. It is possible to modify the security for smart grid to perform the risk assessment categorise [53].

Legacy power grid systems integrated with the physical cyber domain, forming a large scale public telecommunication network [54]. The backbone of the City of Tshwane electricity data protection network, provides communication services to the City's internal telecommunication services for voice and internet services.

The risk of providing the grid with protection against cyber-attacks is tremendous [55] since the cost including the complexities of networking components for deployment is a challenging factor. It is also reasonable for vulnerabilities to be expected in the control and operation of the smart grid, due to their larger scale and size of the grid [56]. The safety and security of the smart grid, should always be prioritised, since the operation of the electricity network is considered as mission critical [57].

Similarly, most power grid hackers prefer using a firmware to target the RTU inside the substations after remotely opening the substation's CBs. A challenging task indicates the most severe attack on the power system network occurring when the computer terminals of electricity main control centre are destroyed, causing the restoration of the power system network after power black-out.

CHAPTER 6 CONCLUSION

The security and cyber-attack of the most important components of the smart grid was studied. The substations were modelled as smart grids using Matlab Simulink/SimPowerSystems and the load at buses Njala @ B1-700MW, Wingate @ B2-49.6 MW, Wapadrand @ B3- 57.8, Willows @ B4- 38.6 MW, Wattloo @ B5- 46 MW were reduced with the launch of a cyber-attack. Remote load shedding of the grid is affected by opening the circuits breakers. The results simulated the cyber-attack using Matlab/SimPowerSystems indicates being useful to analyse the influence of the cyber-attack on a smart grid network.

The study also examined the role of cyber-attacks on the selected number of substations forming part of the City of Tshwane power grid. For each type of attack, the characteristics response of the grid is analysed with the results displayed as graphs. The outcome of the study can be summarised.

- SimPowerSystems library components in Matlab can be used to simulate and analyse a smart grid cyber – Attacks. Harmonics, load and other electrical power system assisted investigating the performance of the designed model [58]
- More research is needed to integrate and include the IEC61850 relays into model. This can only be achieved once the telecommunication libraries are included into the Matlab systems.

Long-term attacks on the power system have a wider impact on the network, and the normal faults introduced on the power system can be severe if contingency is not implemented [59]

This research shows that an assailant can hack into the communication and alter the relay settings of the of the power system inside the substations. This may trigger cascading effects, resulting in the major power outages that can be catastrophic if the major in-feed 275KV substations relays are altered.

The results of attacks on the system were analysed how the system perform theoretically and all the theoretical analysis validated using Matlab/SimPowerSystem simulations. Simulating the behaviour of the power system is challenging because the electrical power system is complicated and comprises multiple components such as relays, telecommunications equipment, electronic components, RTU and sensors. Integrating each of these components into a single layer to analyse the power systems behaviour, require many simulations to be executed, being complex and a challenging.

The analysis of cyber-attack can be extended to include the most critical components of the substations. Attacks can also be initiated by hacking more loads in the substations, using LAA. The voltage and current stability of the grid was varied by dropping the substation load to simulate an attack. Frequency variation indicated another method used in the simulation, were the power grid frequency was deviated from its normal operation.

REFERENCES

[1] J. Liu, Y. Xiao, S. Li, W. Liang and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grid, in *IEEE Communications surveys and tutorials*, vol. 14, 4th ed. pp.1-2, 31 January 2012.

[2] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks," IEEE Transaction on Power Delivery, Year: 2014, Volume 29, Issue:3 Pages: 1092-1102.

[3] Md. M. Hasan and Hussein T. Mouftah, "Optimal Trust System Placement in Smart Grid SCADA Networks", in *IEEE Access*, vol. 4, no. 1, pp. 2907 – 2919, 09 May 2016.

[4] U. A. Khan, J. K. Seong, S. H. Lee, S. H. Lim and B. W. Lee, "Feasibility Analysis of the Positioning of Superconducting Fault Current Limiters for the smart grid Application Using Simulink and SimPowerSystem," in *IEEE transactions on applied superconductivity*, vol. 21, no. 3, pp. 2165-2169, June 2011.

[5] V. Kumar and P. Rai, "Active Power Analysis of a Smart Grid- Using MATLAB/SIMULINK Approach", *International Journal of Innovative Research in Advanced Engineering*, Vol 1 (Issue 8), pp. 397- 403, September 2014.

[6] F. Clevelland, (2012, June) "IEC 62351 Security standard for the power system information infrastructure" Last accessed: Sept. 2016, [Online]. Available:

http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf.

[7] L. Langer, F. Skopik, P. Smith and M. Kammerstetter, "From old to new: Assessing cybersecurity risks for an evolving smart grid," Computers & Security, Volume 62, September 2016, Pages 165-176.

[8] Z. Pan, Q. Xu, C. Chen and X. Guan "NS3-MATLAB Co-Simulator for Cyber-physical Systems in Smart Grid", in *Proceedings of the 35th Chinese Control Conference, Chengdu, China*, pp. 9831 - 9836, 27-29 July 2016.

[9] Y. Jia, Z. Xu, Loi L. Lai, K P. Wong, "Risk-Based Power System Security Analysis Considering Cascading Outages," IEEE Transactions on industrial Informatics, Year 2016, Volume 12, Issue:2, Pages 872-882.

[10] R. Deng, P. Zhuang, H. Liang, "CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid," IEEE Transactions on Smart Grid, Year:2017, Volume:8, issue: 5, Pages 2420-2430.

[11] N. Komninos, *Member,* E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," IEEE Communication Surveys and Tutorials, Year: 2014, Volume 16., Issue: 4, Pages 1933 - 1954

[12] T. Mander, F. Nabhani, L. Wang and R. Cheung "Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security," in *IEEE Power Engineering Society General Meeting*, pp. 8-9, 23 July 2007.

[13] G. N. Ericsson, "Cyber Security and Power System Communication- Essential Parts of a smart grid Infrastructure," in *IEEE Trans on Power Delivery*, vol. 25 No. 3, pp. 3-7, 3 July 2010.

[14] C. Jian, C. Yanbo, Z. Lihua, "Design and Research of Off-grid Wind-Solar Hybrid Power Generation Systems", in *Power Electronics Systems and Applications (PESA), 4th International Conference*, pp. 1-5, 8-10, June 2011.

[15] Y. Wang, D. Ruan, D. Gu, J. Gao, D. Liu, J. Xu, F. Chen, F. Dai and J. Yang "Analysis of smart grid Security Standard" in *Computer Science and Automation Engineering (CSAE) IEEE International Conference*, vol. 4, 2011, pp. 697-701, 14 July 2011.

[16] V. Urias, B. Van Leeuwen, and B. Richardson,"Supervisory Command and Data Acquisition (SCADA) system Cyber Security Analysis using a Live, Virtual, and Constructive (LVC) Testbed," in *IEEE Military Communication Conference*, pp.1-8, 28 January 2013**.**

[17] R. Samdarshi, N. Sinha and P. Tripathi, "A Triple Layer Intrusion Detection System for SCADA Security of Electric Utility ", in *India Conference (INDICON), IEEE*, pp. 1-5, 17-20 December 2015.

[18] C. Jian, C. Yanbo and Z. Lihua, "Design and Research of Off-grid Wind-Solar Hybrid Power Generation Systems", in *Power Electronics Systems and Applications (PESA), 4th International Conference*, 2011, pp. 1-5, 8-10 June 2011.

[19] F. Clevelland, (2012, June) "IEC 62351 Security Standard for the Power System Information Infrastructure" Last Accessed: Oct. 2015, [Online]. Available: http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf

[20] M. Wagner, M. Kuba and A. Oeder, "Smart grid Cyber Security: A German Perspective" in *2012 International Conference on smart grid Technology, Economics and Policies, International Conference, Short Course and Table top Exhibition*, pp. 1-4, 24 October 2014.

[21] N. Ericsson, "Cyber Security and Power System Communication- Essential Parts of a smart grid Infrastructure," in *IEEE Trans on Power Delivery*, vol. 25 No. 3, pp. 3-7, 3 July 2010.

[22] J. Farquharson, A. Wang and J. Howard, "Smart Grid Cyber Security and Substation Network Security", in *IEEE PES Innovative Smartgrid*, pp. 3, 2011. pp. 1-5, 16-20 January 2012.

[23] T. Baker, M. Mackay, A. Shaheed and B. Aldawasari "Security-Oriented Cloud Platform for SOA-Based SCADA", in *966, 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2015, 4-7 May 2015.

[24] R. Dodge, C. Carver and A. Ferguson, "Phishing for user security awareness" *Computers & Security*, vol. 26, no. 1, pp. 73–80, Feb. 2007.

[25] Electric Grid Vulnerability: Industry Responses Reveal Security Gaps. Last Accessed 21 May 2013, [Online]. Available: https://arpa.energy.gov/sites/default/files/documents/files/REBELS_ProgramOverview.pdf

[26] H. Karbouj and S. Maity, "On Using TCBR Against Cyber Switching Attacks on Smart Grids", *IEEE Innovative smart grid Technologies - Asia (ISGT-Asia)* Melbourne, Australia, pp. 665-669, 28 November 28 – 1 December 1 2016.

[27] J. Wei and G. J. Mendis "A Deep Learning-Based Cyber-Physical Strategy to Mitigate False Data Injection Attack in Smart Grids", *IEEE Innovative smart grid Technologies - Asia (ISGT-Asia)*, pp. 1-6, 12 April 2016.

[28] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, A. Selcuk Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," IEEE Communications Surveys & Tutorials, Year:2017, Volume:19, Issue: 1, Pages 446 -464.

[29] X. Liu, M. Shahidehpour, *Z.* Li, and Y. Cao, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems", *IEEE Transactions on smart grid* Volume 8: Issue 2, pp. 572 - 580, March 2017.

[30] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy "Denial of Service Attacks in Wireless Network: The Case of Jammers," *IEEE Communications surveys and Tutorials*, vol. 13, no. 2, pp. 245 - 257, 2011

[31] S. Liu, X. P. Liu and A. Saddik, "Denial-of-Service (DoS) Attacks on Load Frequency Control in Smart Grids", *Innovative smart grid Technologies (ISGT),* IEEE PES, pp. 1–6, 24-27 February 2013**.**

[32] S. Liu, X. P. Liu, A. Saddik, "Denial-of-Service (DoS) Attacks on Load Frequency Control in smart grids", Innovative smart grid Technologies (ISGT), IEEE PES, Page(s): 1 – 6, 24-27 Feb. 2013.

[33] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li and L. Song, "Bad Data Injection in Smart Grid: Attack and Defence Mechanisms", Cyber Security for Smart grid Communications, vol. 51, (Issue 1), pp. 27-33, 04 January 2013**.**

[34 X. Liu and Z. Li, "Trilevel Modelling of Cyber Attacks on Transmission Lines", *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720-729, March 2017.

[35] W. Kehe, Z. Tong and L. Wei, "Research and Design of Security Defence Model in Power Grid Enterprise Information System" *Multimedia Technology (ICMT), International Conference*, 2010, pp.1-4, 29-31 October 2010.

[36] H. He, J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," IET Cyber -Physical Systems; Theory and Applications, Year 2016, Volume: Issue 1, Pages: 1-27

[37] Y. Zhang, Y. Xiang and L. Wang, "Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems", *IEEE Transactions on Smart Grid*, Volume: PP, Issue: 99, pp. 1-15, 12 February 2016.

[38] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for smart grid Communications" in *IEEE Communication Survey and Tutorial*. vol.14, No 4, Fourth Quarter 2012. pp. 998-1010, 31 January 2012**.**

[39] P. Kaster, P. K. Sen, "Power Grid Cyber Security: Challenges and Impacts", *IEEE* North American Power Symposium (NAPS), pp. 1-6, 7-9 Sept. 2014**.**

[40] B. Geng and C. Siaterlis, "Developing Cyber-Physical Experimental Capabilities for the Security Analysis of the Future smart grid" in *Innovative smart grid Technologies (ISGT Europe), IEEE PES International Conference*, 2011, pp. 1-7, 5 March 2012

[41] W. Kehe, Z. Tong, L. Wei, "Research and Design of Security Defence Model in Power Grid Enterprise Information System" in *Multimedia Technology (ICMT), International Conference*, 2010, pp. 1-4, 29-31 October 2010.

[42] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos and K. L. Butler-Purry, "A smart grid Vulnerability Analysis Framework for Coordinated Variable Structure Switching Attacks", in *IEEE Power and Energy Society Meeting*, pp. 1-6, 12 November 2012**.**

[43] H. Holm, W. R. Flores and G. Ericsson, "Cyber Security for a smart grid –What About Phishing?", *IEEE PES Innovative smart grid Technologies Europe (ISGT Europe), Copenhagen*, IEEE, 2013, pp. 1-5, 6-9 October 2013**.**

[44] S. Amini, H. Mohsenian-Rad and F. Pasqualetti, "Dynamic Load Altering Attacks in smart grid", *IEEE Power and Energy Society Innovative Smart grid*, pp. 1-5, 18-20 February 2015.

[45] H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. on smart grid*, vol. 2, no. 4, pp. 667–674, December 2011.

[46] H. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. Leon- Garcia, "Autonomous Demand Side Management Based on Game- Theoretic Energy Consumption Scheduling for the Future smart grid," *IEEE Trans. on smart grid*, vol. 1, no. 3, pp. 320–331, December 2010.

[47] H. Mohsenian-Rad and A. Leon-Garcia, "Optimal Residential Load Control with Price Prediction in Real-Time Electricity Pricing Environments," *IEEE Trans. on smart grid*, vol. 1, pp. 120-133, September 2010.

[48] M. Ghamkhari and H. Mohsenian-Rad, "Energy and Performance Management of Green Data Centers: A Profit Maximization Approach*," IEEE Trans. on smart grid*, vol. 4, no. 2, pp. 1017-1025, June 2013.

[49] S. J. Baird, S. Flynn, B. F. Hawkins and A. J. Mackrell, "Integrated Protection and Control Communications outwith the Substation: Cyber Security Challenges" in *Developments in Power System Protection, IET 9th International Conference*, page(s): 698 – 70, IEEE, 2008, pp. 691-701, 2 May 2008.

[50] J. Ren, and M. Kezunovic, "Modelling and Simulation Tools for Teaching Protective Relaying Design and Application for the smart grid", *Modern Electric Power Systems* 2010, Wroclaw, Poland, pp. 1-8, 20-22 Sept. 2010.

[51] C. Konstantinou and M. Maniatakos, "Impact of Firmware Modification Attacks on Power Systems Field Devices", *IEEE International Conference on smart grid Communications (SmartGridComm): Cyber Security and Privacy*, 2015, pp 283-288, 2-5 November 2015**.**

[52] G. Nicolaescu, H. Andrei and S. Radulescu, "Modelling and Simulation of Dynamic Voltage Restorer for Voltage Sags Mitigation in Medium Voltage Networks with Secondary Distribution Configuration", in *Optimization of Electrical and Electronic Equipment (OPTIM)" IEEE,* 2014, pp.52-58, 22-24 May 2014**.**

[53] NIST7628: The smart grid Interoperability Panel cyber Security Working Group, http://www.nist.gov/smart grid/upload/nistir-7628_total.pdf / (Accessed 21 February 2016).

[54] D. V. Dollen, "Report to NIST on the smart grid interoperability standards roadmap," *Tech. Rep., Electric Power Research Institute (EPRI),* 2009, [Online]. Available: http://www.nist.gov/smart grid/upload/Report to NIST August 10 2.pdf.

[55] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on smart grid*, vol. 1, no. 1, pp. 99-107, 2010.

[56] X. Fang, S. Misra, G. Xue, and D.Yang, "Smart Grid The New and Improved Power Grid: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[57] Guidelines for smart grid Cyber Security, The SmartGrid Interoperability Panel: Cyber Security Working Group, Gaithersburg, Md, USA, 2010. [Online]. Available: https://www.nist.gov/sites/default/files/documents/smart grid/nistir-7628_total.pdf

[58] SimPowerSystems, 2014, Last Accessed: Nov 2014. [Online]. Available: https://www.mathworks.com/products/simpower.html/

[59] H. Holm, W. R. Flores and G. Ericsson, "Cyber Security for a smart grid –What About Phishing?", *IEEE PES Innovative smart grid Technologies Europe (ISGT Europe), Copenhagen*, IEEE, 2013, pp. 1-5, 6-9 October 2013.

APPENDIX A

Table 1.0 List of research outputs published in international journals and available in the web

No	Journal Name	IEEE Journal	Free Web Access	Internal Conferences	IJIRAE Journal	Science Direct	IET Journal
1	IEEE Communications surveys and tutorials	X					
2	IEEE Access	X					
3	IEEE transactions on applied superconductivity	X					
4	International Journal of Innovative Research in Advanced Engineering				X		
5	IEC 62351 Security standard for the power system information infrastructure		X				
6	IEEE Power Engineering Society General Meeting	X					
7	IEEE Trans on Power Delivery	X					
8	Computer Science and Automation Engineering (CSAE)			X			
9	Proceedings of the 35th Chinese Control Conference			X			
11	Power Electronics			X			

	Systems and Applications (PESA)						
12	IEEE Military Communication Conference			X			
13	India Conference (INDICON), IEEE			X			
15	International Conference on smart grid Technology			X			
17	IEEE PES Innovative Smartgrid	X					
18	IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing	X					
19	Electric Grid Vulnerability		X				
20	IEEE Innovative smart grid Technologies			X			
22	IEEE Transactions on smart grid	X					
24	Innovative smart grid Technologies (ISGT)	X					
25	IEEE PES	X					
26	Cyber Security for Smart Grid Communications	X					
28	Multimedia Technology (ICMT)			X			
30	IEEE Communication Survey and Tutorial	X					

31	North American Power Symposium (NAPS)			X			
32	Innovative smart grid Technologies (ISGT Europe)	X					
34	IEEE Power and Energy Society Meeting			X			
35	IEEE PES Innovative smart grid Technologies Europe (ISGT Europe)			X			
37	IEEE Trans. on smart grid	X					
39	Developments in Power System Protection			X			
40	IEEE International Conference on smart grid Communications (SmartGridComm)			X			
41	NIST7628		X				
42	EPRI		X				
46	Guidelines for smart grid cyber Security		X				
47	SimPowerSystems		X				
48	Computers and Security					X	
49	IEEE Transactions on industrial Informatics	X					
50	IET Cyber -Physical Systems						X