CYBER-POWER SYSTEM ANALYSIS USING A REAL TIME TEST BED

By

CEEMAN BRIGHTSON VELLAITHURAI

A thesis submitted in partial fulfillment of
the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

WASHINGTON STATE UNIVERSITY
School of Electrical Engineering and Computer Science

JULY 2013

To the Faculty of Washington State University:

The members of the Committee appointed to examine the thesis of CEEMAN BRIGHTSON VELLAITHURAI find it satisfactory and recommend that it be accepted.

_____

Anurag K. Srivastava, Ph.D., Chair

_____

Anjan Bose, Ph.D.

_____

Carl H. Hauser, Ph.D.

ACKNOWLEDGEMENTS

I would like to extend my gratitude to Dr. Anurag K Srivastava, who as the committee chair and advisor has been the guiding force behind this thesis. I would also like to thank my committee members Dr. Anjan Bose and Dr. Carl Hauser for their assistance. I thank all my friends with whom I have worked in the laboratory and others outside of the laboratory who have provided support. I would like to thank Doug McGinnis for his valuable inputs.

I would like to acknowledge my family members, especially my parents Vellaithurai and Santhana Mary, who have been constantly providing support and encouragement throughout my studies. Special thanks to my brother Sylvester Pious for his support. I would also like to thank my grandparents Rajendran and Gnana Arputham for their support over the years.

I would like to acknowledge and thank all the sponsors of the Smart Grid Demonstration and Research Investigation lab, especially to Trustworthy Cyber Infrastructure Power Grid funded by Department of Energy and Department of Homeland Security.

CYBER-POWER SYSTEM ANALYSIS USING A REAL TIME TEST BED

ABSTRACT

By Ceeman Brightson Vellaithurai, M.S.
Washington State University
July 2013

Chair: Anurag K. Srivastava

The Electric Power System (EPG) has been identified as one of the most critical infrastructure that is considered to be vulnerable to cyber-physical attacks. With the emphasis on making the grid "smarter", there have been an increase in the deployment of several smart devices in the power grid, and automation of the power system has received a major investments. It is necessary to consider the interdependencies of cyber and physical networks for cyber-power system analysis with increasing automation. Applications and algorithms developed for the smart grid need to be tested and evaluated using an integrated cyber-physical test bed. This work relates to cyber-power system analysis using developed real time test bed utilizing the Real Time Digital Simulator (RTDS) and Network Simulator 3 (NS3) supported by other software and hardware resources. Integration of network simulator with power system simulator indicates that communication links are generally not a bottleneck for wide area monitoring and control. Results from the simulation of an Aurora type of attack on a generator using the test bed indicate that the generator is likely to suffer mechanical damage, if the attack is successful. Real time simulation results for micro-grid reconfiguration and voltage stability of transmission grid using the developed cyber-physical test bed provides insight for implementation of these specific applications.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The basic structure of the Electric Power Grid (EPG) has not changed drastically over the last few decades. Several blackouts over the past few decades demonstrated the vulnerability of EPG and pointed the need for continued improvements [1.1]. The management and control of EPG has room for improvement to provide automated analysis, better visibility and situational awareness. The smart grid has evolved over the years to help with this major upgrade needed for the EPG. The smart grid concept is a major upgrade in EPG infrastructure for improved efficiency, reliability and sustainability, with integration of renewable and alternative energy sources, through automated control and modern automated technologies [1.2]. Some of the technology to support smart grid includes Phasor Measurement Units (PMU), Digital Fault Recorders (DFR) and smart meters for measurements, wired and wireless communication technology for data transfer, and distributed and parallel computing for fast analysis of data using various applications. With data available at a faster rate and control possible within 10s of milliseconds in the system, the scope for development of applications and algorithms to be used in the EPG has widened.

The increase in number of digital devices and flow of data in the network due to the thrust towards a smarter grid has shifted the focus to cyber-security of the EPG. It is appealing to assume that existing cyber solutions can be directly applied to the EPG. Unfortunately, due to the idiosyncrasies of the power grid, this is not a possibility. The disruptions due to a cyber-attack on the smart grid transcend the cyber realm and affect the physical realm as well. This means that the approach to security of the smart grid has to bring both cyber security and system security under the same name of Cyber-Physical Security

(CPS) [1.3]. It is important to test algorithms, devices and applications to be deployed in the smart grid under the notion of CPS. To enable testing of such devices and applications, there is a need to prototype and simulate the actual operating conditions with sufficient detail and accuracy. To carry out testing of applications and related objectives, this work explores the possibility of setting up a cyber-physical test bed using the Real Time Digital Simulator (RTDS) and Network Simulator 3 (NS3) along with supporting software and hardware resources.

1.2 Overview of Electric Power Grid

The EPG consists of four major components: Generation, Transmission, Distribution, and Load. Generation facilities are usually located in remote places where the fuel needed for production of electric power such as fossil fuels such as coal, nuclear, geothermal etc. is easier to access. At the point of generation, the voltage levels are lower, and usually between 10 kV to 15 kV. Transmission and distribution systems are designed for carrying the electric power from the point of generation to the point of use, which is the load center's located away from generation sites. In order to reduce losses, the voltage is stepped up to higher levels of up to 765 kV and above to enable transmission of power long distances with minimum losses. The Transmission system usually represents voltage levels above 132 kV [1.4]. There are different voltage levels based on requirements, which are usually influenced by the cost involved in laying towers and the environment in which they are to be laid. The transmission system has a higher permeation of smart devices and meters. The distribution system involves voltage levels below 33 kV. Generally, the distribution system has poor visibility due to the low level of automated metering present today. However, this is fast changing with the deployment of advanced smart metering infrastructure as part of the smart grid initiative. Load centers may draw power from the sub-transmission or distribution levels in the system depending on the requirement. Sub-transmission level load centers are typically industrial

users and the kV range is 33 to 132 kV [1.5]. The power system has to maintain a balance between the electric power generated and consumed in the system. It is governed by a simple equation defined as:

$$P_{generation} = P_{load} + P_{losses} \quad (1.1)$$

This is necessary to maintain synchronization and reliability of the power grid. Figure 1.1 shows a simple representation of the power system [1.4].

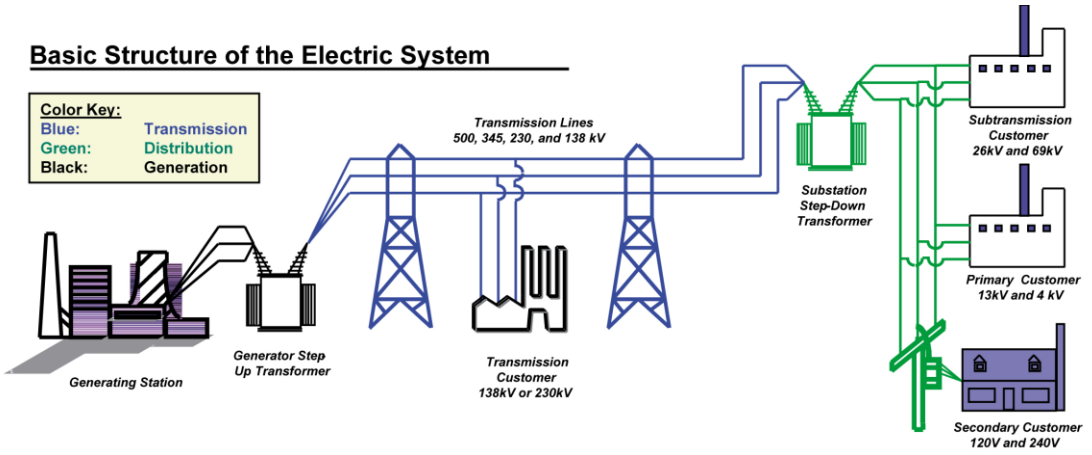

Figure 1.1: Basic structure of the EPG

The power system can be visualized as a network of interconnected nodes. The nodes represent physical locations in the system and the interconnections represent the transmission lines in the system. A node/bus may have generation, load, both, or neither. Apart from these additional devices may be employed to keep the voltage levels in the system with operable limits. One of the examples is Flexible AC Transmission System (FACTS) devices [1.6], which are usually power electronics devices which control voltage or current through absorbing/supplying reactive power.

The primary aim of the EPG is to reliably supply load centers through high level of continuity of service while minimizing the extent of supply loss resulting due to a power outage from contingencies. In order to do this, several metering and protection devices are

installed throughout the power system. Control systems and operational procedures such as the N-1 contingency security criteria exist to ensure power system reliability. Protective relaying is another example of local control which is used to monitor and isolate faulty parts of the system. Reliability and economical operation could be two contradicting objectives as reliability usually requires an increase in redundancy of the system. Redundancy in a power system may relate to spinning reserve maintained to serve the system in case of sudden increase in load, installing additional metering equipment to provide redundant measurements for monitoring or as back up for failure etc. The North American power grid involves more than 3500 utility organizations [1.7]. Inter working of these utilities is a major challenge as the limitation of communication network in the power grid, and the constraint in deployment of different control systems has led to inadequate situational awareness for utility operators who have inefficient information to disturbances in neighboring control areas. In the United States, the North American Electric Reliability Corporation (NERC) is responsible for ensuring the reliability of the North American bulk power system, and with help of eight regional entities that enforce standards and reliability compliance. While a non-governmental entity, the Federal Energy Regulatory Commission (FERC) had designated NERC the electric reliability organization for the United States, which effectively grants NERC legal authority to enforce energy standards in the U.S.

1.3 Cyber-Physical Vulnerability of Power System

The vulnerability of EPG cannot be assessed as two separate metrics: cyber vulnerability and physical vulnerability. In a power system, the compromise of a cyber-asset such as a control, protection, or monitoring device or system by an attacker maybe used to cause outage/damage to the physical power system components such as generators/transformers. It may take a long time to replace/bring these devices back to service. Successful cyber-attacks typically make use of vulnerability in the communication

protocol, routing, or authentication of a cyber-asset to install malware, deny legitimate services, or directly intrude into an information system [1.8]. The level of physical consequences due to a cyber-attack is dependent on the nature and depth of the attack. It is possible that the compromise of a cyber-asset may have no bearing on physical equipment.

1.3.1 Motivation for Cyber Security

Over the past few years, there have been several numbers of events reported for industrial control systems vulnerability and victims of cyber-attacks. In March 2007, Idaho National Laboratory conducted an experiment in which physical damage was caused to a diesel generator through the exploitation of a security flaw in its control system by disabling the sync check element in the protective relay [1.9]. More on the Aurora attack demonstration is discussed in section 1.4.5. In 2008, during the Russian-Georgian war, cyber-attacks widely believed to have originated in Russia brought down the Georgian electric grid during the Russian army's advance through the country [1.10]. In April 2009, the Wall Street Journal reported that cyber spies had penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. The most significant of cyber-attacks on industrial control systems was Stuxnet, which happened in 2010 [1.11]. Stuxnet, a large complex piece of malware with many different components and functionalities, targeted Siemens industrial control systems and exploited four zero-day vulnerabilities running Windows operating systems. As a result, 60 percent of Iranian nuclear infrastructure was targeted, hence triggering genuine fear over the commencement of cyber warfare. It is therefore of utmost importance to address the cyber security aspect of the smart grid, specifically the area concerned with the communication mechanisms [1.12].

1.3.2 Cyber Security Requirements

In general, the cyber security requirements of a system deployed in response to cyber threats includes three main properties: confidentiality, integrity and availability [1.3]. These three properties are designed around the cyber paradigm and are not directly applicable from

a cyber-physical system security point of view. However, these properties help in establishing basic security requirements. Confidentiality prevents an unauthorized user from obtaining secret or private information. Integrity prevents an unauthorized user/attacker from modifying the information. Availability ensures that a resource is available to the legitimate user when needed. Table 1.1 shows the relative importance of the cyber properties for price information, control commands, and meter data [1.3]. It is to be noted here that there are/will be several types of data/information flow in the smart grid apart from these three also.

Table 1.1: Importance of cyber properties for price, control and meter data

	Price Information	Control Command	Meter Data
Confidentiality	Low	Low	High
Integrity	High	High	High
Availability	High	High	Low

1. Confidentiality

   The requirement of confidentiality pertains to preventing unauthorized disclosure/access of information. In the power grid, confidentiality of meter data is important, because power usage data can provide information about the usage pattern of market participants, which can reveal personal activities through non-intrusive appliance monitoring. Additionally in a competitive market environment, by studying the usage pattern it might be possible to gain monetary benefits. Confidentiality of price information is not important when the information is publicly available. It is to be noted that the confidentiality of the software should not be critical, because the security of the system should not rely on the software, but on secrecy of the keys used [1.3].

2. Integrity

   Integrity of data pertains to the prevention of unauthorized modification/destruction of data in the system. The potential impacts on the power system due to a loss of data integrity, especially of protective control commands and metering data can be devastating due to the physical damage that could happen. For

example, measurement data can be modified to reflect that the system is in stable condition while in reality the system might be heading towards a collapse. Conventional methods of ensuring integrity require message authentication codes (MAC) be appended to the end of messages, which can be decoded by a receiver with some manner of shared authentication key to validate integrity [1.13]. Integrity of software is critical in a smart grid since compromised software can be used to control device components which are associated with the compromised software.

3. Availability

Availability is the requirement associated with the availability of the system resources for a legitimate user [1.14]. Denial-of-Service (DoS) attacks are resource consumption attacks that send fake requests to a server or a network, and the Distributed DoS (DDoS) attacks are accomplished by using distributed resources. In smart grid, availability of data and information is a key aspect. Availability of pricing information is particularly important due to serious financial implications and has the ability to affect demand adversely. Time critical operations such as control commands to and from protective relays require high availability. Automatic generation control (AGC) systems at an energy control center generally perform as the secondary control function of maintaining generator output to match changing demand [1.15]. If a cyber-attack were to deny availability of the communication system used for monitoring, processing, and control functions between remote assets and an energy control center, the AGC would have difficulty coordinating generator operations needed to maintain a stable system frequency. Additionally, if a cyber-attack were to remove generators from service through an Aurora type of attack [1.16-1.17], generation units would be rendered unavailable until repaired. The loss of generating units available for dispatch would constrain the ability of an AGC to

maintain system stability. Due to the Cyber-Physical nature of the power grid, a cyber-attack involving destruction of equipment can result in loss of availability.

1.3.3 Classification of Cyber Attackers

In general, attackers are classified into two basic groups: Insider and Outsider. Table 1.2 gives the taxonomy of cyber attackers [1.18]. For each of the adversary types, the corresponding skill levels, maliciousness, motivation and methods are listed.

Table 1.2: Taxonomy of cyber-attackers

Adversary Class	Skills	Maliciousness	Motivation	Method
script kiddies, newbies, novices	very low	low	boredom, thrill seeking	Download and run already-written hacking scripts known as "toolkits".
hacktivists, political activists	Low	moderate	promotion of a political cause	engage in denial of service attacks or defacement of rival cause sites
cyber punks, crashers, thugs	Low	moderate	prestige, personal gain, thrill seeking	write own scripts, engage in malicious acts, brag about exploits
insiders, user malcontents	moderate	high	disgruntlement, personal gain, revenge	uses insider privileges to attack current or former employers
coders, writers	High	moderate	power, prestige, revenge, respect	write scripts and automated tools used by newbies, serve as mentor
white hat hackers, old guard, sneakers	High	very low	intellectual gain, ethics, respect	non-malicious hacking to help others and test new programming
black hat hackers, professionals, elite	very high	very high	personal gain, greed, revenge	sophisticated attacks by criminals/thieves; involved in organized crime
cyber terrorists	very high	very high	ideology, politics, espionage	state-sponsored, well-funded cyber-attacks against enemy nations

1. Low Skill Level Hackers

This is the least sophisticated category of adversaries. The attackers in this category are comprised of individuals with limited programming skills. This category

includes script kiddies, cyber thugs, hactivists etc. Script kiddies are new to hacking and rely on pre-written scripts known as “toolkits” in their exploits; examples of these include NeoSploit, WebAttacker, and IcePack [1.19]. With the increasing sophistication of the available toolkits, their ability to pull off larger-scale attacks is on the rise, as in the case of the denial-of-service attacks perpetuated by “Mafia Boy” in Canada [1.20]. Hactivists/Political Activists are different than the other classes in that they are motivated by a political cause rather than a form of personal gain. Their attacks consist primarily of denial of service and defacement attacks against the sites of rival organizations, though they have also been known to employ worms and viruses [1.21]. Cyber thugs are adversaries who have similar motivations but greater skills than those in the script kiddies category. They are capable of writing their own (limited) scripts and engaging in malicious acts such as spamming, defacing, and identity theft.

2. Sophisticated Hackers and Coders

This category includes coders, writers, sneakers, professional, and the elite. Coders and writers are attackers, who are primarily involved in writing the codes and exploits that are used by others, especially those in the low skill level category. Professional and elite, as the name suggests are professional criminals, who use their technical skills in pursuance of their criminal activities. Rather than seeking fame, they prefer to lay low and evade authorities. These hackers are both rare and very dangerous, as they have strong technical skills and are often able to support themselves through their criminal exploits. Such adversaries are often employed by organized crime. Although this is one of the most dangerous types of cyber adversaries, it is also the one about which the least is known [1.20].

3. Cyber Terrorists

The most dangerous and skilled of all cyber attacker classes, cyber terrorists engage in state-sponsored information technology warfare. Their job is to conduct attacks that destabilize, disrupt, and destroy the cyber assets and data of an enemy nation or government organization. Attacks by cyber terrorists are typically well-funded and highly secretive; individuals engaging in such activities have extremely high skills and are motivated by ideology. One of the best known examples of such terrorism occurred in Estonia in 2007, following the removal of a Russian World War II monument; a massive denial of service attack crippled the websites of Parliament, several national newspapers, and the central bank [1.22]. A similarly crippling Distributed Denial of Service (DDoS) attack preceded the conflict between Russia and the Republic of Georgia in 2008 [1.23]. Such attacks are hard to prosecute, which makes them even more dangerous, and guarding against these attacks has become a top national priority.

1.3.4 Classification of Cyber Attacks on Power System

Now that a classification of cyber attackers has been established, we will look into a brief classification of cyber-attacks. The cyber-attacks can be broadly classified into three categories with a view of the confidentiality, integrity and availability paradigm: Corruption of Information, Theft of Information, and Denial of Service.

1. Corruption of Information

This cyber-attack classification covers loss of confidentiality, integrity, and availability. In this type of attack, an unauthorized user is able to acquire, modify or destroy data in the system. Altering of information results in issues in acquisition devices such as Remote Terminal Units (RTU), IEDs which can send incorrect data or in the case of SCADA systems, erroneous commands maybe sent, incorrect alarms may set off etc. Due to incorrect alarms, operators might be forced to take

unnecessary control actions. In a coordinated attack scenario this might have drastic consequences. Additionally, modification of settings data may result in incorrect settings of IEDs. Modification of data such as price signals can affect the demand in an adverse way [1.24].

2. Theft of Information

This results in loss of confidentiality. Theft of information is related to passive monitoring or stealing of data without altering the normal operation of the system. It serves to bolster the information available to the attacker about the system. Theft of information regarding security mechanisms, security passwords and keys has long term impact. Obtaining this information about the system helps the adversary to gain a strong foothold to exploit the cyber systems further. This serves to increase the impact of the next attack launched by the adversary. An attacker can obtain sensitive information by monitoring network traffic, which could result in privacy breaches by stealing power usage, disclosure of the controlling structure of smart grids and future price information [1.24]. For example, an attacker can gather and examine network traffic to deduce information from communication patterns, and even encrypted communication can be susceptible to traffic analysis attacks. Traffic sniffer protocol analysis tools can be used to intercept SCADA DNP3 frames and collect unencrypted plaintext frames that contain valuable information, such as source and destination IP addresses and port numbers. This intercepted data, could also include setting and control information. This information can be used to successfully attack the SCADA system or compromise the IED.

3. Denial of Service

This kind of attack results in loss of availability of resources in the system. It involves the use/blocking of system resources by unauthorized users. Denial of service attacks are achieved by flooding the communication channels and system

resources with miscellaneous information. It is important that all the communication channels in the system are available at all times for proper working of SCADA and related systems [1.24]. For example, when the power system is operating near the point of instability and an important control action needs to be taken, it is paramount for the device to be available. Denial of Service/Theft of Resources kind of attacks in such a situation can cause adverse impacts to the physical equipment. A DoS/DDoS attack against various grid components including smart meters, networking devices, communication links, and utility business servers can be carried out. If the attack is successful, then it would not be possible to control the power supplied to the target region through automated systems.

1.3.5 Cyber-Physical Consequences

It has been mentioned before that a cyber-attack may have physical consequences. This is usually a consequence of the three kinds of attacks discussed above. The loss of a component in the information and communication systems is important because it can cause the unavailability of a critical device/resource. Physical destruction due to cyber-attacks is rare and difficult to accomplish. The control systems are inherently complex and difficult to maliciously interface with [1.25]. Physical assets are protected by multiple protective mechanisms that remove components from service if potentially damaging operating states of frequency, voltage, current, etc. are detected. Backup protection schemes are coordinated to protect physical components in the event local protection fails.

If an attacker gains access to the power control/communication network, the attacker can perform a wide range of attacks depending on the information available to the attacker. If the attacker is an outsider, it would be safe to assume that the information available to him is very limited. However, through theft of information attacks, it is possible to bolster the information available to the attacker as discussed in section 1.6.2. It has been mentioned

previously that the unique nature of the EPG means that there is a cyber-physical impact for certain cyber-attacks and that it is not universal.

An example of physical destruction in the power system is the Aurora attack which was simulated at the Idaho National Laboratories (INL) in 2007. This kind of attack involves the disabling of the sync check element in the generator protective relay, which relates to a denial of service kind of attack discussed in section 1.6.3. Additionally, it requires that the period of attack is coordinated to prevent other protective relays from operating to prevent tripping of the generator. The basic idea of an Aurora type of attack is to cause isolation of the generator by tripping the circuit breaker associated with it. The period of isolation is kept very small, of less than 15 cycles and the breaker is closed to put the generator back in the system as shown in figure 1.2.

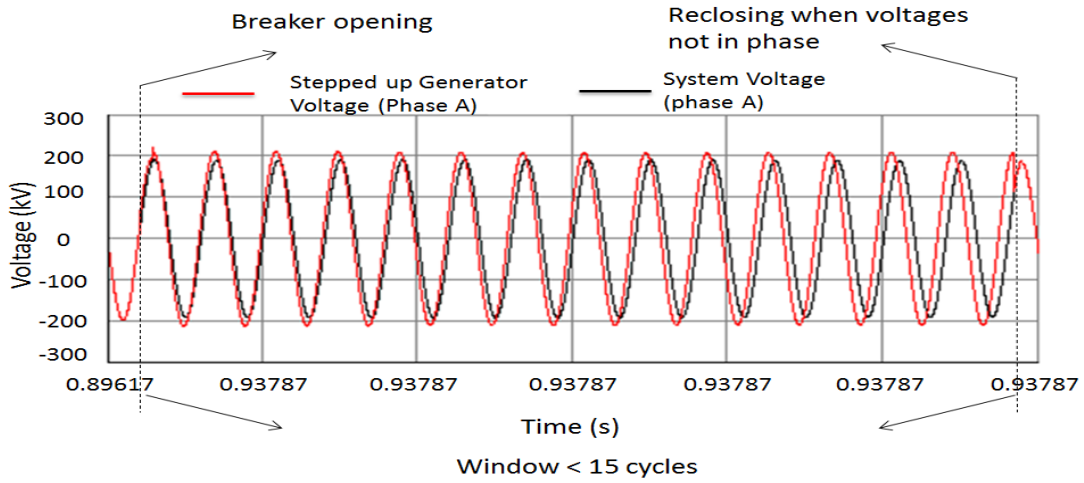

Figure 1.2: Plot depicting the voltage separation during an Aurora attack.

Within this small period, the generator frequency is changes from system frequency. Consequently, the voltages are no longer in phase. When the circuit breaker is reclosed under these conditions, the generator experiences mechanical stress which causes physical damage. The demonstration at INL shows the blowing up of a Diesel generator due to an Aurora type of attack [1.9].

The Stuxnet attack is another example of a physical destruction attack. Stuxnet involved the compromising of Siemens Industrial Programmable logic controllers (PLC). The destruction of industrial motors was achieved by changing the rotational speed of motors governed by these PLCs. By corrupting the settings of the PLC, Stuxnet was able to periodically increase the motor frequency to 1410Hz, then dropping it down to 2Hz, and then returning it to the 1064Hz normal operating speed of the motors. Due to the fluctuation in the rotational speed of the motors, centrifugal forces caused stress on the mechanical parts of the motor which resulted in damage. Additionally, Stuxnet was also able to install software to corrupt the motor speed monitoring data, which concealed the true state of the motor speed from SCADA monitoring systems. This prevented corrective actions from being taken before physical damage was realized [1.11].

1.4 Cyber-Power Modeling and Simulation

An introduction to power modeling and cyber simulators is provided in this section.

1.4.1 Power System Modeling

There are a number of tools for power system modeling and simulation. The two tools used in this work are described here.

1. RTDS: The RTDS is a fully digital power system simulator capable of continuous real time operation. It performs electromagnetic transient power system simulations with a typical time step of 50 microseconds by using a combination of custom software and hardware. The time-step may vary depending on the components used to model the power system. It is an ideal tool for the design, development and testing of power system protection and control schemes with capacity for both digital and analogue signal exchange through numerous dedicated, high speed I/O ports. The physical protection and control devices are interfaced with the RTDS through these devices to interact with the simulated power system [1.26].

2. MATPOWER: It is an open-source Matlab based power system simulation package that provides a high-level set of power flow, optimal power flow (OPF), other tools. MATPOWER consists of a set of Matlab M-files designed to give the best performance possible while keeping the code simple to understand and customize. MATPOWER employs all of the standard steady-state models typically used for power flow analysis. The details on the equations used for these models are described in [1.27].
3. Other Power System Simulators: There are several other options available when it comes to modeling of power system. These include Power System Simulation Software (PSMS) from etap, Power System Analysis Toolbox (PSAT) for Matlab, and Power World Simulator to name a few.

1.4.2 Cyber Simulation Tools

Network simulators are used by people from different areas such as academic researchers, and industrial developers to design, simulate, verify, and analyze the performance of different networks protocols among several possible uses [1.28]. They are typically used to evaluate the effect of different parameters on the protocols being studied. Generally a network simulator will comprise of tools which help users to build complex networks from basic building blocks like clusters of nodes and links. With their help, one can design different network topologies using various types of nodes such as end-hosts, hubs, network bridges, routers, optical link-layer devices, and mobile units. A good network simulator is expected to support a number of existing protocols and allow for user defined protocols to be simulated as well.

The basic difference between simulation and emulation is that the latter is expected to emulate the required delays due to processing, propagation, transmission and queuing experienced in a communication network depending on the topology configured. Essentially, the packet generation is real; however the communication network is simulation. Hence, a

network emulator is one which supports real packet flow between end systems [1.28]. This is particularly useful for testing purposes. In this section, a comprehensive list of network simulators with their description is provided.

1. Network Simulator 2: Network Simulator 2 (NS2) is a discrete event simulator which was originally developed at the University of California, Berkley. It is built using C++, and uses Object Tool Command Language (OTcl) for configuration and scripting interface. It is one of the most popular academic research network simulators and supports a wide range of network protocols and models. It has the ability to support large communication topologies without much trouble. Wired mesh network topologies of up to 1000 nodes can be run with some optimizations. NS2 also supports emulation mode of operation. However, the functionality is very limited. With the emergence of Network Simulator 3 (NS3), the support for NS2 has reduced although there are still several active groups contributing to it. One of the main drawbacks in using NS2 is in the visualization. NS2 using NAM which just reproduces the trace file generated during simulation [1.29].
2. Network Simulator 3: The Network Simulator 3 (NS3) is a discrete-event simulator targeted primarily for research, and educational use. The ns-3 project, started in 2006 is an open-source project developing ns-3. It is the successor to the highly popular NS2. It is to be noted here that NS3 is written from scratch and not derived from NS2. It uses C++ for scripting with python bindings. As such there is no backward compatibility between NS3 and NS2. NS3 is relatively new and requires a lot of contribution and feedback from the research community to establish credibility to the project. NS3 supports emulation mode of operation and has the ability to do this in real time [1.30]. More details on this are provided in chapter 3.
3. Common Open Research Emulator: The Common Open Research Emulator (CORE) is a tool for emulating networks on one or more machines. These networks can be

connected to live networks. CORE consists of a Graphical User Interface (GUI) for drawing topologies of light weight virtual machines, and python modules for scripting network emulation. CORE has been developed by a network technology research group that is part of the Boeing Research and Technology Division. The Naval Research Laboratory is supporting further research of the open source project. The major key feature of CORE is that it allows real-time connection of real networks allowing hardware in the loop. It is highly customizable and allows distributed emulation with multiple COREs running [1.31].

4. OPNET: OPNET is one of the popular commercial network simulators. It can be flexibly used to study communication networks, devices, applications, and protocols. Object-orient programming design is used to map the graphical configuration and topology to the implementation. OPNET inherently has three main functions: modeling, simulating, and analysis. For modeling, it provides intuitive graphical environment to create all kinds of models of protocols. For simulating, it uses 3 different advanced simulations technologies and can be used to address a wide range of studies. For analysis, user friendly graphs, charts, statistics, and even animation can be generated by OPNET. It also provides kernel support for both 32-bit and 64-bit parallel simulation. Additionally, it has grid computing support, allows discrete event, hybrid, and analytical solution. For the purpose of providing the emulation mode of operation and to interface with real nodes, OPNET provides the simulation in the loop module [1.32].
5. OMNeT++: OMNet++ is a discrete event simulation environment. It is free for academic and non-profit use. Its primary application area is the simulation of communication networks, but because of its generic and flexible architecture, is successfully used in other areas like the simulation of complex IT systems, queuing networks or hardware architectures as well. OMNet++ provides component

architecture for models. Components (modules) are programmed in C++, and then assembled into larger components and models using a high-level language. OMNet++ has extensive GUI support, and due to its modular architecture, the simulation kernel (and models) can be embedded easily into applications. It is different from other open source networks simulators NS2 and NS3 in this aspect, as these do not have extensive GUI support [1.33].

6. SSFNET: SSFNET is a set of Java network models built over the Scalable Simulation Framework (SSF). SSF is a specification of a common application programming interface (API) for simulation, which assures portability between compliant simulators. There are multiple Java and C++ implementations of SSF. DartmouthSSF (DaSSF) [1.34], for instance, is a C++ implementation of SSF oriented to allow parallel simulation of very large scale communication networks [1.35].

1.5 Thesis Objectives

To explore the cyber-physical nature of critical infrastructure such as the EPG, it is important to be able to prototype the actual working conditions accurately with sufficient detail. While the review of system components individually is critical, it is also important to review the cyber-power interdependencies for the integrated system deployed in a real environment. Keeping this in view, it is important to test applications and algorithms with relevance to cyber-power paradigm before deployment in a real world environment. With regard to this, the thesis objectives are stated as follows:

1. Develop communication architecture for standard power system test cases.
2. Perform analysis on the communication network architecture derived for standard power system test cases using network simulator 2 and network simulator 3, and compare the results to determine suitability for emulation.
3. Setup cyber-physical test bed with hardware in the loop. This involves the integration of power simulator, network simulator and end systems/software's

with the resources available at the Smart Grid Demonstration and Research Investigation Laboratory (SGDRIL) at Washington State University (WSU).

4. Use the developed test bed to validate devices and algorithms.
5. Explore the possibility of integrating cyber-simulators with existing Operator Training Systems (OTS) to better equip operators in dealing with cyber-physical contingencies.

1.6 Thesis Organization

The thesis has been organized in six chapters. Chapter 1 provides an introduction to the electric power grid, cyber security requirements, need for cyber-physical approach to problems in EPG, power simulators, and cyber simulators. The motivation and objectives of this thesis are also listed in this chapter. Chapter 2 deals with the description of the communication architecture to be derived from a power system point of view. The assumptions to be used for simulation of communication system for the standard power system test cases are discussed. The results obtained for the systems using NS2 and NS3 are discussed and compared.

In chapter 3, an outline of the devices and software available at the SGDRIL laboratory utilized in the cyber-power simulation is presented. The operation of NS3 in emulation mode and integration with RTDS other resources to form the cyber-physical test bed is discussed in detail in this chapter. The different mode of operation for the developed cyber-physical test bed is also discussed. In chapter 4, the applications of the developed cyber physical test bed is presented. The testing of applications such as Local area Voltage Stability Monitoring Algorithm (LVSMA), Wide area Voltage Stability Monitoring Algorithm (WAVSMA) on the cyber-physical test bed is discussed. In chapter 5, we discuss the possible integration of a cyber-simulator with the conventional Operator Training Simulators (OTS) to provide a complete cyber-physical contingency response training to operators. Contributions, conclusions and possible future research directions are discussed and presented in chapter 6.

1.7 Summary

A general overview of the power grid was presented in this chapter. Additionally, the cyber challenges faced by the power grid and the possible cyber-physical consequences are also discussed. Motivation for cyber-physical studies are justified based on details presented in this chapter. A brief survey on the available communication network simulators was also discussed. The thesis objective of setting up a cyber-physical test bed is stated followed by a brief introduction to the organization of this thesis.

1.8 References

[1.1] V.C. Gungor, D. Sahin, T. Kocak, S.Ergut, C. Buccella, C. Cecati, G.P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards", IEEE Transactions on Industrial Informatics, vol.7, no.4, pp. 529-539, Nov. 2011.

[1.2] C. Cecati, C. Citro, A. Piccolo, P. Siano, "Smart Operation of Wind Turbines and Diesel Generators According to Economic Criteria", IEEE Transactions on Industrial Electronics, vol.58, no.10, pp. 4514-4525, Oct. 2011.

[1.3] Mo Yilin, T.H.-H. Kim, K. Brancik, D. Dickinson, Lee Heejo, A. Perrig, B. Sinopoli, "Cyber–Physical Security of a Smart Grid Infrastructure", Proceedings of the IEEE , vol.100, no.1, pp. 195-209, Jan. 2012.

[1.4] Greg Moller, "Principles of sustainability", Chapter 6, part 3. [Online]. Available: htt p://www.webpages.uidaho.edu/sustainability/chapters/ch06/ch06-p3a.asp

[1.5] A. Chakrabarti, S. Halder, Power System Analysis: Operation And Control, third edition, PHI Learning Pvt. Ltd., pp. 1-3, 2004.

[1.6] N. G. Hingorani and L. Gyugyi, Understanding FACTS: Concepts and Technology of Flexible AC Transmission Systems, IEEE, New York, 2000.

[1.7] C.H. Hauser, D.E. Bakken, A. Bose, "A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid", IEEE Power and Energy Magazine, vol.3, no.2, pp. 47-55, March-April 2005.

[1.8] M. Govindarasu, A. Hann, P. Sauer, “Cyber-Physical Systems Security for Smart Grid”, PSERC Publication 12-02, Feb. 2012.

[1.9] CNN report on Aurora attack demonstration by INL. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/

[1.10] New York Times report on Georgian power grid cyber-attack. [Online]. Available: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0

[1.11] N. Falliere, L. O. Murchu, and E. Chien, “W32.Stuxnet Dossier”, v1.4, Symantec, Cupertino, CA, 14 Feb. 2011. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[1.12] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, C. Assi, "Communication security for smart grid distribution networks”, IEEE Communications Magazine, vol.51, no.1,pp. 42-49, January 2013.

[1.13] J. Kurose and K. Ross, Computer Networking: A Top-Down Approach, ed. 5. Boston, MA: Pearson Education Inc., pp. 704-709 & 747-759, 2010.

[1.14] Standards for Security Categorization of Federal Information and Information Systems, National Institute of Standards and Technology, Standard FIPS PUB 199, Feb. 2004.

[1.15] J. J. Grainger and W. D. Stevenson, Power System Analysis, McGraw-Hill, 1994, pp. 562-572 & 641-687.

[1.16] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, P. Shengyi, U. Adhikari, "Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information”, IEEE Transactions on Smart Grid, vol.4, no.1, pp. 235-244, March 2013.

[1.17] M. Zeller, “Myth or reality-does the aurora vulnerability pose a risk to my generator”, in Proc. 37th Annual Western Protective Relay Conf., Spokane, WA, Oct. 2010.

[1.18] C.A. Meyers, S.S. Powers, and D.M. Faissol, "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches", Technical Report, Lawrence Livermore National Laboratory, 2009.

[1.19] R. Westervelt, "Cybercriminals employ toolkits in rising numbers to steal data", Search Security, September 6, 2007. [Online]. Available: http://searchsecurity.techtargt.com/news/article/0,289142,sid14_gci1271024,00.html.

[1.20] M. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy", Digital Investigation, vol.3, pp. 97-102, 2006.

[1.21] D. Denning, Networks and Netwars: the Future of Terror, Crime, and Militancy, Rand Monograph MR-1382, chapter 8, 2001. [Online]. Available: http://www.rand.org/pubs/monograph_reports/MR1382/index.html.

[1.22] M. Landler and J. Markoff, Digital fears emerge after data siege in Estonia, The New York Times, May 29 2007. Available: http://www.nytimes.com/2007/05/29/technology/29estonia.html.

[1.23] J. Markoff, Before the gunfire, cyberattacks, New York Times, August 12, 2008. [Online]. Available: http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[1.24] C. Tranchita, N. Hadjsaid, A. Torres, "Overview of the power systems security with regard to cyberattacks", Fourth International Conference on Critical Infrastructures, pp. 1-8, March 27-April 30. 2009.

[1.25] D. Shea, "Critical Infrastructure: Control Systems and the Terrorist Threat", Congressional Research Service, Library of Congress, Washington, DC, Report RL31534, 21 Feb. 2003.

[1.26] P. Forsyth, T. Maguire, R. Kuffel, "Real time digital simulation for control and protection system testing", IEEE 35th Annual Power Electronics Specialists Conference, vol.1, pp. 329-335, 20-25 June 2004.

[1.27] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education", IEEE Transactions on Power Systems, vol. 26, no. 1, pp. 12-19, Feb. 2011.

[1.28] Jianli Pan, J. Raj, "A Survey of Network Simulation Tools: Current Status and Future Developments", Project report. [Online]. Available: http://www.cse.wustl.edu/~jain /cse567-08/ftp/simtools/

[1.29] The Network Simulator, NS–2 [Online]. Available: http://www.isi.edu/nsnam/ns/

[1.30] NS3 official website. [Online]. Available: http://www.nsnam.org/documents.html

[1.31] CORE official website. [Online]. Available: http://cs.itd.nrl.navy.mil/work/core/

[1.32] OPNET Modeler. [Online]. Available: http://www.opnet.com/

[1.33] OMNeT++ official website. [Online]. Available: http://www.omnetpp.org/

[1.34] Scalable Simulation Framework (SSF). [Online]. Available: http://www.ssfnet.org

[1.35] Dartmouth SSF (SSF). [Online]. Available: http://www.crhc.uiuc.edu/jasonliu/ projects/ssf/

CHAPTER TWO

COMMUNICATION REQUIREMENT EVALUATION USING NETWORK SIMULATOR-2 AND NETWORK SIMULATOR-3

2.1 Introduction

The main objective of this chapter is to describe the offline simulations of communication network and compare the results obtained using NS2 and NS3. Same system has been modeled with similar assumptions for both the simulators. The architecture and working of NS2 and NS3 are described in detail to provide some insight into the working of these simulators and their fundamental differences. The communication architecture derived from the power system layout is discussed for the IEEE 14 bus standard power system test case. For the purpose of simulation, it is necessary to make certain assumptions about the location of devices, data transfer locations etc., which are discussed in detail as well. A short discussion on the different latency contributors in the communication network is given.

2.2 Event Driven Simulation

It is important to understand the concept of event driven simulation as this is the basis of working for both NS2 and NS3. Event-driven simulation is a subclass of time-driven simulation. Time-driven simulations proceed chronologically, by using a simulation clock which keeps track of the simulation time. The simulation exit condition may either be a threshold clock value or a forceful exit from the script file. An event-driven simulation is initiated and run by a set of events. The simulator usually maintains a list of scheduled events and proceeds through the list chronologically. The list does not have to be predefined at the start of the simulation. Certain events in the simulation may lead to the creation of more events, which are added to a list and sorted chronologically. The simulation moves from event to event on the timeline. After the completion of one event, the simulation clock shifts to the

time the next event is scheduled. A graphical representation of event handling is shown in figure 2.1 [2.1].

At time t=0, the simulation starts. At time t=a, an event is scheduled, so the clock time jumps to the time at t=a. The event is executed and now the simulation clock jumps to t=b. This process is repeated until all the events are executed, or if the time threshold is exceeded, or if some external exit condition is satisfied.

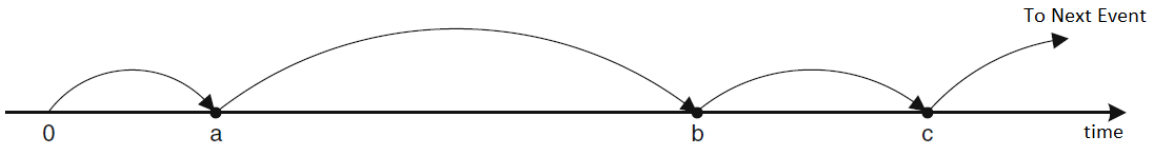

Figure 2.1: Clock advancement in an event-driven simulation

2.3 Basic Architecture of Network Simulator 2

NS2 consists of two key languages: C++ and Object-Tool oriented Command Language (OTcl). C++ in NS2 is basically used as the core and backend. It defines the internal mechanism of the simulation objects. All protocol and agent implementations are carried out in C++. OTcl is used for setting up the simulation by assembling and configuring the objects to be created and scheduling the events. The binding between C++ and OTcl is achieved by the use of Tcl with classes (TclCL). It is possible to map and bind variables between the two domains. OTcl variables mapped to C++ objects are referred to as handles. By itself, it has no functionality. The functionality is provided in the mapped C++ object. Figure 2.2 shows a simplified view of NS2 overall architecture [2.2-2.3].

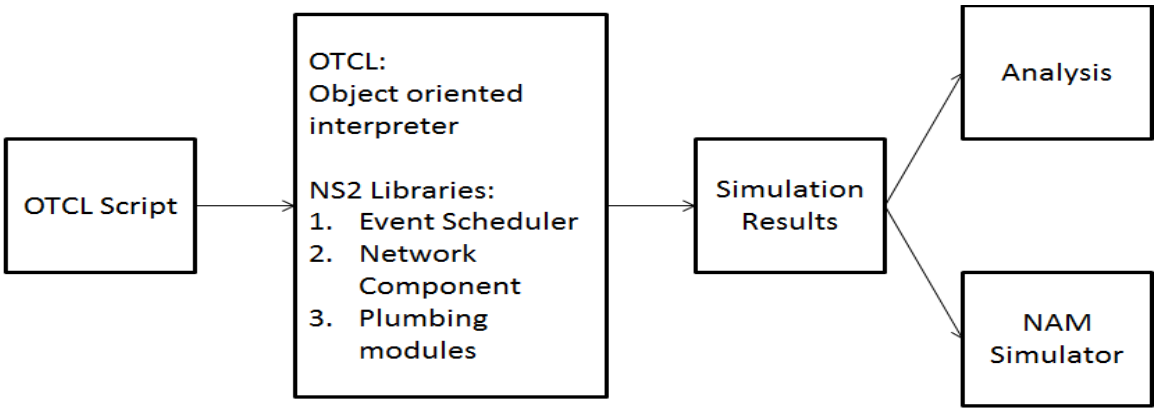

Figure 2.2: Simplified view of NS2 architecture

NS2 provides a large base of built-in agents and protocols. While the coverage is comprehensive, it is also possible to write and implement user defined applications and protocols in NS2. These can then be validated through simulation.

The Network AniMator (NAM) tool is a Tcl based animation tool for viewing network simulation traces and real packet traces. It supports topology layout, packet level animation, and various data inspection tools. NAM has been designed to be able to read large animation data sets. This is achieved by setting a minimum amount of information regarding the animation in memory. Event commands are kept in the file and re-read from the file whenever necessary. NS2 creates a nam extension file, which contains data in the format readable by NAM. In the tcl script used for configuring the simulation, a nam trace is also created. The file generated can be run afterwards using the NAM console.

2.4 Basic Architecture of Network Simulator 3

As previously mentioned in chapter 1, NS3 is completely unrelated to its predecessor NS2. NS3 has been written from scratch and uses a C++ core. The scripting interface can be either python or C++. NS3 has a modular implementation and contain a core library which takes care of the generic aspects of the simulator and a simulator library which deals with specifying simulation time objects, schedulers and events. A common library defines objects independent to specific network architectures, such as the tracing objects. The node and

device libraries are responsible for the definition of classes to be used for building the network and devices in the simulator. Protocol entities are written to be closer to real world implementation. Packet implementations are based on real world packets in order to enable to communication between simulated agents and external world. One of the major features of NS3 is the ability to run distributed simulation. Here distributed simulation is defined as the ability of the process to use multiple processors or machines. Figure 2.3, shows the basic architecture of a NS3 simulation [2.4].

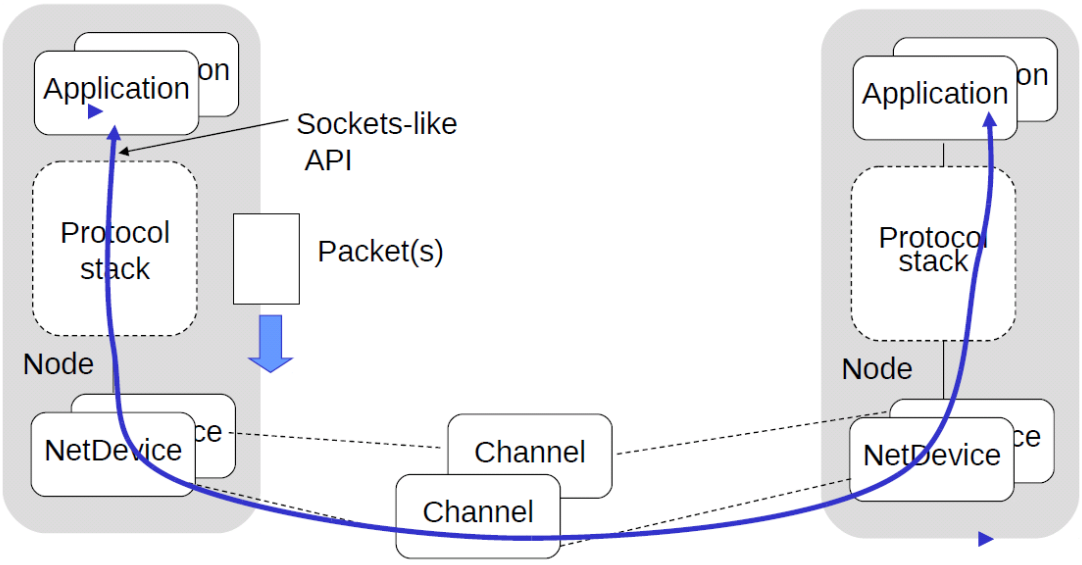

Figure 2.3: Basic view of NS3 Simulation

NS3 generates trace files of two major extensions: ASCII and PCAP. PCAP stands for packet capture and any standard packet capture software can read these files. The most commonly used open source software among these is Wireshark. For the purpose of visualization, NS3 has two major options: PyViz and NetAnim.

PyViz is a visualization console based on Python. The most important feature in this animator is that it does not use any trace files and can be used as a live simulator. This is particularly useful for debugging purposes. It works independent of the scripting language used for configuring the NS3 simulation.

NetAnim is an offline animator used in NS3. It takes an xml file as input. The generation of this xml file has to be included in the simulation configuration script. It is to be noted here that while NetAnim can be used whether NS3 is run in either simulation or emulation mode.

2.5 Communication Architecture

In a communication network, fiber optic cables are generally used between all main substations and control center. Optic fiber cables are laid along the transmission lines in the power system and these are responsible for carrying data. All-Dielectric Self-Supporting (ADSS) fiber optic cables are installed along the transmission lines and use the same tower support infrastructure. Redundancy is provided to cover for failure of one or two links in the system. If it is not feasible to lay a fiber optic line, private WiMax networks are used. For distribution network communications, such as AMI and Distributed Automation (DA) low speed networks with bandwidth in the range of 200 kbps are used. In some cases, public communication lines may be leased. Multiprotocol Label Switching (MPLS) is used for managing the Internet Protocol (IP) network traffic. Some of the different service segregation used to differentiate traffic is telemetry protection, AMI, SCADA and enterprise access.

The communication architecture to be used here is similar to the one proposed in [2.5]. It is assumed here that dedicated fiber optic links are used to transfer data from substations to control center. Two types of architectures are possible: Point to Point Star Topology and Mesh Topology. The star and mesh topologies are shown in figure 2.4. Star topologies are very costly to build, since it involves building dedicated lines for each substation and it may not be economically feasible. Hence, the star topology will not be considered. Mesh topologies involve use of single communication link by multiple nodes thereby increasing link utilization and putting the infrastructure to better use.

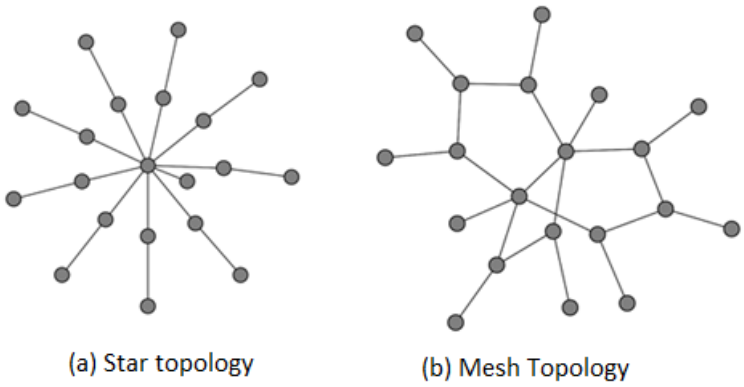

Figure 2.4: Star topology and Mesh topology.

The communication architecture is derived as follows:

1. The first step is to reduce the power system network topology into substations. Usually a bus represents a substation in a power system layout. However, in the event that a transformer is present between two buses, it is reasonable to assume that the transformer and the associated buses are located in the same substation.
2. As mentioned before optic fiber cables are laid along the transmission lines in the power system. It is reasonable to deduce the length of these data transfer lines from the transmission line length. The length of the transmission lines are derived using [2.6] for appropriate voltage levels. For distribution level voltages, it is assumed that per mile reactance is 0.5 ohm.
3. It is assumed in this topology that at each substation, the PMU data is concentrated before being sent out to the control center or any other data gathering center. While at present this may not be a valid assumption, this could well be the architecture moving towards a fully PMU equipped smart grid. Figure 2.5 shows the overall communication architecture for 'N' number of substations. The substation represented in the figure, contains multiple PMUs whose outputs are concentrated by the PDC before being sent out to the control center. The communication topology is dependent on the node reduction discussed next.

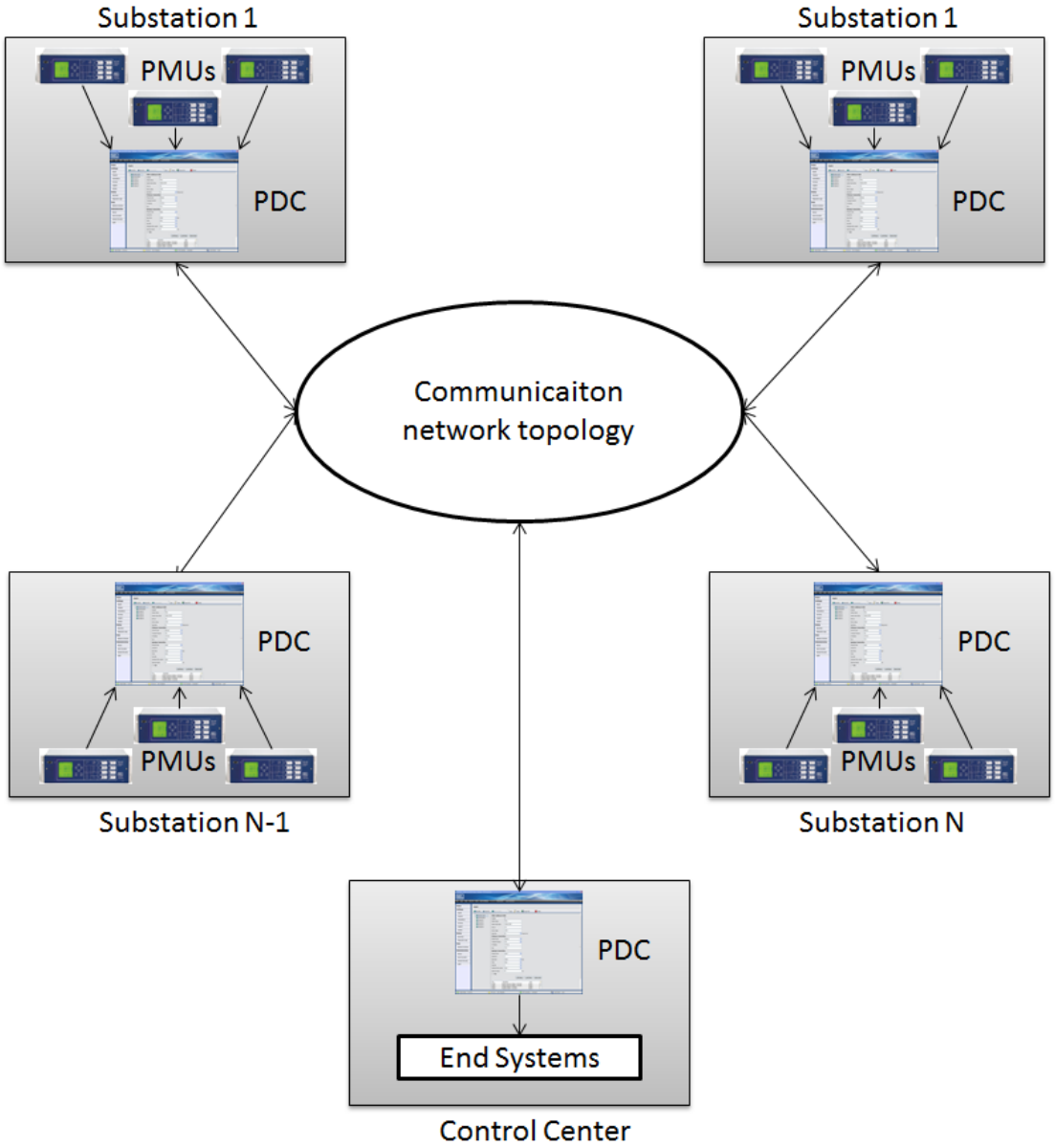

Figure 2.5: Overall communication architecture view

4. Node Reduction: For the purpose of node reduction, a MATLAB script is written which takes the common data format (CDF) file of the power system test cases and gives the reduced node list and bus grouping under each node. The node reduced IEEE 14 bus is shown in figure 2.6, and the subsequent communication model is shown in figure 2.7 for the same.

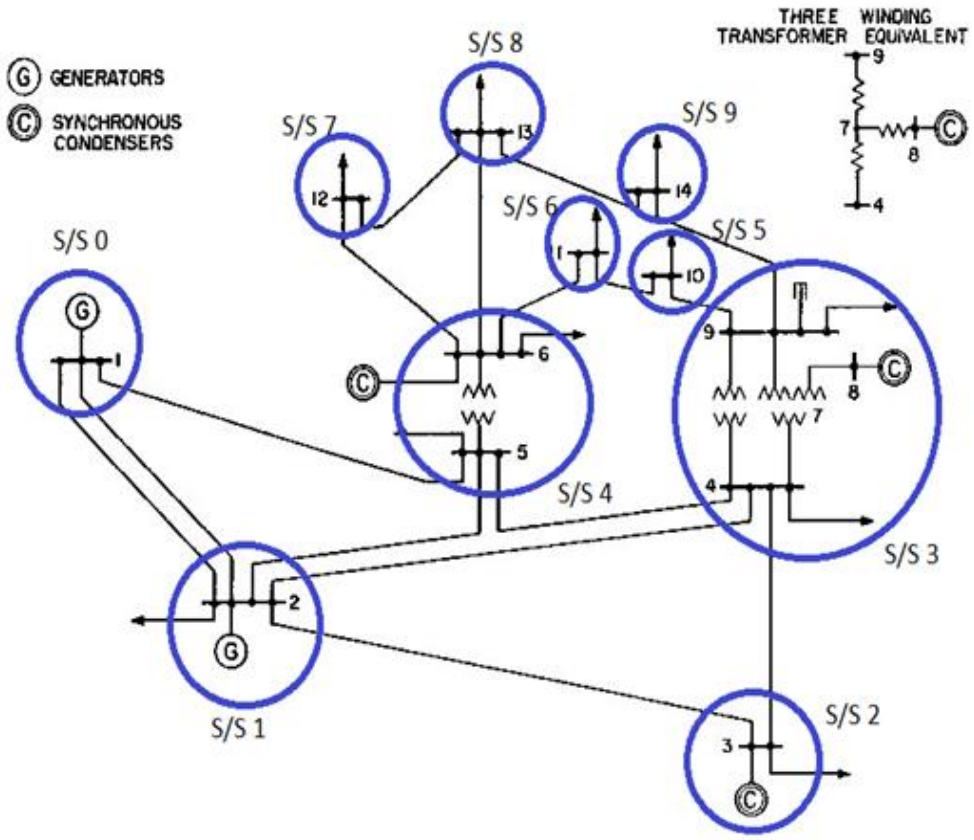

Figure 2.6: Communication node representation of IEEE 14 bus system

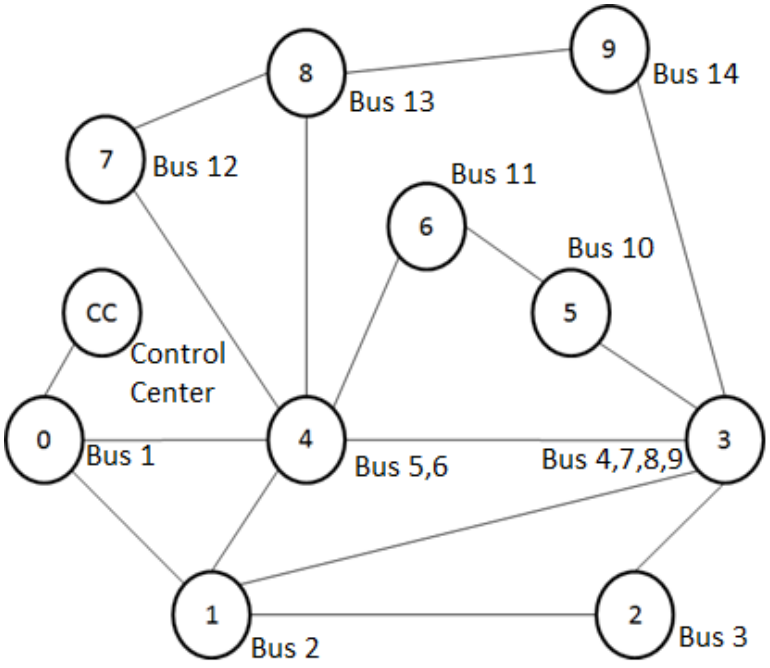

Figure 2.7: Communication model for the IEEE 14 bus system

2.6 Network Latency Contributors

Network latency of packets is defined as the delay from the time of the start of packet transmission at the sender host to the time of the end of packet reception at the receiver host. The sources of network latency are described here [2.7].

1. Network Processing Delay: These delays are incurred when the network gateways, firewalls and servers decide what needs to be done with an incoming packet. The delay depends on the network equipment technology and the specific processing function.
2. Signal Propagation Delay: It is the time taken for a signal to travel in the physical propagation medium, and depends on the medium itself and the distance. Usually the propagation speed of the signal in the medium is about 70% the speed of light.
3. Transmission Delay: There is a definitive time delay for a packet to be completely pushed on to the physical link layer. This delay is called the transmission delay and is dependent on the bandwidth of the link and packet size.
4. Queuing Delay: This kind of delay occurs when multiple packets from an ingress port need to be routed to the same egress port. One packet is transmitted at a time, and a queue is maintained to hold the remaining packets. The time a packet has to spend in a queue is the queuing delay seen by that packet. The total end network latency is the sum of all these delays.

2.7 System Conditions for Simulation

A number of assumptions are made to estimate the parameters to be used in the simulations. We will look into some of the general assumptions which pertain to both NS2 and NS3 here:

1. Only PMU traffic is to be simulated. The sampling rate of these PMUs is assumed to be fixed at 60 samples per second.

2. OC-3 fiber optic cables are assumed to be used. These have a bandwidth of 155 Mbps.
3. The propagation delays for the links are calculated based on the transmission line length. The speed of light in the propagation media is taken as 2 * 10^8 m/s.
4. The system is assumed to be static with no spikes in data, unless caused by data loss in Transmission Control Protocol (TCP) data transmission.
5. Constant Bit Rate applications are used to emulate the constant streaming of data from PMUs. The transfer protocol used is the Unified Datagram Protocol (UDP). TCP is not considered here.
6. The LAN delays are factored into the link between substation server and gateway by adding a delay of 0.03 milliseconds.
7. The packet size calculation is based on the assumption that a breaker and a half scheme is implemented at the substations. For the calculation of packet size, the C37.118.2 format data frame is used [2.8]. The quantities to be measured are the bus voltage, current on the feeders and the breaker status. Therefore, for a substation which has three feeders, there are total of twelve phasors. In addition to this, for each feeder, two analog values are to be transmitted. Adding the header size, Table 2.1 shows the packet size calculated for the IEEE 14 bus test case.

Table 2.1: Packet size for IEEE 14 bus system

Node Number	Packet Size (Bytes)
Node 0	142
Node 1	208
Node 2	142
Node 3	242
Node 4	274
Node 5	142
Node 6	142
Node 7	142
Node 8	176
Node 9	142

8. The control center is assumed to be near the slack generator substation node.

2.8 Results

There are several different types of traffic which have been discussed in [2.9]. However, since the motive of this chapter is to perform comparative analysis for communication requirements using the NS2 and NS3, we will consider only the data flow from substation to control center.

1. Network Simulator 2: The link utilization in Mega Bits per Second (Mbps) and its percentage value is given by:

$$\% \text{ Link Utilization} = \frac{\text{Bits per second in link}}{\text{Bandwidth of link}} * 100 \tag{2.1}$$

The link utilization and percentage between the gateway nodes alone is given in table 2.2.

Table 2.2: Link utilization between gateway nodes

From Node	To Node	Link Utilization in Mbps	Link Utilization (percentage)
0	4	0.6048	0.390194
0	2	0.06816	0.043974
1	3	0	0
1	4	0	0
2	3	0	0
3	4	0.11616	0.074942
3	5	0	0
3	9	0	0
4	6	0.13632	0.087948
4	7	0.06816	0.043974
4	8	0.15264	0.098477
5	6	0.06816	0.043974
7	8	0	0
8	9	0.06816	0.043974

It can be seen that for some of the links, the link utilization is zero. Since shortest path algorithm is used to setup the routing tables, some links are unused. The average

delay from each substation server to the control center located at the slack bus is given in table 2.3. Figure 2.8 shows the communication topology implemented in ns2.

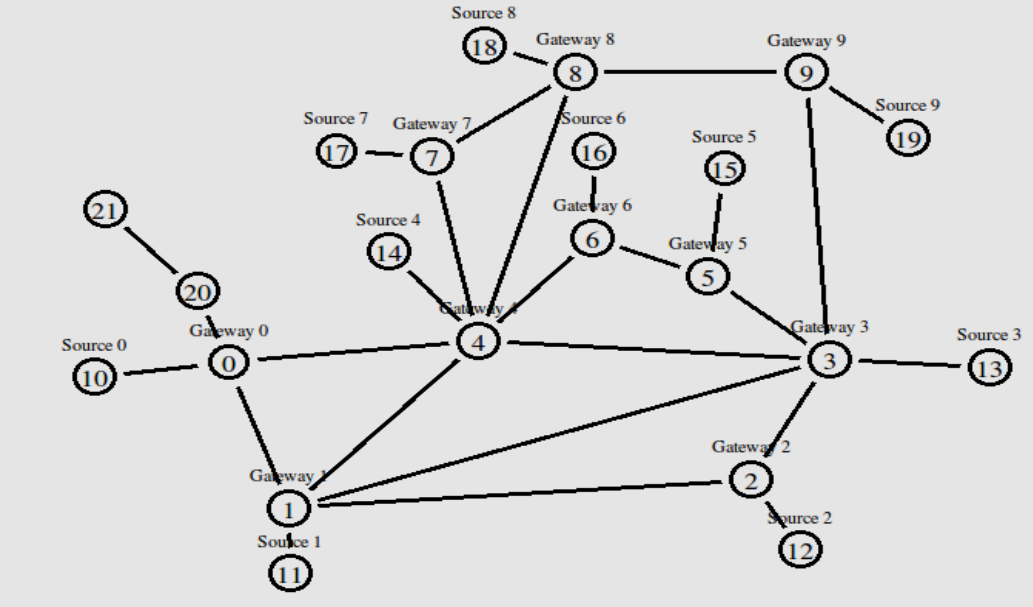

Figure 2.8: Communication network visualization in NS2 using NAM

Table 2.3: Average delay between substation servers to control center

Substation Server	Average Delay (in ms)
0	0.17601
1	0.80767
2	1.81750
3	1.58277
4	1.36125
5	1.53235
6	1.43295
7	1.46022
8	1.40977
9	1.59010

The queuing delays seen in the system are very small in the order of microseconds. It is to be noted here that, as the size of the system and volume of traffic increases in the system, the contribution from this type of delay will go up.

2. Network Simulator 3: The link utilization in Mbps and its percentage value between the gateway nodes alone is given in table 2.4.

Table 2.4: Link utilization between gateway nodes

From Node	To Node	Link Utilization in Mbps	Link Utilization (percentage)
0	4	0.73824	0.476283871
0	2	0.08736	0.05636129
1	3	0	0
1	4	0	0
2	3	0	0
3	4	0.13536	0.087329032
3	5	0	0
3	9	0	0
4	6	0.17472	0.112722581
4	7	0.08736	0.05636129
4	8	0.19104	0.123251613
5	6	0.08736	0.05636129
7	8	0	0
8	9	0.08736	0.05636129

The average delay from each substation server to the control center located at the slack bus is given in table 2.5.

Table 2.5: Average delay between substation servers to control center

Substation Server	Average Delay (in ms)
0	0.179313
1	0.860583
2	1.8815
3	1.63325
4	1.405417
5	1.598417
6	1.496667
7	1.524083
8	1.469083
9	1.642833

3. Comparison: From the two results it can be seen that they match very closely. The major difference between the two simulators is that, NS3 adds additional headers when it is processed by each net device. This header is specific to the net device in addition to the IPv4 header. Hence, the total packet size is different from the values in table 2.1. This effectively increases the packet transmission delay resulting in higher latencies calculated in table 2.4. Additionally, the link utilization also increases due to increase in packet size.

2.9 Summary

In this chapter the basic architecture of NS2 and NS3 are introduced and the basic differences between these simulators are discussed. The communication architecture and the communication network topology have been discussed. A brief review on the network latency contributors from the cyber perspective has been given as well. It is to be noted here that apart from these, delay in measurement devices such as transducers and processing delay at PDCs, there will be additional delays. But these delays are external to the communication simulation and are not discussed here. The communication system conditions for the simulation have been presented in this chapter. The results obtained between the two simulators for the same system are discussed. It is seen that the NS3 node implementation being closer to real world network devices and protocol stacks, is better suited for emulation purposes.

2.10 References

[2.1] T. Issariyakul, E. Hossain, "Introduction to Network Simualtor NS2", Springer, Jan 2009.

[2.2] Ns Manual. [Online]. Available: http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf

[2.3] Ns2 Simulator for Beginners [Online]. Available: http://www-sop.inria.fr/members/Eitan.Altman/COURS-NS/n3.pdf

[2.4] NS3 Tutorial. [Online]. Available: http://www.nsnam.org/docs/release/3.17/tutorial/ns-3-tutorial.pdf

[2.5] Kansal, P.; Bose, A., "Bandwidth and Latency Requirements for Smart Transmission Grid Applications", IEEE Transactions on Smart Grid, vol.3, no.3, pp.1344-1352, September 2012.

[2.6] P. M. Anderson and A. A. Fouad, Power System Control and Stability. Ames: Iowa State Univ. Press, pp. 450, 1977.

[2.7] Network Latency Contributors. [Online]. Available: http://www.d.umn.edu/~gshute/net/new/delays-losses.xhtml

[2.8] IEEE Standard for Synchrophasor Data Transfer for Power Systems", IEEE Std C37.118.2-2011, pp. 1-53, 28 December 2011.

[2.9] Kansal, P.; Bose, A., "Smart grid communication requirements for the high voltage power system", IEEE Power and Energy Society General Meeting, 24-29 July 2011

CHAPTER THREE

CYBER-PHYSICAL TEST BED USING REAL TIME DIGITAL SIMULATOR AND NETWORK SIMULATOR 3

3.1 Introduction

One of the major objectives of this thesis is analysis of the cyber-power system using a cyber-physical test bed. The developed Cyber-Physical test bed is an outcome of the integration of RTDS which simulate the power system in real time, and NS3 which emulates the communication network. The hardware and software resources for monitoring and control are also a part of the test bed. In this chapter, the different components that make up the test bed and their individual capabilities are discussed briefly. We then look at the capabilities of NS3 which enable interaction with external systems and go through a brief description on how it is used in emulation mode through the use of a simple example. The complete description of the Cyber-Physical test bed setup through integration of the different hardware and software resources is also discussed. The different modes of operation of the test bed are presented in the last section.

3.2 Test Bed Components

This section provides a brief description of the different hardware/software resources used to make up the cyber-physical test bed. Figure 3.1 shows the overall test bed.

3.2.1 Real Time Digital Simulator

RTDS is the powerful simulation tool used for the simulation of power system. An introduction to the simulator has been given in section 1.5.1. The RTDS at Smart Grid Demonstration and Research Investigation Laboratory (SGDRIL) has three Gigabit Processor Cards (GPC), and two PB5 processor cards which form the backbone of processing. In addition to this, for the purpose of simulating PMUs, Giga-Transceiver Network Communication Card (GTNET) PMU card is available. Up to eight PMUs can be simulated

using one processor. The GTNET PMUs support phasor data rate of up to 240 frames per second. The DNP firmware can be swapped into the GTNET card to allow usage of DNP protocol communication instead of PMU. Using the DNP protocol, the GTNET can communicate with one DNP master and accommodate the following maximum communication capacity: 1024 binary simulation status points (i.e. breaker position), 512 binary simulation control points (i.e. breaker commands), 500 analog status points (i.e. output from simulator), and 100 analog control points (i.e. input to simulator) [3.1].

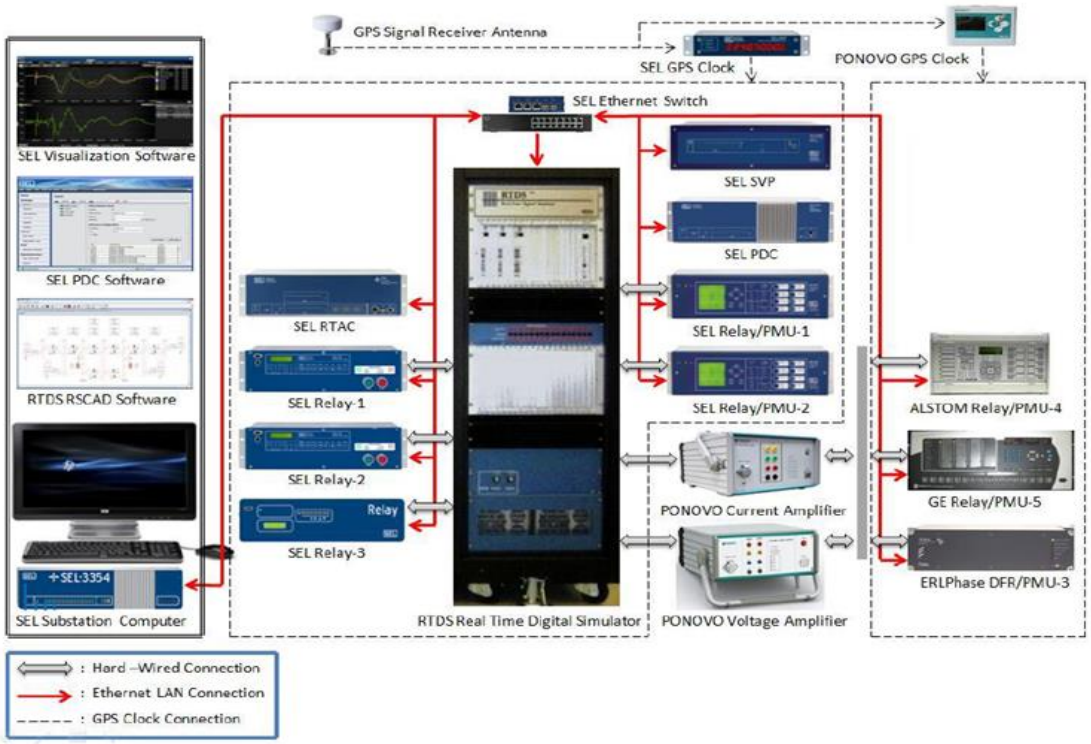

Figure 3.1: Overall Test Bed

3.2.2 Hardware and Software Devices

In the developed test bed, there are a total of seven PMUs available from four different vendors: Alstom, General Electric (GE), ERL Phase and Schweitzer Engineering Laboratory (SEL). All the PMUs are compliant with the IEEE C37.118-2005 standard, and have protective relay or digital fault recording capabilities.

1. Alstom P847

   The Alstom P847 is a PMU available with ancillary protection, control and recording functions. The data sampling rate of the PMU can be up to 60 frames per second [3.2].

2. GE D60 Line Distance Relay/PMU

   The D60 line distance protection system is suitable for protecting transmission lines and cables including lines equipped with series compensation devices. It supports single-pole and three-pole tripping applications. It also includes inter-relay protection communications. Additionally, it is equipped with PMU functionality [3.3].

3. ERL Phase Tesla 4000

   The TESLA 4000 is a multi-time frame power system monitoring recorder. It creates records simultaneously in three time domains – fault (fast), dynamic swing (slow) and trend records. It also comes with an integrated Phasor Measurement Unit (PMU) functionality [3.4].

4. SEL 351

   The SEL 351 protection system is used for directional overcurrent applications. The high-speed breaker failure element and native breaker failure logic enhance breaker failure protection. It comes with built-in PMU functionality [3.5].

5. SEL 387E

   The SEL 387E is a current differential and voltage relay which provides protection to two or three winding transformers. It is also equipped with automation features. This is the only relay in the test bed which does not have PMU functionality added to it [3.5].

6. SEL 421

   The SEL 421 protection, automation and control system is used for high-speed distance and directional protection, and complete control of a two-breaker bay with

PMU functionality. It can be used to protect transmission lines using a combination of five zones of phase- and ground-distance and directional overcurrent elements [3.5].

7. Voltage and Current Amplifier

   For the purpose of amplifying the low level signals from the RTDS, current and voltage amplifiers are required. The PONOVO PAC60Cip current amplifier and PONOVO PAV250Bip voltage amplifier are used for this purpose [3.6].

8. SEL 2407

   The SEL 2407 is a Global Position System (GPS) clock which provides seven IRIG-B time synchronization signals [3.5].

9. SEL 3354

   The SEL 3354 is a substation computer which is capable of withstanding harsh environments. The operating temperature is in the range of -40 to +75 degree Celsius. The test bed has two of these computers, one running Windows Operating System (OS), and the other running Linus OS [3.5].

10. SEL 3373

    The SEL 3373 is a phasor data concentrator (PDC) which has integrated archiving capabilities and is designed to operate in hard substation environments. Archiving is built in, allowing all PMUS data to be saved on the solid-state drive in a secure database. It can be configured with up to 40 PMU inputs and supports data rates from 1 to 240 samples per second [3.5].

11. SEL 3378

    The SEL 3378 is a synchrophasor vector processor (SVP) which can process PMU data with flexible programmable logic. It time-aligns incoming messages, processes them based on the logic configured in the SVP, and sends control commands to external devices based on the logic [3.5].

12. SEL 3530

    The SEL 3350 is called the Real-Time Automation Controller (RTAC). It is primarily a PLC device. The RTAC can provide any degree of functionality from that of a simple intelligent port switch to the sophisticated communication and data handling required for advanced substation integration [3.5].

13. Workstations

    There are a total of four Dell Precision workstations which are used for running end-applications and algorithms.

This part of the section provides a brief description of the major software resources that are used to support the test bed.

1. RSCAD

   RSCAD is the power system modeling software, used for modeling the power system to be simulated in the RTDS.

2. SEL 5073

   The SEL 5073 referred to as SynchroWave is a software PDC. It runs on the windows platform. Unlike its hardware counterpart, the SEL 5073 can concentrate data from up to 500 PMUs. It can connect to any IEEE C37.118-2005 compliant PMU [3.5].

3. OpenPDC

   The openPDC is an open source project administered by the Grid Protection Alliance (GPA). It provides different options for archival and retrieval of data [3.7].

4. SEL 5078 and 5078-2

   The SEL 5078 and 5078-2 are used for visualization of phasor data from PMUs. The 5078-2 provides some additional tools such as modal analysis for oscillation monitoring [3.5].

3.3 Network Emulation Using NS3

NS3 has been designed for integration into virtual machine environments and used in developed test bed. To understand the discussion provided in this section, it is important to know the definitions of Node and Net Device from an NS3 stand point. A node in NS3 is equivalent to the shell of a computer, while a net device represents the network cards and other things related to it such as protocols. For the purpose of emulation, two kinds of net devices are used in NS3: Emulation Net Device and Tap Net Device.

Emulation net device allows the NS3 simulations to send data on a real network. The Emulation net device requires that a physical interface be specified for its operation. This interface needs to be in promiscuous mode of operation. The Emu net device opens a raw socket and binds to the interface. MAC spoofing is done to separate simulation network traffic from other network traffic. The Emu net device can be bound to a physical interface of interest which drives the test bed hardware. An example of this environment is the Open-Access Research Test bed for Next-Generation Wireless Networks (ORBIT) [3.8]. The figure shows separate hosts running NS3 and communication between each other through the test bed hardware. In this case, the test bed is used as the data delivery mechanism, and NS3 is used to generate data which is to be passed through the network. However, for the cyber-physical test bed, the primary purpose of NS3 is to simulate the communication channel rather than to generate data. This is accomplished by using the Tap net device.

The Tap net device allows real or virtual host systems which support TUN/TAP devices to participate in the NS3 simulation. The goal is to make the real node see the NS3 node as a gateway for reaching other subnets. Essentially the real host node net device needs to see the NS3 node as a local device. The tap network device inside the NS3 simulation is called a Tap bridge. The Tap net device has three modes of operation: ConfigureLocal,

UseLocal and UseBridge. In the ConfigureLocal mode, the configuration of the tap device is made in the NS3 simulation.

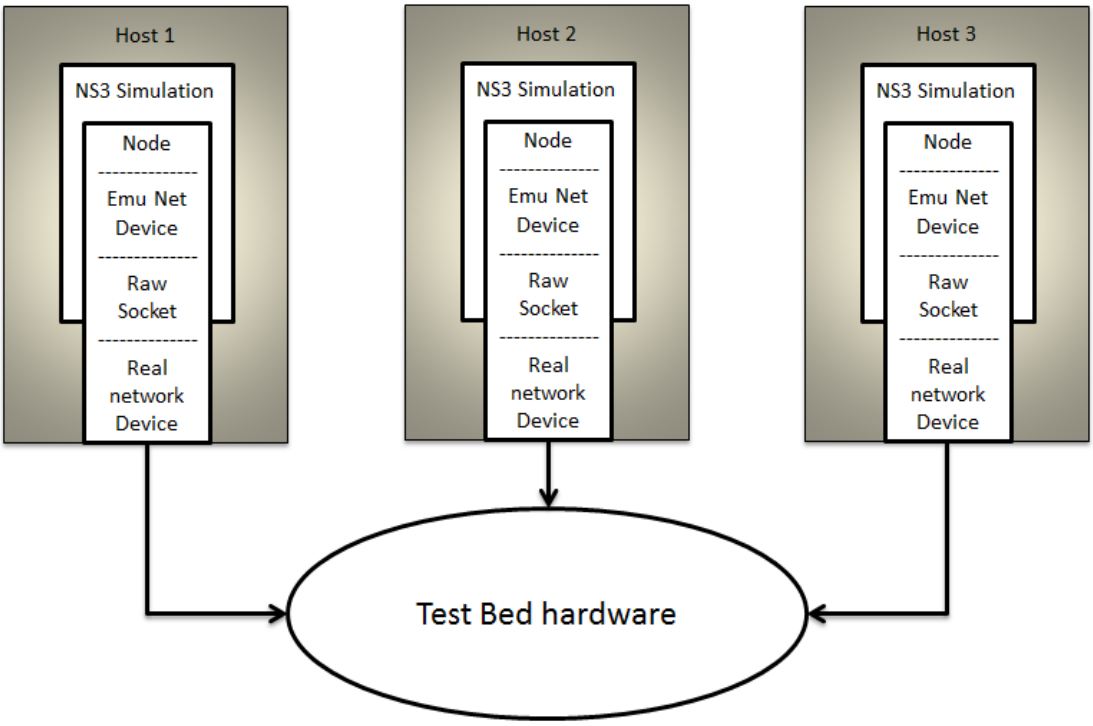

Figure 3.2: Using NS3 to drive test bed hardware

When the simulation is executed, it automatically creates the tap device in the operating system. The problem with this configuration is that since the tap device is to be created only at the time of simulation start, it is not possible to enslave it to any OS bridges. The major difference between the UseLocal mode and ConfigureLocal mode is that the tap device is to be created and configured first in the operating system. This mode uses this configured TUN/TAP device. The drawback in this mode is that the MAC address of the traffic flowing in needs to be unique. This is due to the nature of working of the device. The UseBridge mode also uses the preconfigured TUN/TAP devices. Inside the NS3 simulation, the name of the TUN/TAP device to be used by the tap bridge is specified. The tap bridge then logically extends the OS bridge to encompass the NS3 net device. What this essentially means is that there may be several Linux net devices on the non-NS3 side of the bridge. Thus there may be many real nodes sending/receiving data through a single tap bridge. Therefore

out of the three modes, we use the UseBridge mode of operation. The exact details on their configuration and operation can be found in [3.9].

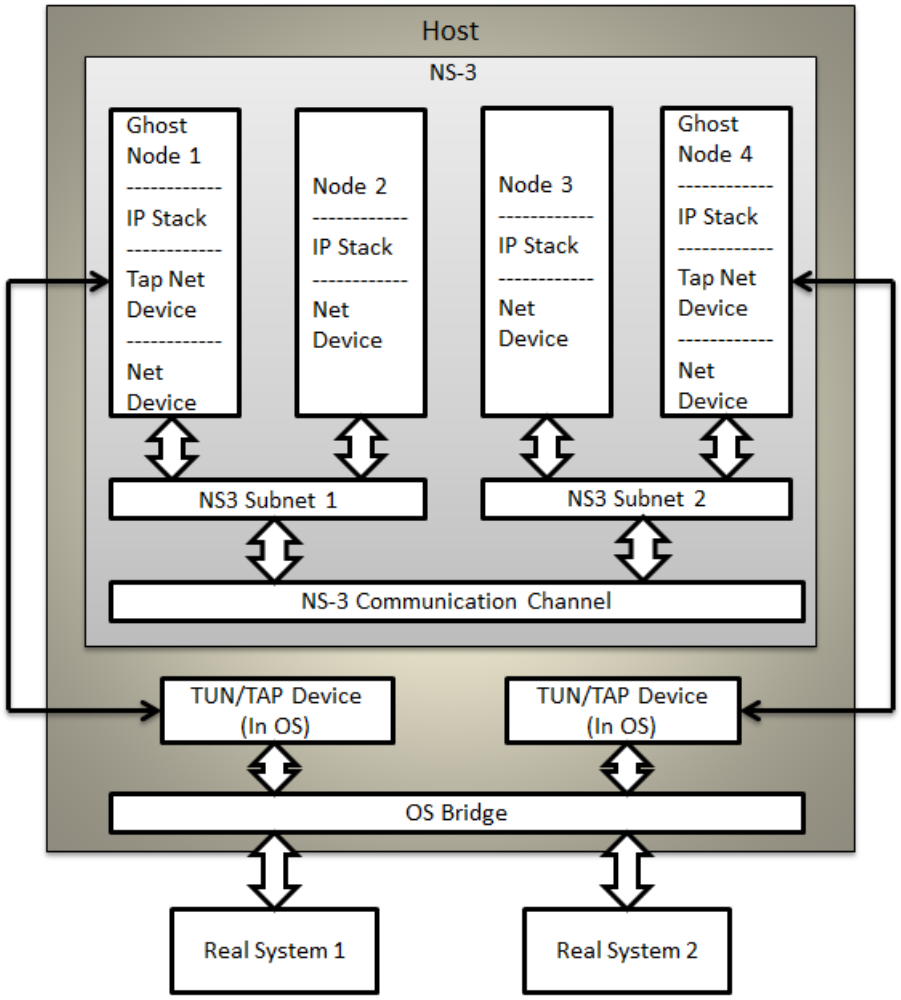

Figure 3.3: Expected NS3 emulation mode configuration

In figure 3.3, the conceptual representation of how NS3 is to be setup for the purpose of simulating the communication for real end systems with UseBridge mode of the tap net device is shown. Here, a real system refers to an end system, which is to send/receive data. The OS bridge is a software bridge defined inside the host OS. It is completely a software bridge and exists only in the Linux kernel. The tap devices shown are TUN/TAP devices which are software only, virtual Ethernet ports [3.10]. These devices also exist only in the OS and can be configured to be used in a variety of ways. In this case, the TUN/TAP device is configured to connect to a user defined application, which is NS3 and act as a data transport

interface. The Tap net device is to be used in 'UseBridge' mode, which means that the NS3 only needs to know the name of the TAP device to be able to use it as the data transport interface for that node. The node which has the Tap net device configured in it is called a ghost node since it is used only for the purpose of communicating with the tap device through the tap bridge and serves no other purpose in the NS3 simulation. The ghost node uses the node connected to its own subnet for forwarding the packet to other nodes in the simulation. The subnet 1 and subnet 2 are LAN networks. NS3 communication channel configuration will depend on the topology defined in the simulation.

Now that the setup has been explained, an insight into the data transfer mechanism is provided here. For this purpose, assume that the real system 1, ghost node 1 and node 2 are on the 192.168.1.0/24 subnet, and that the real system 2, node 3 and ghost node 4 are on the 192.168.2.0/24 subnet. The real system devices will see the NS3 nodes in their own subnet as if they are on the same physical LAN. The scenario is that real system 1 is to send data packets to real system 2. The gateway to reach subnet 2 from real system 1 needs to be set as the IP address of node 2 for the network device on real system 1. Similarly, on real system 2, the gateway to reach subnet 1 has to be set as the IP address of node 3. In this scenario, real system 1 generates the data packets and sends it to the Linux host bridge. The Linux host bridge forwards the packet to the appropriate TUN/TAP device in the OS. The Tap net device receives the data from the tap device and sends it through the communication channel being simulated in NS3 to ghost node 4. Now, data from the Tap net device is written to the appropriate TUN/TAP device in the Linux OS. The packet is forwarded off to the Linux OS Bridge, which forwards it to real system 2.

3.4 Cyber-Physical Test Bed

The cyber-physical test bed can be set up to work under different configurations. In this section, the set up for the standard IEEE 14 bus test case is described as an example. The RSCAD model data for IEEE 14 bus power system test case to be simulated in the RTDS is

shown in appendix A. The data used in creation of the model is given in [3.11]. There are a total of fourteen PMUs available including eight GTNET software PMUs, two SEL 421s with two input channels each, and one each of GE D60, TESLA 4000. The PMUs are configured to send phasor data at the rate of 60 samples per second. A real node sees the simulation node on the same subnet as if it were a local device. Therefore, by assigning IP address of the PDCs to the different subnets configured in NS3, the devices are able to see their respective gateway nodes in the simulation through which data is sent to the control center PDC. The SEL software and hardware PDCs are used to concentrate data at the substations. At the control center, openPDC is used to concentrate data from all the substations.

The data concentrated by openPDC is stored in a local database at the control center. Additionally, the PDCs at the substation also have their own local database where they archive the local PMU data. PMU data can be vital for post-mortem analysis and for studying any disturbance in the power grid. In order to prevent loss of data in the event of a communication failure with the substation, local substation databases continue to archive data which can be retrieved once communication is reestablished. However, it is to be noted that the database size will not be very large since its primary usage is to serve as a backup for a short duration of time till the communication failure is corrected. The time critical end applications need data from the database as soon as it is available. For this purpose, we use scripts to read data from the database, time-align the data and feed them as input to the applications. Depending on the application the requirement of data might vary. For accessing the SEL PDC databases, a python program interacts with the MySQL database in which the historian is present. The data is written to the historian in chunks. The program is written such that it waits for fresh data to be inserted into the historian and the extracts the new data and writes it to the output file. The program runs in an infinite loop that goes on till it is manually terminated. The flow chart for this script is given in figure 3.4.

The openPDC database is accessed using a Matlab script. The script checks if the database has been updated. If there is new data, then the data is read into a matrix. This matrix is predefined with the inputs that need to be time aligned. This process is repeated until at least one line in the matrix is completely filled. Once the line is filled, all complete rows are written to a text file in a format preferable to be read by the end application. All incomplete rows above the complete row are deleted since it is of no use for the end application unless it is a historical analysis application. This takes of time alignment, and incomplete data set issues.

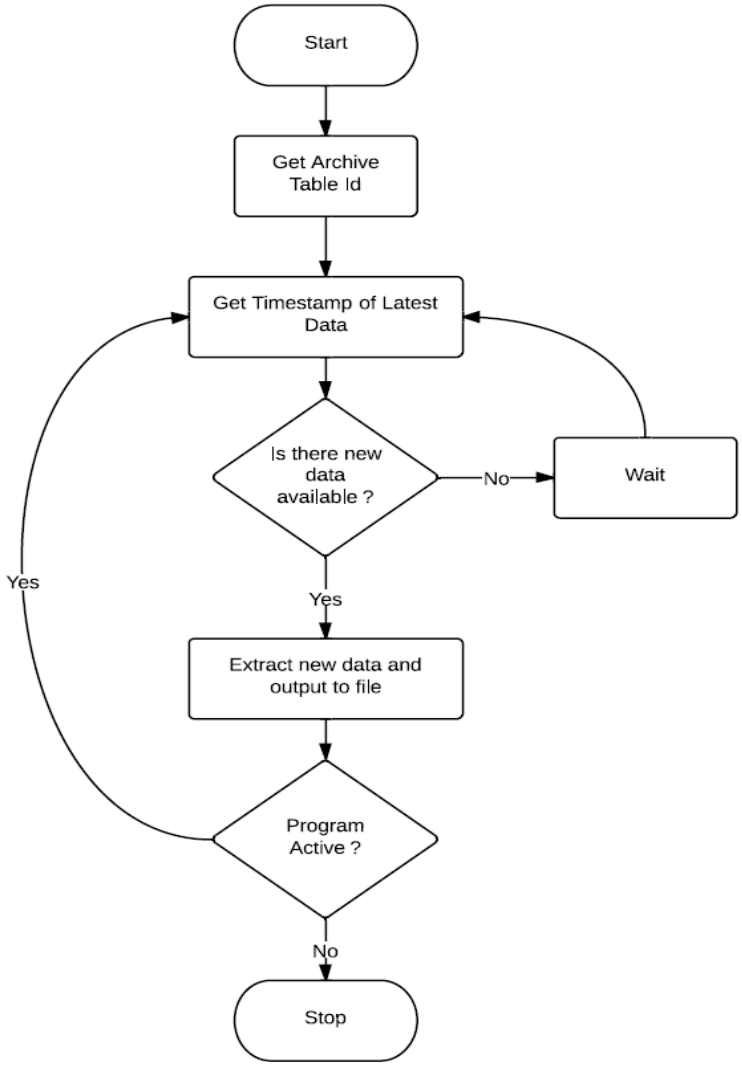

Figure 3.4: Script for accessing SEL PDC database

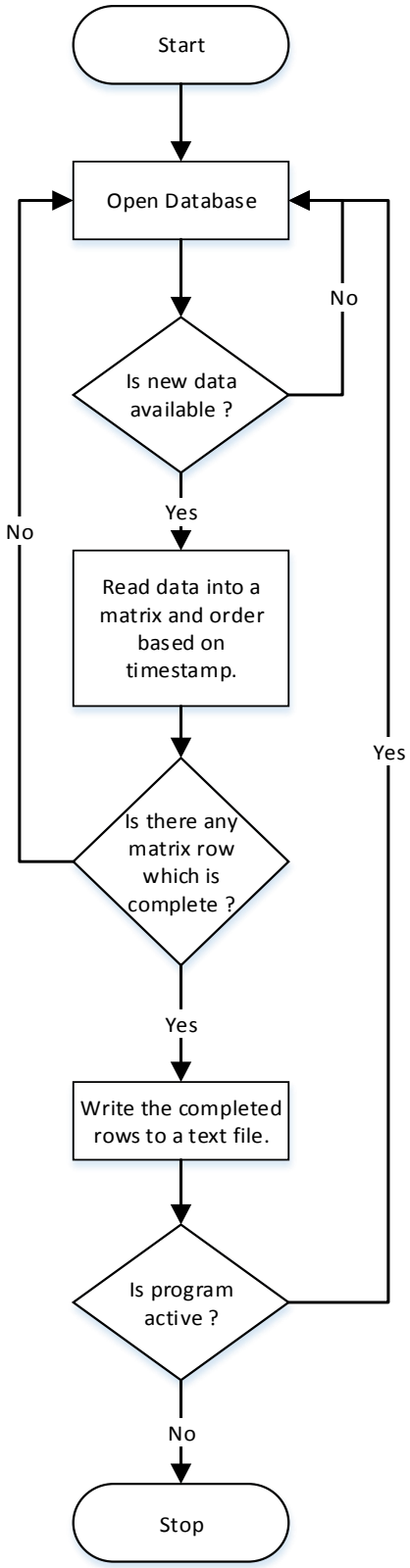

Figure 3.5: Script for accessing openPDC database.

The substation view and control center view are presented in figure 3.6. In the substation view, it is shown that there are multiple PMUs sending phasor data to the PDC, which has a local database and is connected to the control center PDC through NS3. Additionally, engineering access might also be needed to change settings in the PMUs or to retrieve event data which also happens through NS3 should a request come from the control center.

In the control center view, the PDC receives phasor data from different substation PDCs. The data is then stored in a database local to the control center. Applications which require these data receive them from data retrieval scripts. If any control algorithm is running at the control center, the control actions specified are transmitted to the PMUs through NS3. These control signals are then sent back to RTDS through hardwiring of terminals between the PMUs and RTDS. It is to be noted here that only the physical PMUs have this hardwiring option and the software PMUs do not have this option.

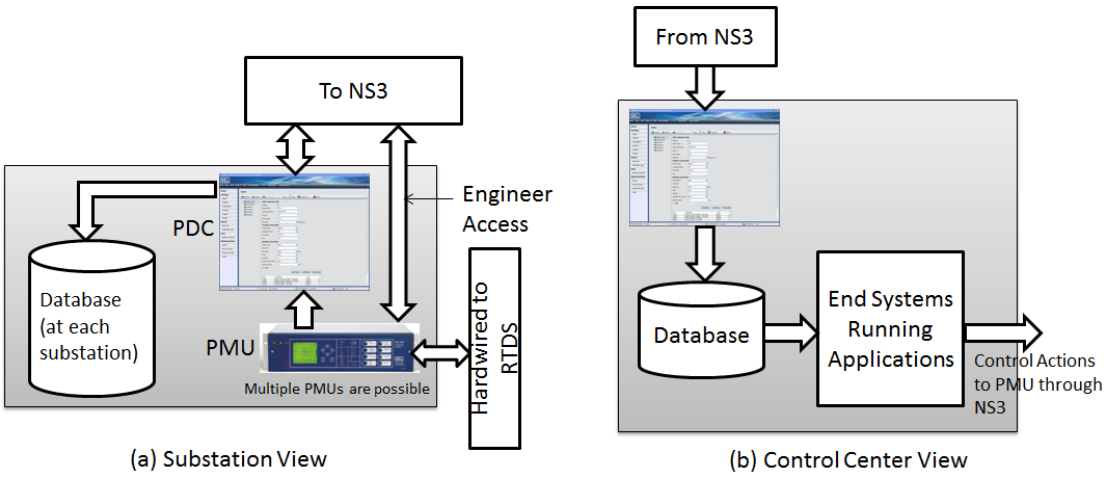

Figure 3.6: The substation and control center view of the test bed.

The complete integrated cyber-physical test bed is shown in figure 3.7. Providing a short recap; the loop starts with the RTDS simulating the power system and giving out signals to measurement devices. The measurement devices then send the data to local PDCs which send them to the control center PDCs through the NS3 communication backbone. The control

actions if any are conveyed through the NS3 network. The final action taken by the relay such as opening of a breaker is sent back to the RTDS through the hardwiring interface.

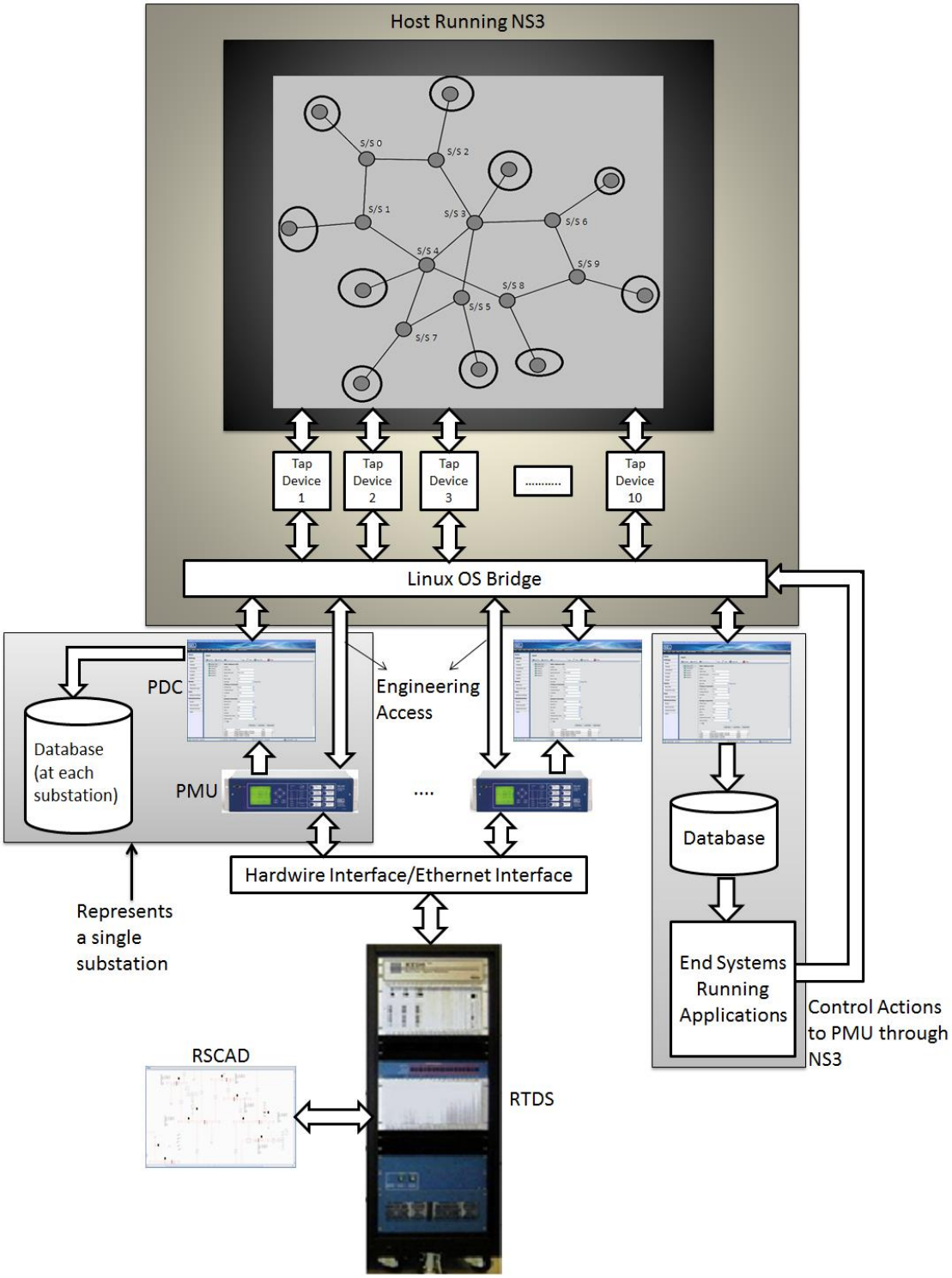

Figure 3.7: Complete cyber-physical test bed setup

3.5 Operational Modes of the Test Bed

The NS3 simulation can have a combination of simulated, virtual, or real devices as data sources/sinks, using the NS3 communication channel. Simulated devices are completely inside the NS3 simulation itself. By configuring applications and data sinks in the NS3 simulation script, simulated data sources can be setup. The virtual data sources are an interesting option. It is possible to have virtual machine environments to act as data sources and sinks by writing applications inside the individual platforms. There are some timing issues when running several virtual environments in the same host, which are well documented in [3.12]. An alternative to using a full virtual machine is the use of Linux containers. Linux containers provide operating system-level virtualization, which is not a full virtual machine, but rather it provides a lightweight virtual environment that has its own processes and network space. Reference [3.13] provides a simple tutorial on how Linux container maybe used as virtual nodes in NS3 simulations.

3.6 Evaluation of Operation

For verifying the operation of the network simulator, a Linux based PC was placed at the slack bus and Internet Control Message Protocol (ICMP) packets are sent to each gateway in the network using the default ping application available in Linux. The results are plotted in figure 3.8.

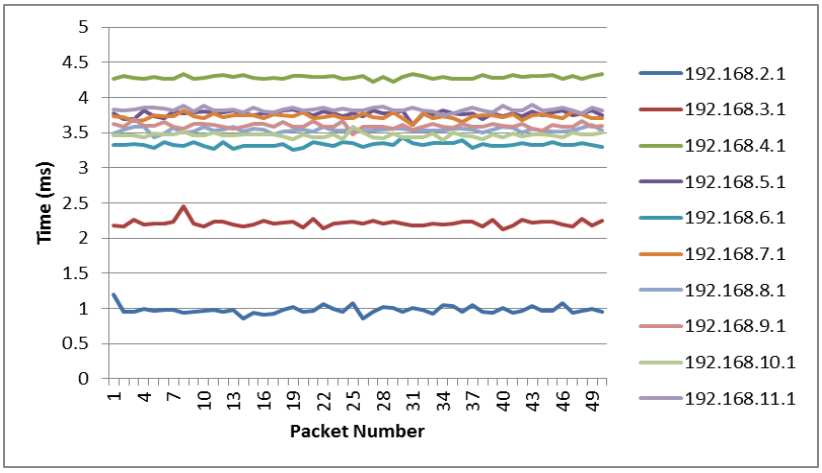

Figure 3.8: Round trip time between real host and gateways at each node.

The IP addresses shown are the gateway IPs from node 0 from node 9. It has been verified that the delays seen are close to the configured delays in the communication network simulator. Figure 3.9 shows a sample of the delay introduced on the reception of PMU packets at the assumed control center due to the presence of the network simulator in the test bed loop.

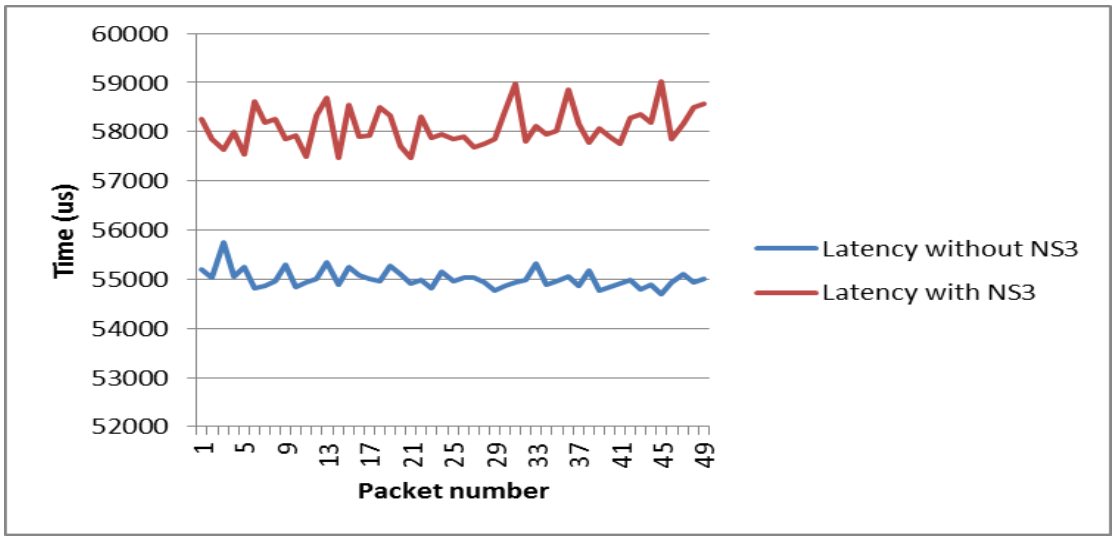

Figure 3.9: Latency measurement with and without NS3 in the loop

3.7 Time Synchronization

At this point, it is important to emphasize and clarify about the different time domains that are encountered in the test bed. There are essentially four time domains involved: power system simulation, network simulation, monitoring & control system, and application execution. The power system simulation using RTDS is called a real time simulation since it is able to run with a time-step of 50 micro seconds. Hence, the underlying power system simulator is able to produce data points to be measured by the PMUs without any delays. The network simulation needs to emulate the delays encountered in the communication system. For this purpose, the simulator just needs to guarantee that it is able to emulate the necessary delays within a certain error limit. The measurements are made by actual PMUs and control actions such as a breaker

opening or closing is done through actuating relay contacts. Hence, the operation time of these components is the same as that encountered in a real system. For application execution, the execution times may vary depending on the workstation used to run it. Additionally, the frequency of application execution may not necessarily be as fast as possible. It may depend on other factors such as criticality of the application. Hence, it is sufficient to run the application on a dedicated workstation for the test bed. Due to all these factors, the operation of the cyber-physical test bed is said to be in real time.

3.8 Summary

The test bed components have been listed and a short description for each resource has been reviewed. The working of NS3 in emulation mode using real time scheduler (wall clock) is explained along with an example. It is observed that NS3 can send and receive data from external devices in addition to being able to carry real network data between real end systems. The integration of RTDS, NS3, and other components resulting in a Cyber-Physical test bed has been explained. In addition to these, the data delivery mechanisms to end applications in the test bed have also been discussed with flow charts for better understandings.

3.9 References

[3.1] RTDS Official Website. [Online]. Available: http://rtds.com/hardware/gtnet/gtnet .html

[3.2] MiCOM Alstom P847 Manual. [Online]. Availabel: http://www.alstom.com/grid/ products-and-services/Substation-automation-system/protection-relays/MiCOM-Alstom-P847/

[3.3] GE Digital Energy. [Online]. Available: http://www.gedigitalenergy.com/multilin /catalog/d60.htm

[3.4] ERL Phase Power Technologies [Online]. Available: http://www.erlphase.com/products.php?ID=TESLA%204000

[3.5] Schweitzer Engineering Laboratories. [Online]. Available: https://www.selinc.com/

[3.6] Ponovo. [Online]. Available: http://www.relaytest.com/product_category.php?ID=3

[3.7] openPDC Project. [Online]. Available: http://openpdc.codeplex.com/

[3.8] ORBIT Official Website. [Online]. Available: http://www.orbit-lab.org/

[3.9] NS-3 Model Library, 21 December 2012. [Online]. Available: http://www.nsnam.org/docs/release/3.16/models/ns-3-model-library.pdf

[3.10] Tun/Tap Interface Tutorial. [Online]. Available: http://backreference.org/2010/03/26/tuntap-interface-tutorial/

[3.11] LXC Linux Containers. [Online]. Available: http://lxc.sourceforge.net/

[3.12] IEEE 14 bus data in common data format. [Online]. Available: http://www.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm

[3.13] David Nicol, "Simulation & Emulation in Smart Grid Assessment", TCIPG Seminar, 5 Oct 2012. [Online]. Available: http://tcipg.org/tcipg-seminars#archives

CHAPTER FOUR

APPLICATIONS OF CYBER-PHYSICAL TEST BED

4.1 Introduction

This chapter provides a discussion of the different applications that are implemented and tested using the developed cyber-physical test bed. A brief introduction to some of the emerging applications used in the smart grid is provided. Each application has different requirements, which include: number of data point tags, rate of data input, frequency of application usage etc. Depending on the scenario required for specific application testing, the overall test bed described in section 3.4 needs to be adapted to the needs of the application.

4.2 Power Grid Applications

In order to avoid major system failures and regional blackouts due to lack of monitoring and situation awareness, electric utilities have installed Supervisory Control and Data Acquisition (SCADA) systems to support computer-based systems at the energy control center. SCADA systems poll Intelligent Electronic Devices (IED) in the field for data through suitable protocols such as Distributed Network Protocol 3.0 (DNP3). The polling happens every 2-4 seconds. The SCADA system polling is not time synchronized, and hence the obtained data is not from a single snapshot of the system; rather it represents measurements taken between intervals of time. With the availability of GPS Synchronized time stamped data from PMUs, this problem can be overcome. The database created by the data acquisition systems is intended for use by a number of application programs to monitor and assess the state and stability of the system.

1. State Estimator: State estimator is an essential tool which is used to estimate the state of the power grid from measurements such as voltage magnitude, real power

generation, real power consumption etc. It is important to get a best possible estimate of the given state of the system before any analysis. Applications such as power flow require some indirect computed values including the real and reactive power injections at a bus. Additionally, errors in the measurements can lead to non-convergence of the power flow. These limitations are overcome by the use of state estimator which is used to estimate the system states and remove errors present in the measurements to a certain degree [4.1]. The EPG is inherently built with redundant measurements and these are used in the state estimator to help identify and eliminate bad data. The output of the state estimator represents the state of the system, which is then used to run other applications such as power flow, contingency analysis, small signal stability, dynamic security assessment etc.

2. Small-Signal Stability: Small signal stability of the power grid is defined as its ability to maintain synchronism when subjected to small disturbances. The small-signal stability problem is usually one of insufficient damping of system oscillations. Small-signal analysis using linear techniques provides valuable information about the inherent dynamic characteristics of the power system [4.2]. The phasor-based Real Time Dynamics Monitoring System (Phasor-RTDMS) is one such implementation. During the WECC 1996 blackout, the model based estimations had estimated/predicted a stable state. However, using the Phasor-RTDMS to study the blackout, it was found that there were negatively damped oscillations present in the system which had led to the blackout [4.3].
3. Voltage Stability: Voltage Stability is concerned with the ability of a power system to maintain acceptable voltages at all buses in the system under normal conditions and after being subjected to a disturbance. A system enters a state of voltage instability when a disturbance, increase in load demand, or change in system condition causes a progressive and controllable decline in voltage. The main factor

causing instability of the power system is the inability of the power system to satisfy the reactive power demand in the system. Voltage instability has been identified as the cause of several major systems collapses [4.2]. Control actions typically involve switching on capacitor banks, bringing on synchronous condensers or shedding load.

4. Post-Mortem Analysis: When a contingency occurs in the system triggering wide area impact, it is important to carry out a post-mortem analysis to uncover the cause and possible control actions that could have been taken to avoid such a situation. Several gigabytes of system conditions data along with required auxiliary data is archived for this purpose.

4.3 Latency and Bandwidth Analysis

The offline simulation for the latency and link utilization analysis using NS2 and NS3 has been provided in chapter 2. The same analysis can be done using the real time test bed. This replicates a more realistic analysis, although it is not scalable. For the purpose of latency and bandwidth analysis, the following are the requirements:

1. There is assumed to be at most one PMU at each bus in the system. For the IEEE 14 bus system, this constitutes fourteen PMUs spread across ten nodes. It has already been established that there are 14 PMUs available and hence this topology is possible.
2. The communication network topology assumptions are the same as described in chapter 2.

The overall test bed setup for enabling the latency and link bandwidth utilization analysis is shown in figure 4.1.

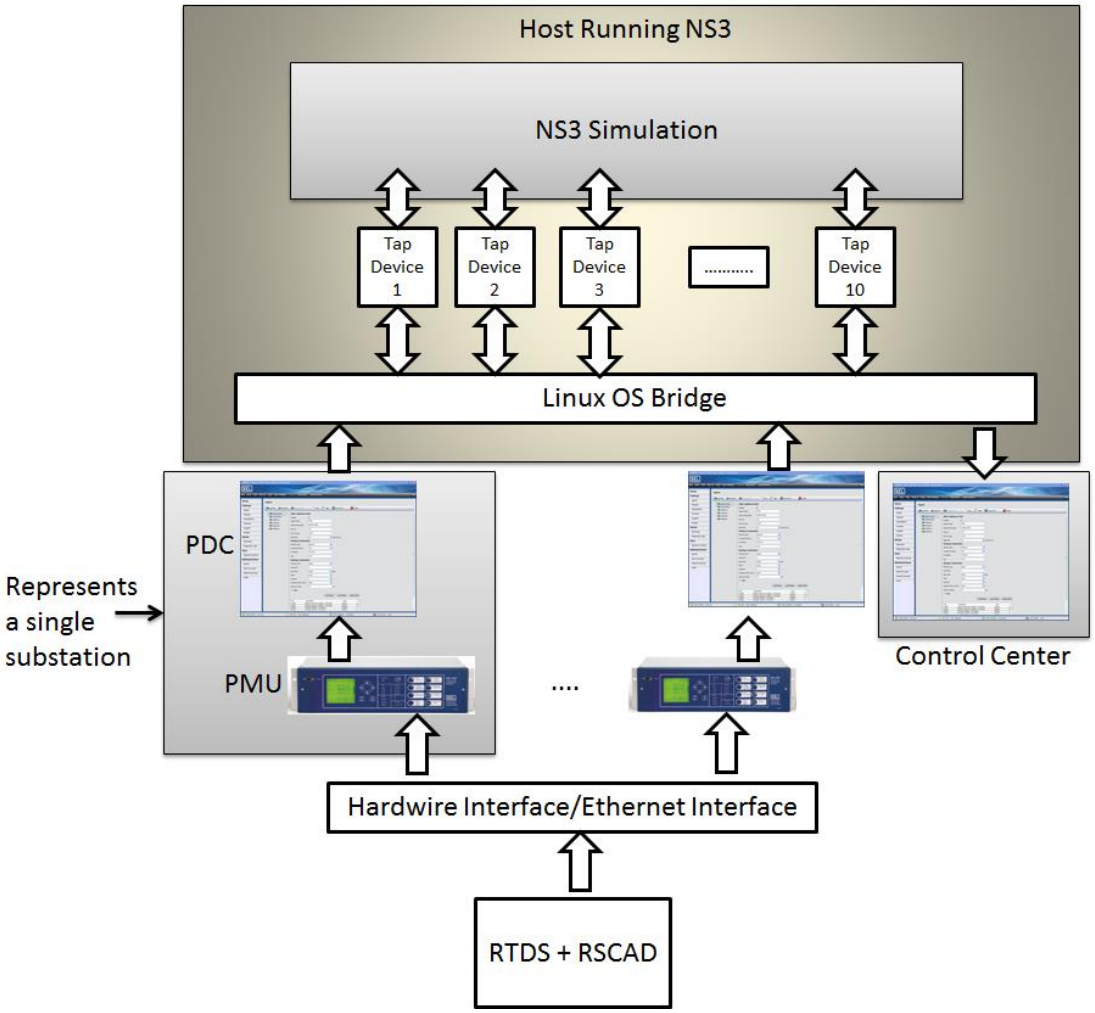

Figure 4.1: Test Bed setup for Latency and Bandwidth utilization analysis

The arrows represent the direction of data flow between the devices. The PMUs receive measurements signals from the RTDS and estimate the phasors. The phasor measurements are then concentrated at the substation PDCs before being sent out the control center. At the control center end, SEL 5073 PDC is used for concentrating the data from the substations. The SEL 5073 has an inherent way of calculating the latency of the tags received based on the comparison of timestamps. For the purpose of link bandwidth analysis, the NS3 trace files generated are analyzed using the scripts discussed in section 3.4. It has been discussed in section 3.5 that it is possible to have virtual and real end systems running together. While it is certainly possible to use simulated or virtual nodes, an alternative to replicating a PMU for the purpose of analysis can be done using openPDC. For the purpose of

latency/link bandwidth utilization analysis, it is not important to transfer actual estimated phasor data. It would be fine to use a single PMU output replicated fourteen times to replicate the presence of fourteen PMUs in the network. openPDC has the option of creating virtual outputs, where a real PMU input to the openPDC is mapped to tags belonging to the virtual PMU. This virtual PMU can then be used as a source PMU to the control center PDC. In this way, it would be possible to have a number of virtual PMUs apart from the actual physical PMUs.

4.4 Application and Device Testing Using the Test Bed

This section provides an insight into how the test bed can be used in different configurations to enable the testing of different applications that may be used in the EPG.

4.4.1 Local Voltage Stability Monitoring Algorithm

The development of the algorithm is not within the scope of this thesis. Hence, no details on the algorithm are provided here, and only the implementation is discussed [4.4-4.5]. The requirements of the algorithm are stated as follows:

1. The Local Voltage Stability Monitoring Algorithm (LVSMA) is to be run in substations only. As such a substation computer is required to carry out the analysis locally at the substation. For this purpose, the SEL 3354 substation computer is used.
2. In addition to the local phasor data, the algorithm requires the use of voltage angle of the slack bus to obtain the angles with reference to the slack bus. So, the slack bus voltage angle is sent to each substation in the network.
3. The calculated voltage stability index is then transferred to the control center through the communication network. A control algorithm may be present at the local or the control center. This algorithm is responsible for taking any control actions necessary to avoid voltage collage due to voltage instability.
4. The application running time is in the range of microseconds. Hence the application running frequency is restricted only by the availability of data.

The test bed setup for the LVSMA application is shown in figure 4.2.

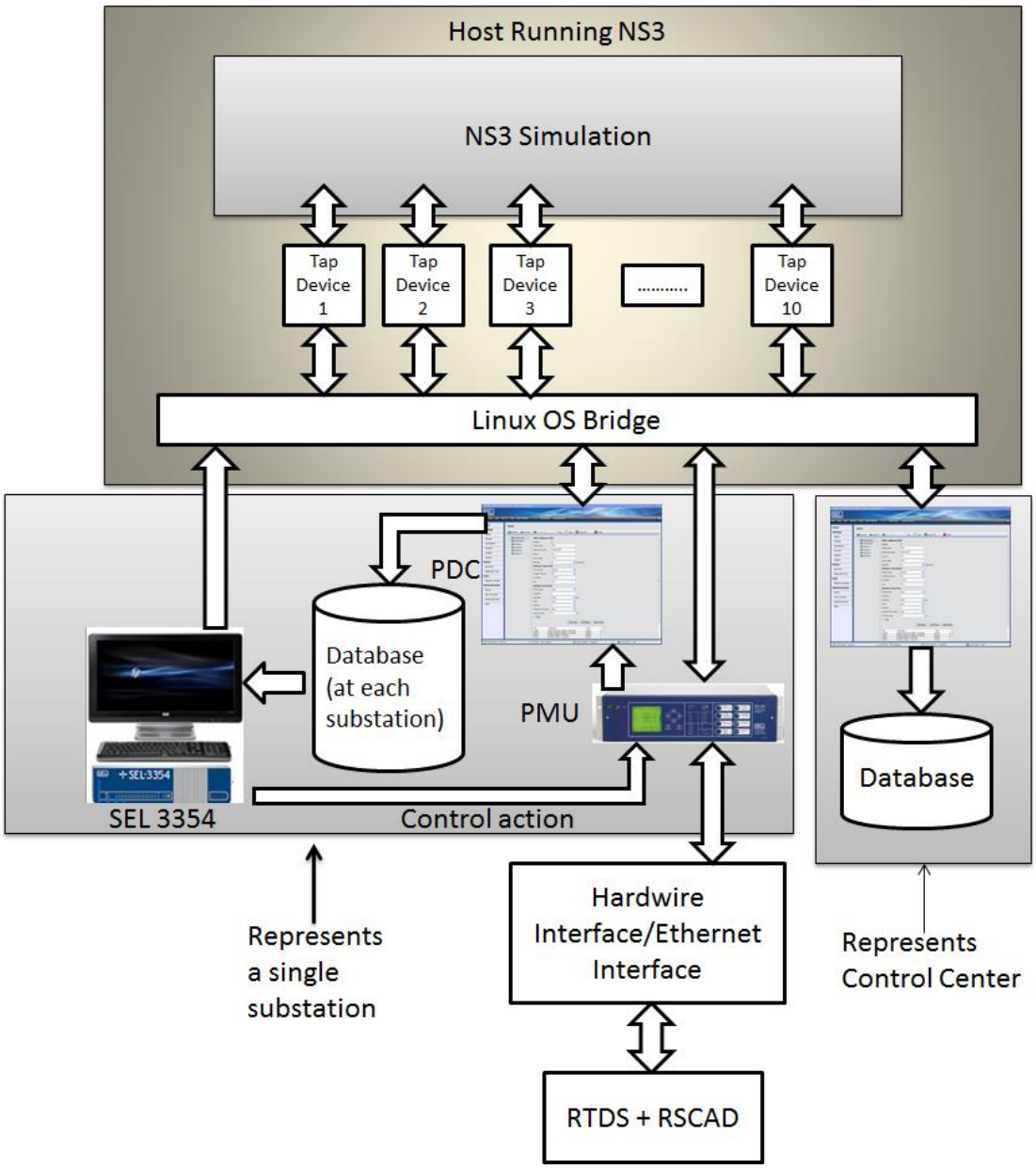

Figure 4.2: Test bed setup for testing LVSMA

The substation PDC receives the voltage angle from the slack bus through the control center PDC. The scripts for obtaining data from the database at the substation are executed locally in the substation computer. The local VSMA is computed and based on the index; control action might be taken to prevent a voltage instability situation.

4.4.2 Wide Area Voltage Stability Monitoring Algorithm

The Wide Area Voltage Stability Monitoring Algorithm (WAVSMA) is a wide area monitoring system tool. The requirements of this application are as follows:

1. The WAVSMA tool is assumed to be run at the control center. However, it could be used at different locations depending on necessity. One of the Dell precision workstations available in the test bed is used as the platform for running the tool.
2. The application needs the voltage phasor, current phasor and the net power injections of each bus in the system in addition to the breaker status.
3. The WAVSMA calculates the voltage stability assessment index, and based on this any necessary control action may be taken. The control action is relayed to the appropriate substation for action.

This setup is very similar to the one described in section 4.3.1. All substation PDCs send their phasor data to the control center PDC, where a script is used to retrieve the data in the format the application expects it. It is to be noted here that the algorithm running time is small, and the frequency of application execution is restricted generally by the rate of data input. Any control action specified by the application is relayed to the appropriate substation through the use of NS3 communication channels.

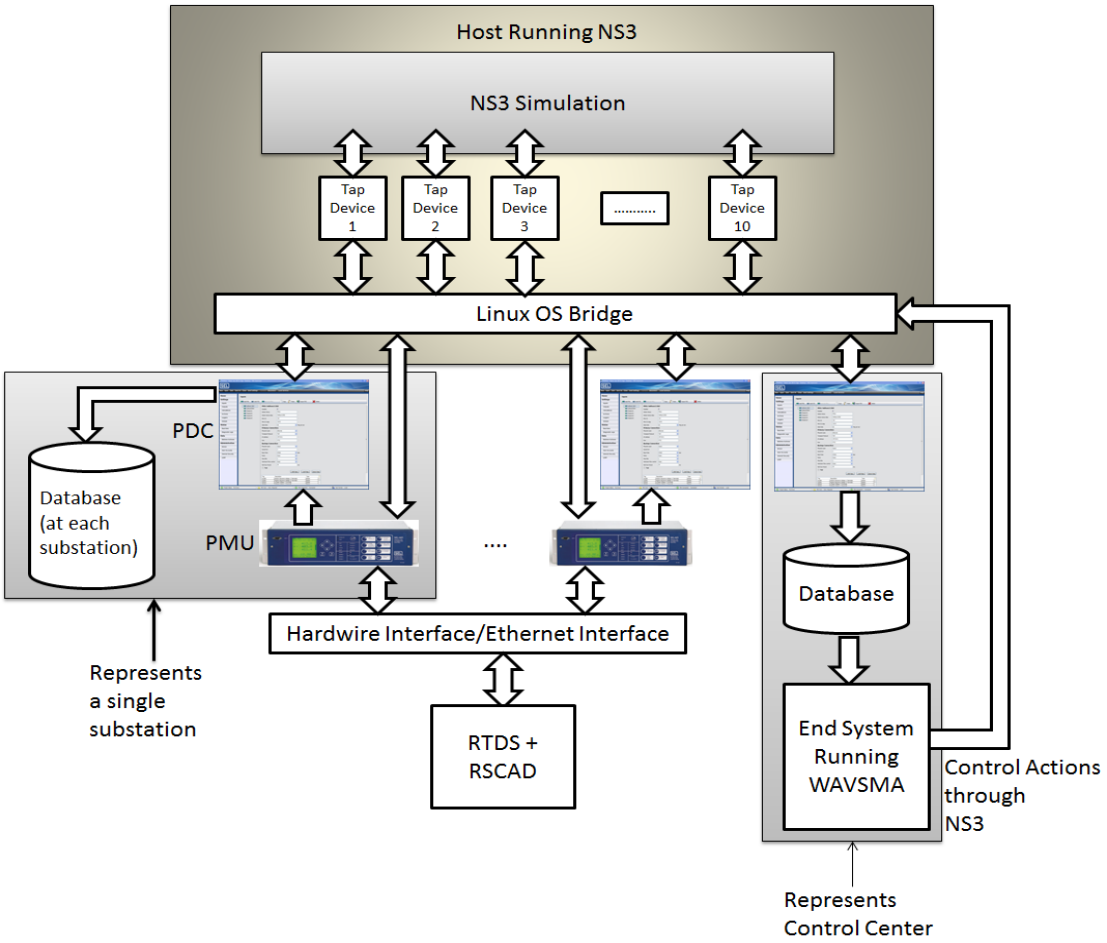

Figure 4.3: Test bed setup for testing WAVSMA

4.4.3 Shipboard Power System Reconfiguration

The Shipboard Power System Reconfiguration Algorithm (SPSRA) is an application that does not use any PMU data. It is assumed here that all the data communication is through DNP. It is a genetic algorithm based application. The algorithm is written in structured text and is run inside the SEL 3530 RTAC. The algorithm needs the power generation, load and breaker status data in the system. In the event of generation loss due to a contingency, the RTAC computes the reconfiguration algorithm based on the load priorities assigned to reroute power to the most critical loads. Figure 4.4 shows the test bed setup for SPSRA.

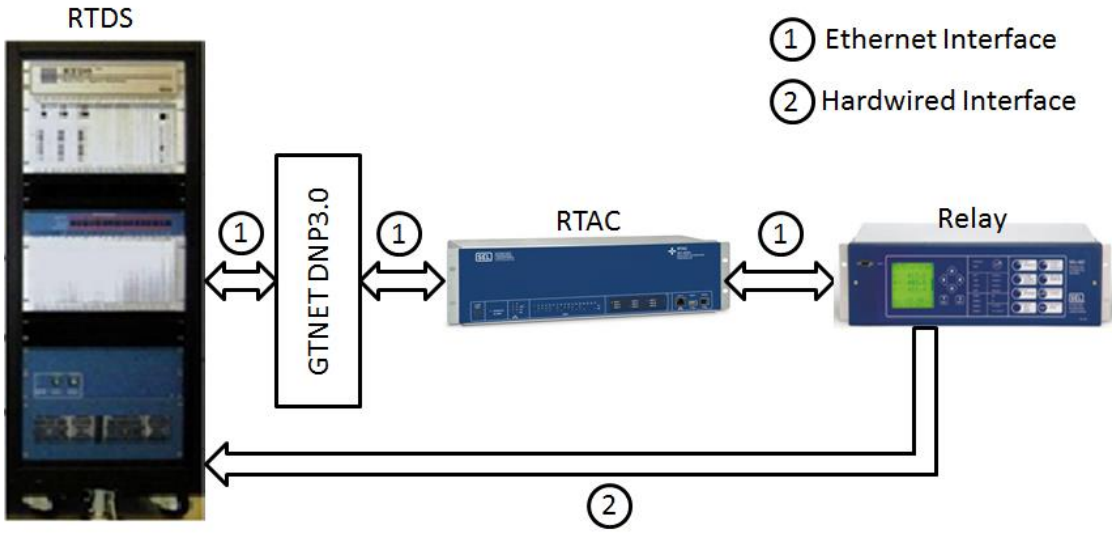

Figure 4.4: Test Bed setup for SPSRA

4.4.4 Aurora Attack Simulation

An introduction to the Aurora attack has been given in section 1.3.5. The simulation of the attack using RTDS will be discussed in this section. The generator to attack for the IEEE 14 bus system was selected based on the integration of the generator contingency ranking based on incomplete information and cyber vulnerability index for relays [4.6]. Four different cases were simulated. The first two cases represent an 'N-1' contingency situation. The other two cases represent an 'N-2' contingency situation.

Case 1:- Breaker opened for 0.25 seconds and closed for 0.25 seconds, single generator (G5) attack (scenario 1): The results obtained are shown in figure 4.5. It was observed that there is rapid variation in the electrical torque, current, speed and power output of the machine. When the machine is connected out of phase with the grid, it experiences a synchronizing torque which tries to pull the machine back into synchronism. The machine experiences very high mechanical stress which will lead to potentially irreversible damage to the machine.

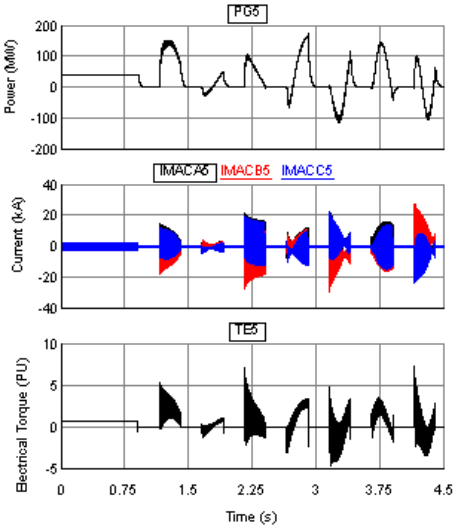

Figure 4.5: Power Output, Current, Electrical Torque for Case 1 in RTDS

Case 2:- Breaker opened for 0.25 seconds and closed for 0.75 seconds, single generator (G5) attack (scenario 2): Simulation results are shown in figure 4.6.

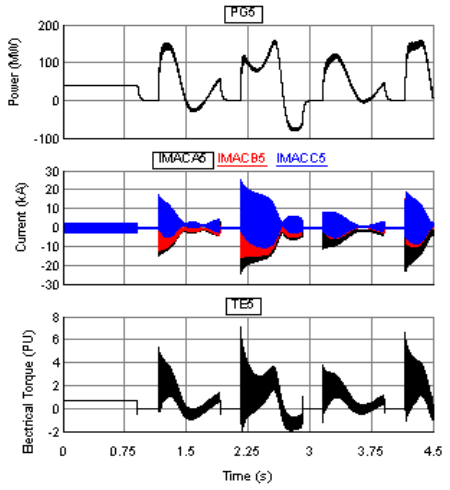

Figure 4.6: Power Output, Current, Electrical Torque for Case 2 in RTDS

Case 3:- Breaker opened for 0.25 seconds and closed for 0.25 seconds, two generator attack (G3 and G5) (scenario 1): In this case, the attack is coordinated to attack two generators simultaneously. G3 and G5 are selected based on the contingency ranking. This is repeated six times and then the generators are taken out of the system to simulate effect on system due to loss of the generators. It was observed that there is a voltage collapse as the power required cannot be supplied by the slack bus/other

generators due to capacity limitations. This leads to a blackout. Simulation results from RTDS are shown in figure 4.7.

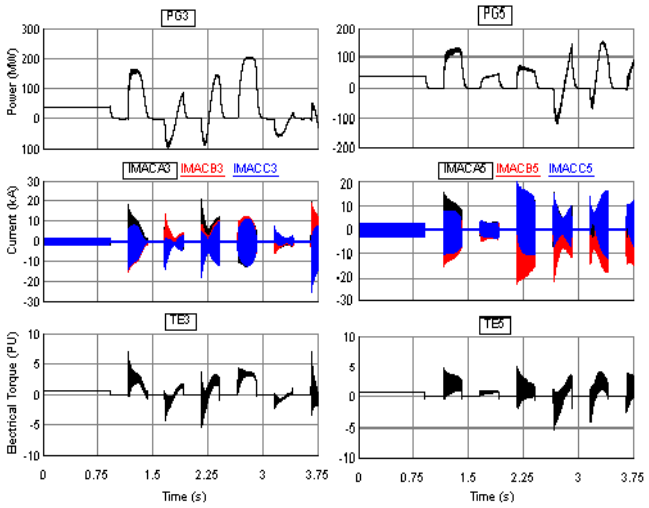

Figure 4.7: Power Output, Current, Electrical Torque for Case 3 in RTDS

Case 4:- Breaker opened for 0.25 seconds and closed for 0.75 seconds, two generator attack (G3 and G5, scenario 2): Simulation results are shown in figure 4.8.

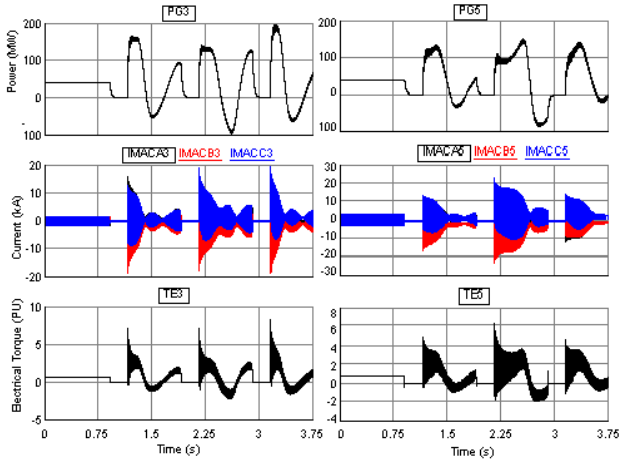

Figure 4.8: Power Output, Current, Torque for Case 4 in RTDS

These results demonstrate the impact of an Aurora kind of attack on the test case considered here. Repeated transients such as the ones seen in the simulation will lead to potential damage to generators. The generators will not be available for restoration operation.

The above attack is completely simulated in the RTDS i.e., no hardware components in the test bed are used to complement the simulation. The test bed can be used to simulate the

complete cyber-physical interaction apart from the security aspect since NS3 does not have an inherent security model. The test bed setup to enable the Aurora attack to be simulated is shown in figure 4.9. The test bed has the same setup as in the case of WAVSMA. However, since the motive here is to simulate an Aurora attack and not data delivery, we ignore the data delivery aspects and consider only the engineer access to the relays through the NS3 communication channel. It can be assumed that an attacker has hacked into the communication system and gained access to the relay through the engineer access mechanism. Through the use of suitable software, the relay timers are programmed to toggle the output contacts connected to the breaker trip and close terminals. The timers can be programmed with the intervals that have been discussed previously in this section. In this way, the breakers will be closed and opened based on the interval the timers are set for repeatedly till the generator blows out or if the relay is reprogrammed to prevent this operation.

4.4.5 Phasor Data Concentrator Testing

For the purpose of testing the operation of Phasor Data Concentrators (PDC), the test bed setup shown in figure 4.3 can be used. By manipulating the position of PDCs in the network, it is possible to have a combination of local PDCs and super PDCs configured in the network. NS3 allows for implementation of error models in communication channels to induce data corruption, and data loss. Additionally, by controlling the bandwidth setting of the communication channels, it is possible to cause the loss of some packets in the network. By controlling these parameters, various scenarios can be created under which the PDCs can be tested [4.7].

4.5 Summary

An introduction to few of the applications used in the smart grid is given at the beginning of the chapter. The cyber-power system test bed has been developed for the purpose of analyzing applications. Some of the applications that have been/ will be tested

using the test bed have also been discussed. The changes that need to be made in the test bed for enabling the testing of these applications are listed and the setup is explained with supporting layout diagrams.

4.6 References

[4.1] J. J. Grainger and W. D. Stevenson, Power System Analysis, McGraw-Hill, pp. 562-572 & 641-687, 1994.

[4.2] Prabha Kundur, Power System Stability and Control, McGraw-Hill, pp. 700-1022, 1994.

[4.3] Vaithianathan (Mani) Venkatasubramanian, Y. Li, "Analysis of 1996 Western American Electric Blackouts", Bulk Power System Dynamics and Control - VI, pp. 685-721, August 22-27, 2004.

[4.4] S. Biswas, C. Vellaithurai, A. Srivastava, "A Fast Algorithm for Voltage Stability Monitoring of Power Systems with Consideration of Load Models", accepted for publication, IEEE Industry Applications Society.

[4.5] S. Biswas, Jeong Hun Kim, A. Srivastava, "Development of a smart grid test bed and applications in PMU and PDC testing", North American Power Symposium (NAPS), 2012 , pp. 1-6, September 9-11, 2012.

[4.6] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, P. Shengyi, U. Adhikari, "Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information", IEEE Transactions on Smart Grid, vol.4, no.1, pp. 235-244, March 2013.

[4.7] S. Biswas, A. Srivastava, "A Novel Method for Distributed Real Time Voltage Stability Monitoring using Synchrophasor Measurements", IREP Bulk Power System Dynamics and Control Symposium, August 25-30, 2013.

CHAPTER FIVE

A TRAINING SIMULATOR FOR CYBER-POWER INFRASTRUCTURE SECURITY

5.1 Introduction

In order to guarantee secure energy delivery to loads and protect power grid infrastructure, power system operators should monitor and control the cyber network along with the physical system. Traditionally, these operators gain experience and expertise through working with an actual system. The down side to this is that even a simple mistake may result in catastrophic consequences such as a cascading failure leading to a blackout. Hence, a better training and transfer of experience is needed to make sure that inexperienced operators can acquire experience without any damage to the grid. In order to satisfy this requirement, Operator Training Simulators (OTS) are used to simulate the electrical network with the user interface reflecting that of the one used in an actual control center. This enables the training of operators without having to worry about consequences to the grid. The fundamental limitations of static and dynamic attack detection and their identification procedures are studied in [5.1]. Counter measures against arbitrary unobservable attacks on SCADA/EMS using known secure PMUs in the system is studied in [5.2]. None of the above mentioned solutions aims at training operators regarding the cyber threats and possible countermeasures. The objective of this chapter is to lay out a conceptual integration of a cyber-attack simulator into an existing OTS, to study the difference in operator response to contingencies with/without the cyber simulator.

5.1.1 Operator Training Simulator

OTS simulates the electrical network, user interface and power system behavior. The training simulator simulates the power system in a realistic manner by providing static and dynamic responses to the Operators actions which are similar to those observed by the

Operator in a real control center. The OTS has three distinct functional areas: Power system model, control center model, and the instructor model. It provides a realistic environment for operators to practice operating under normal, emergency or restorative conditions. The data delivery rate of the OTS is also adjusted to mimic the data acquisition rate of the control center thereby providing the real time simulation element associated with a real environment. However, OTS does not simulate the cyber-side of the power grid and concentrates on simulation of the physical power system only. Some of the available OTS are:

1. Power Simulator 5 from IncSys
2. E-Terrasimulator from Alstom
3. ABB OTS
4. OpenOTS from Open Systems International

5.1.2 Power Simulator 5

PowerSimulator has been built by a cooperative effort from EPRI (Palo Alto, California), Incremental Systems (IncSys) (Bellevue, Washington) and PowerData Corporation (Bellevue, Washington). It simulates the power system behavior under a wide range of conditions including thermal system overload, voltage collapse, off-nominal frequency, Ferranti voltage rise, system islands, large angle variations and cold load pickup. There are three major versions of the PowerSimulator: Custom, Generic and Replica. Each of these comes with varying levels of detail. For our simulation purposes we use the Generic PowerSimulator. It uses a hypothetical generic power system model called the PALCO system to provide realistic power system experience. Figure 5.1 shows the details of the PALCO system. The simulator supports both individual and team modes. In team mode, the roles can include transmission operator, balancing authority area operator, reliability coordinator, generator operator, distribution operator and substation operator. The software does not provide any administrative checks to enforce the roles in demo phase. Each participant needs to know what controls are allowed for the role that he/she is playing. The

mathematical power system simulation consists of algebraic equations that describe the instantaneous relationship between variables and ordinary differential equations that describe the time varying properties of the variables. Since there are many non-linearities in these equations, they are solved numerically. The algebraic equations are typically solved every one to five seconds. This delay serves to induce the delay in data gathering through SCADA systems that receive data by scanning RTUs at specified intervals of time.

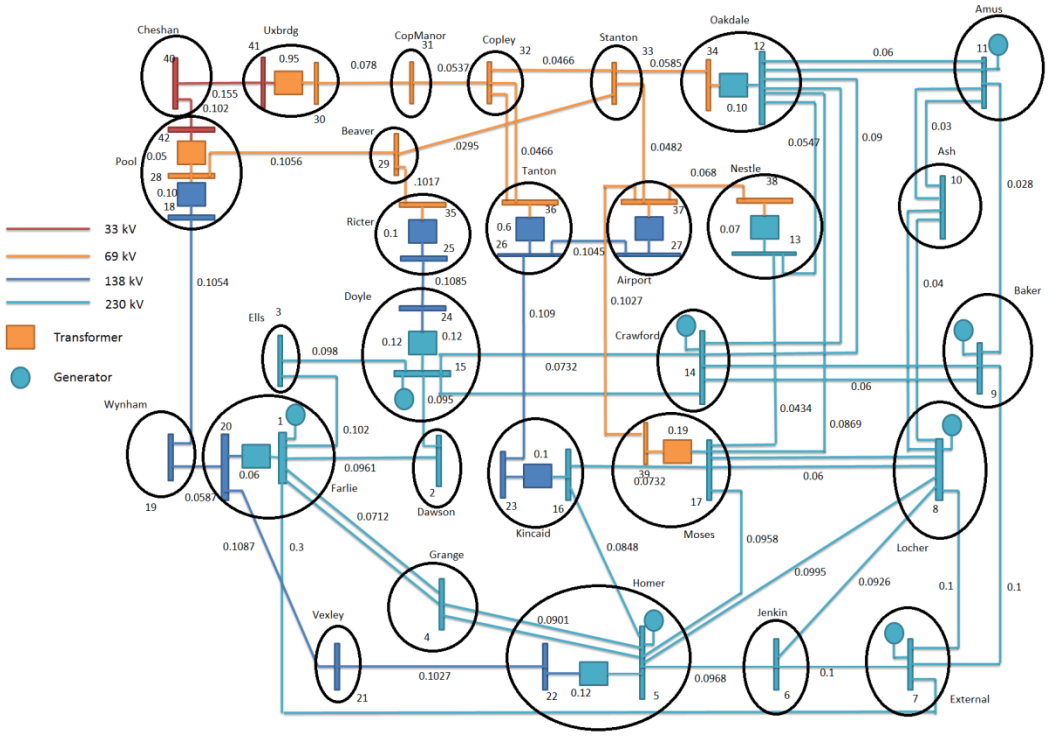

Figure 5.1: PALCO system topology

The event scenario featured in PowerSimulator includes 1) the instructor to create a certain power system situation, e.g., a series of line outages representing a situation which could be aresult of a storm. The recorded event scenario can be played in any simulation run to train operators for taking control actions related to that situation during light or heavy load periods; and 2) to observe the operator's reaction, i.e., sequence of corrective actions taken to bring the system back to stable operation.

5.2 Attack Modeling Using Incomplete Information

The power system vulnerability analysis using incomplete information available to the external attacker is detailed in [5.3]. A general overview of the metrics used to arrive at the contingency ranking for generators is given in this section. To determine the most critical generators for a cyber-attack, the concept of vertex centrality is used. Vertex centrality measures assign ranking coefficients to vertices in a graph, from which we can deduce that the most important generators are those located on buses with a high ranked centrality index. Among all vertex centrality indices, evidence of a close relationship between closeness centrality and impact of generator outages has been shown in [5.3]. The closeness centrality (include variable name) for an 'n bus' system is defined as:

$$C_c(v_i) = \frac{\sum_{i \in V/i} d(i, j)}{n-1} \tag{5.1}$$

The above equation relies on the use of shortest path distance d(i, j) between the vertices which is computed using the Dijkstra [5.4] shortest path algorithm. The closeness centrality index is extended for an 'N – X' case is given by the closeness impact centrality index as [5.5]:

$$CI_c(V_{cont}) = \sum_{i \in V_{cont}} |C_c(v_i)| \tag{5.2}$$

Where, Vcont is the set of generators considered for the N - X case.

5.2.1 Cyber-Physical Contingency Ranking

The calculation of the cyber security metric and the integration of this metric with the physical contingency ranking are discussed in [5.6]. The contingency ranking for the PALCO system based on these metrics for N-1 and N-2 generator contingencies is presented in table 5.1 and 5.2 respectively. The ranking is based on the following equation:

$$CP_{ranking} = CI_c * Sec_i \quad (5.3)$$

where, Sec_i is the security metric value.

Table 5.1: N-1 cyber-physical contingency ranking

Rank	N - 1 Contingencies		
	GEN	BUS	Ci
1	G8	15	1
2	G4	8	0.5
3	G2	5	0.16667
4	G7	14	0.125
5	G5	9	0.1
6	G3	7	0.0555
7	G6	11	0.0476

Table 5.2: N-2 cyber-physical contingency canking

Rank	N - 2 Contingencies		
	GEN	BUS	Ci
1	G8, G4	15,8	1
2	G8, G2	15,5	0.5
3	G8, G7	15,14	0.16667
4	G8, G5	15,9	0.125
5	G8, G3	15,7	0.1
6	G8, G6	15,11	0.0555
7	G4, G2	8,5	0.0476

5.3 Evaluation of Scenarios

In this section, we evaluate the advantage of integrating cyber and physical simulators in corrective control action selection.

5.3.1 Control Actions without Cyber-Power Simulator

We look at how an operator responds to a contingency without a cyber-simulator associated with the operator training module.

1. N - 1 Contingency case: From the contingency ranking given in Table 5.1, G8 outage at bus 15 is chosen to be simulated in the PowerSimulator. For this contingency, it was seen that the system voltage, line loadings and frequency are within acceptable limits. Figure 5.2 shows the frequency curve after the contingency.

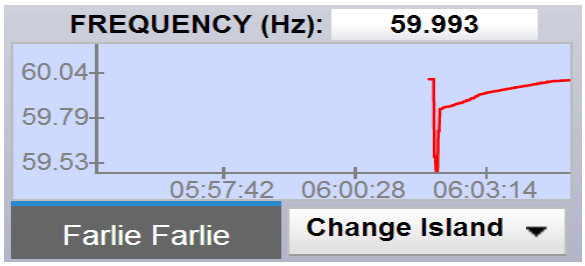

Figure 5.2: Frequency response of system for N-1 contingency case

According to North American Electric Reliability Corporation (NERC) document [5.7], frequency should be restored to at least 58.5 Hertz in ten seconds or less and to at least 59.5 Hertz in thirty seconds or less. It was observed that the frequency dipped to a minimum of 59.47 Hz and recovered quick enough to satisfy this criterion.

2. N - 2 Contingency case: From the contingency ranking given in Table 5.2, G8 and G4 at bus number 15 and 8 are chosen for this scenario. The generation at G8 at the time of tripping is 400 MW, and at G4 it is 645 MW. The control actions necessary to prevent under frequency and bring it back into acceptable limits within reasonable time frame is given in Table 5.3. Figure 5.3 shows the frequency response of the system for the N - 2 contingency case with control actions.

Table 5.3: Control actions for N-2 contingency case

	Control Action
1	Shed load Locher A, 271 MW
2	Shed load Amus A and Amus B, 100 MW each
3	Shed load Grange A, 172 MW
4	Shed load Ash A and Ash B, 80 MW each
5	Shed load Extrnl D, 154 MW
6	Shed load Jenkin, 21 MW

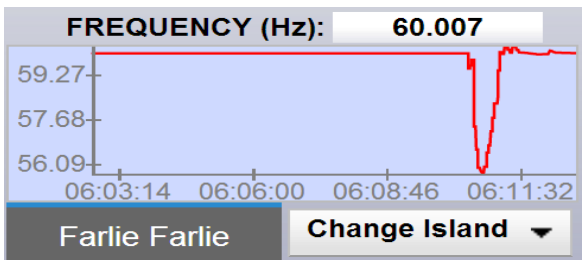

Figure 5.3: Frequency response of system for N-2 contingency case

The total load at the time the contingency occurs is 3160 MW. A total of 978 MW of load is to be shed in order to bring the frequency of the system within acceptable bounds while the other generators in the system start ramping up their generation to satisfy connected load.

5.3.2 Control Actions with Cyber-Power Simulator

The cyber-simulator helps in making the operator aware that the attack on the system has been caused by a cyber-attack and not probably due to a physical malfunction/disturbance/attack. It is assumed here that cyber simulator is also getting real time cyber information and able to identify cyber intrusion. The operator is presented with the option of recovering the cyber assets which have been compromised. In this way, the operator is able to retrieve the essential cyber assets first, and restore the physical power system assets to normal operation thereby reducing the effective downtime of a system outage. For the N-1 Contingency case, it has been seen before that there is no control action required from the operator for the N-1 contingency case as the system is able to deal with such a condition.

For the N-2 Contingency case, control action taken by the operator will be very different in presence of cyber simulator as operator is probably aware that the contingency has occurred due to a cyber-attack which needs to be taken care of as well. The load shedding operations would still be needed as stated in Table 5.3 to keep the system frequency within acceptable bounds. However, since the operator knows the cause of the attack, the time in bringing the generators back online is reduced greatly. G4 at bus 8 is the bigger of the two generators which were taken out. The operator would recover the cyber assets associated with this generator and bring it back up online first followed by G8. It is to be noted here that in the absence of the cyber simulator, the operator and repair crew will not be aware about cyber-assets being compromised. Even if operators restore the physical system, the attacker will take out generators easily again. In such a situation, the cost associated with the contingency cannot be calculated but will be very high. To compute the savings in cost when

the operator is aware of the cyber-attack, we will consider a simple scenario. It is to be noted here that the generator startup and ramping times are still the same, and the time saved in troubleshooting the root cause is the savings for the utility. When the operator notices the contingency, initial reaction is to shed the load to bring system frequency within acceptable bounds for N-2 contingency discussed above. Then the operator tries to bring the generators back into service, however this would not be possible since the cyber assets are compromised. The operator then has to call the maintenance division to take a look at what has happened at the problem location and troubleshoot for the cause. The money lost per hour of troubleshooting is about $67,726 assuming a charge of $0.06925 per kWh for the lost load of 978 MW in this specific case. Assuming the clearance time ranges between one to four hours, the total dollar amount lost by the utility for not serving the load could range from $67,726 to $270,906 neglecting generation costs.

5.4 Summary

In this chapter an enhanced cyber-physical security simulator for training operators is presented. The ranking methodology to model attacks on the power system using incomplete information available to the attacker is discussed in this chapter. It is seen that if the OTS is supplemented with a cyber-simulator, the operator is able to make a more informed choice when choosing control actions. The difference in operator response to contingencies with/without the cyber simulator has been discussed and the advantages of integrating the cyber simulator with OTS have been established.

5.5 References

[5.1] F. Pasqualetti, F. Dorfler, and F. Bullo, “Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design”, 50th IEEE conference on Decision and Control and European Control Conference (CDC-ECC), pp. 2195–2201, 2011.

[5.2] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks: characterizations and countermeasures”, IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 232–237, 2011.

[5.3] T. A. Ernster and A. K. Srivastava, “Power system vulnerability analysis-towards validation of centrality measures”, IEEE Transmission and Distribution Conference and Exposition (T&D), pp. 1–6, 2012.

[5.4] R. Bellman, “On a routing problem”, DTIC Doc., Tech. Rep., 1956.

[5.5] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information”, IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 235–244, 2013.

[5.6] C. Vellaithurai, A. Srivastava, S. Zonouz, "SeCPsim: A Training Simulator for Cyber-Power Infrastructure Security", Submitted to IEEE SmartGridComm conference, 21-24 Oct 2013.

[5.7] NPCC Document A-03, “Emergency Operation Criteria”, Northeast Power Coordinating Council (NPCC), 2004.

CHAPTER SIX

CONCLUSIONS AND FUTURE WORK

6.1 Introduction

The penetration of cyber assets into the Electric Power Grid (EPG) has increased significantly with the thrust towards a smarter grid. The impact of a coordinated cyber-power system attack on the EPG needs to be studied to develop appropriate counter measures. In order to analyze the applications used in the power grid from a cyber-power system view, it is important to be able to test these in real world conditions and test-beds are useful in doing so. This chapter summarizes the research presented in this thesis to develop a cyber-physical test bed for realistic emulation of attack scenarios and testing of applications. The potential improvements and updates that can be made to the cyber-physical test bed to make it function better are also suggested in this chapter.

6.2 Research Contributions

The following are the research contributions that have been made towards the enhancement of cyber-power system research:

1. Communication architecture for the PMU enabled smart grid has been discussed and presented. The offline simulation of the architecture using communication tools such as NS2 and NS3 has been also presented. It is seen from the results that the propagation delay is usually very small with the use of fiber optic lines. With the communication architecture assumed, it is seen that the data delivery to control center is not an issue.
2. The integration of cyber simulator and power system modeling tools has been proposed and implemented using RTDS and NS3. This provides a test bed for a real time cyber-power system analysis.

3. Testing of applications using the developed test bed to show the closed loop potential of the test bed in real time has been discussed. Testing of applications has demonstrated that in addition to the delays described in section 2.6, the major component of delay is the estimation of phasors at the Phasor Measurement Unit (PMU). Additionally, implementation of applications such as local area voltage stability monitoring algorithm demonstrate their real time operation. The execution of the application was found to be restricted by the frequency of data arrival only.
4. The integration of cyber simulator into an operator training simulator for the benefit of educating operators and enabling them to gain experience to deal with cyber-physical contingencies has been proposed.

6.3 Future Work

While the test bed capabilities are well documented in the thesis, the communication architecture that is used has necessitated some compromise on the realism in the test bed due to the limited hardware and software resources available in the laboratory. The RTDS system that can be modeled is limited by the number of processors available. Additionally, with one PMU card, only eight software PMUs can be simulated. Hence, scalability to larger systems is an issue with the developed test bed. Expanding the RTDS hardware to allow more capability on the power system simulation side would enable larger systems to be simulated. Additionally, developed concepts and architecture can be easily extended for bigger system analysis with availability of enhanced hardware and software capabilities. From the NS3 perspective, it is necessary to look into the option of enabling distributed simulation while in emulation mode. This is necessary to be able to run larger systems. At present, distributed and real time simulation are not supported together in NS3. Additionally, the implementation of the real time simulator may be reviewed to improve it for the needs of this particular test bed. Another interesting use case of the test bed to explore would be the possibility of integrating

security models to enable attack-defense mechanism studies for the cyber-power system. In this thesis, the conceptual integration of a cyber-simulator with OTS and the potential benefits are discussed. Moving forward, prototype models would need to be developed to find the optimal way to provide experience for trainee operators.

6.4 Summary

Communication architecture for the standard power system test cases has been discussed and offline simulation results using NS2 and NS3 have been presented. Based on the same communication network assumptions, a real time cyber-physical test bed using RTDS and NS3 has been developed. The modifications to be made to the test bed in order to be able to run specific applications have been discussed. It is to be noted that the test bed is not restricted only to the applications discussed in this work. It is suggested that the existing hardware and software resources be supplemented to realize bigger systems using the test bed.

APPENDIX A

IEEE 14 AND 30 BUS POWER SYSTEM TEST CASE IN RTDS

A.1 IEEE 14 bus test case data

Power Generation Data

Bus Number	Real Power (MW)	Reactive Power (MVAR)	Terminal Voltage
1	232.3959	-16.3758	1.06
2	40	43.4224	1.045
3	0	25.0838	1.01
6	0	12.7395	1.07
8	0	17.6268	1.09

Bus Voltage and Angle Data

Bus Number	Voltage (pu)	Angle
1	1.06	0
2	1.045	-4.99246
3	1.01	-12.73803
4	1.01765	-10.32575
5	1.01949	-8.78669
6	1.07001	-14.23401
7	1.0615	-13.37256
8	1.09001	-13.37256
9	1.05592	-14.95149
10	1.05097	-15.11028
11	1.0569	-14.80364
12	1.05518	-15.08865
13	1.05037	-15.16933
14	1.03552	-16.04667