A SIMULATIVE ANALYSIS OF THE ROBUSTNESS OF SMART GRID NETWORKS AND A SUMMARY OF THE SECURITY ASPECTS

by

SARAH MARIE KUBLER

B.S., Kansas State University, 2009

A THESIS

submitted in partial fulfillment of the requirements for the degree

MASTER OF SCIENCE

Department of Electrical and Computer Engineering
College of Engineering

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2011

Approved by:

Major Professor
Caterina Scoglio

Copyright

Abstract

The need for reliable and quick communication in the power grid is growing and becoming more critical. With the Smart Grid initiative, an increasing number of intelligent devices, such as smart meters and new sensors, are being added to the grid. The traffic demand on the communications network increases as these new devices are being added. This can cause issues such as longer delay, dropped packets, and equipment failure. The power grid relies on this data to function properly. The power grid will lose reliability and will not be able to provide customers with power unless it has correct and timely data. The current communications network architecture needs to be evaluated and improved.

In this thesis, a simulator program is developed to study the communications network. The simulation model is written in C++ and models the components of the communications network. The simulation results provide insight on how to design the communications network in order for the system to be robust from failures. We are using the simulator to study different topologies of the communications network. The communications network often has a simular topology to the power grid. This is because of right-a-ways and ownership of equipment. Modifying the topology of the communications network slightly can improve the performance of the network.

Security of the communications network is a very important aspect. There is a risk of successful attacks on the communications network without the implementation of security protocols. Attacks can come from malicious users of the communications network or from entities outside the network. These attacks may lead to damaged equipment, loss of power to consumers, network overload, loss of data, and loss of privacy. This thesis presents a short overview of the major issues related to the security of the communications network.

The department of Electrical and Computer Engineering (ECE) at Kansas State University (K-State) is working on developing a Smart Grid lab. Burns and McDonnell has collaborated with the ECE department at K-State to develop the Smart Grid Lab. This lab will be located inside of the ECE department. The lab will consist of both power grid equipment and network communication equipment. This thesis describes similar labs. It then describes the initial plan for the lab, which is currently in the planning stage.

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like to thank my major professor, Dr. Caterina Scoglio, for all the help and support. I would also like to thank Dr. Noel Schulz and Ms. Sakshi Pawha for all the advice and guidance they have provided. I would also like to thank Dr. Don Gruenbacher and Dr. David Soldan for their support and suggestions.

I would especially like to thank the Electrical Power Affiliates Program (EPAP) for financially supporting this project. EPAP includes Burns and McDonnell, Westar Energy, Nebraska Public Power District and Omaha Public Power District.

Special credit goes to my husband, Weston Burress, for being there for me now and always.

Chapter 1 - Motivation and Background

The need for reliable and quick communication in the power grid is growing and becoming more critical. With the Smart Grid initiative, an increasing number of intelligent devices, such as smart meters and new sensors, are being added to the grid. As these new devices are being added the traffic demand on the communications network increases. This can cause issues like longer delay, dropped packets, and equipment failure. The current communications network architecture needs to be evaluated and improved.

This thesis presents a simulator program that can be used to evaluate the performance of the communication networks of the power grid. This thesis then evaluates the delay distribution in different possible topologies under multiple fault scenarios. We have two main contributions in this paper. The first contribution is the development of the network simulator. This simulator is designed specifically for the evaluation of power grid communications networks. The simulator models the different aspect of the communications network. The simulator is designed to be able to be used in the future for simulations that are more complex and be linked to a power grid simulator. The second main contribution is the results from the simulations. The results show that a small change in the topology of the communications network has an impact on the performance of the network. The results also showed that the communications network topology that exactly matched the power grid network topology is not the best in terms of network performance. The communication network of the power grid often has many topological similarities to the power grid. Changing the communication network topology slightly can improve the reliability and robustness of the network.

1.1 Motivation

In Kansas like many other states, demand for energy is increasing. In addition the implementation of renewable sources such as wind and solar energy is increasing to reduce the dependence from foreign oil and reduce carbon dioxide emissions. This added demand generation and high reliability expectations are creating additional data and the need for efficient and effective communications for electric utilities. Added to this utilities are facing a push for

the Smart Grid initiative. All of this new information being generated needs to be reliably and securely transmitted back to the control centers of the utility companies. Utility companies, including ones in Kansas, are expressing interest towards improving their communications networks.

1.2 Need for Security

Security of the communications network is a very important aspect. Without the implementation of security protocols, there is a risk of successful attacks on the communications network. Attacks can come from malicious users of the communications network or from entities outside the network. These attacks may lead to damage to equipment, loss of power to consumers, network overload and loss of data, and loss of privacy. With the new North America Electric Reliability Corporation (NERC) Critical Infrastructure Program (CIP) standard, many of the utilities need to improve the security of their networks. If the security of their communications networks does not meet this standard, these utilities could face financial consequences from the results that attacks could have on their networks.

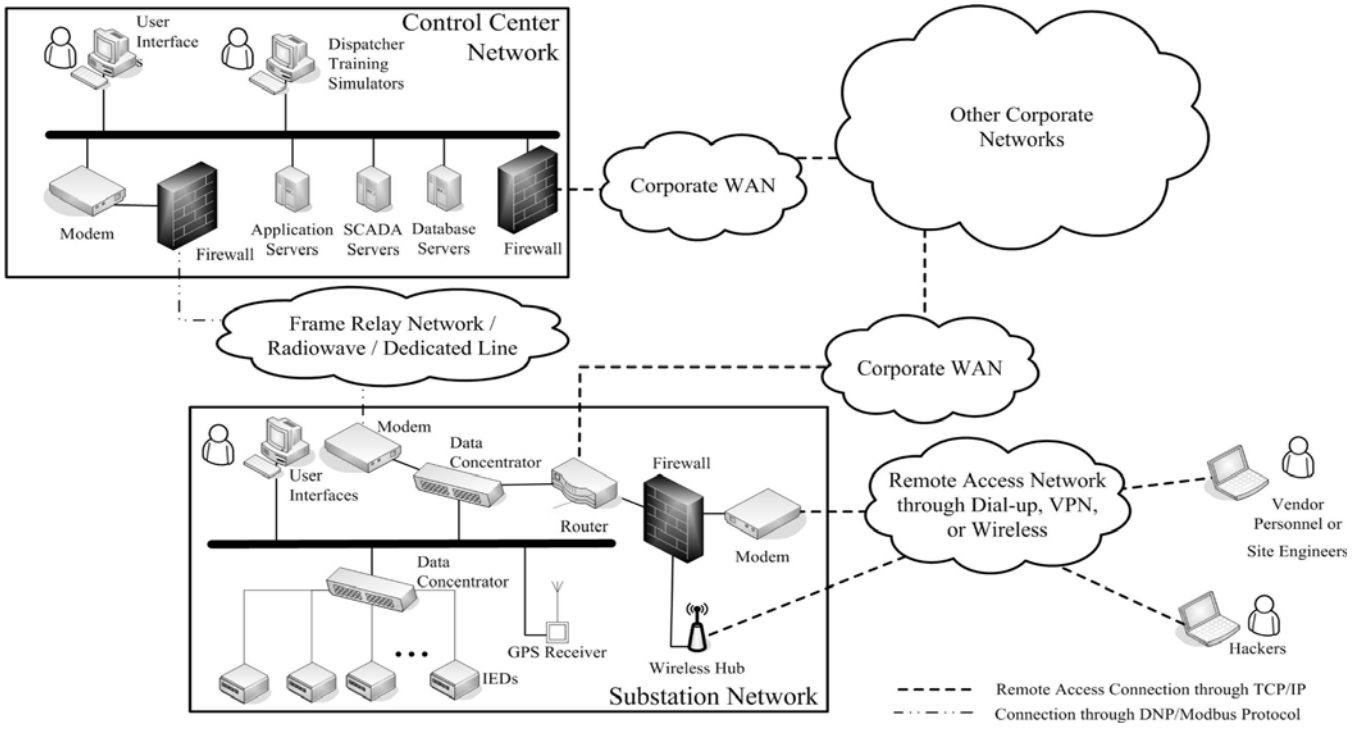
1.3 SCADA Overview

Supervisory Control And Data Acquisition (SCADA) systems are used to control and collect data from the power grid. The protocols developed for SCADA systems are not very secure. Researchers are modeling the SCADA systems and the power systems to study the security and reliability. Researchers are developing new SCADA systems and protocols to increase the security and reliability of the grid.

The reliability of the communication of SCADA systems is very important. SCADA systems are able to react automatically to certain events, like changes in voltage levels. SCADA systems are able to control the physical hardware of the systems [1]. Loss of data on a SCADA system could cause the control center to show incorrect information to the operator. Figure 1.1 is a diagram of a control center for a power system. The top left of Figure 1.1 represents the control center. This is where all of the servers are stored and is usually located inside the main power plants. The bottom left of Figure 1.1 represents a substation. At the substation, there are many sensors and data collection devices. The data from the substation needs to be

communicated back to the control center. The rest of the diagram shows communications network's connection points.

Figure 1.1 Power System Control System from [1]



From this diagram, it is apparent that the control systems are complex networks. The communications networks have many different access points. Malicious users can use these access points to gain control of a SCADA system. The network administrators need to implement security measures to decrease the effectiveness of the attacks.

In this thesis, we will be evaluating the network communication systems. . The security aspects are very important and a literature review is presented in Chapter 3. In Chapter 2, we present the related projects. These related projects mostly concentrate on the security aspects of the communications networks. Chapters 4 and 5 present our simulator and the results from the simulations. Our focus in these chapters will be on the topological aspects of the communications network

Chapter 2 - Related Work

This section explores the different SCADA models, which have been developed by researchers from around the world. Some of the models described are the VIKING project, the National SCADA test bed project, the CRUTIAL test bed, the TRUST-SCADA test bed, and the RINSE simulator. In addition, there has been a paper recently published in *Nature [2]* about interdependent networks.

2.1 Viking Project

The VIKING (Vital Infrastructure, networKs, INformation and control system manaGement) project is a SCADA test-bed project [3]. The European Community's Seventh Framework Program provides funding for it. VIKING's goals are to improve data integrity, reliability, and robustness of SCADA systems. The VIKING project has four main objectives [3].

The first objective is to identify vulnerabilities by providing a framework of a SCADA system. This framework should be able to predict security risks and predict any failures that may happen. The second objective is to model the effects on the power system if the SCADA system does not work correctly. The third objective is to model new features and solutions for the SCADA systems. The last objective is to educate the power industry about the vulnerabilities of SCADA networks and power systems.

The VIKING project has been active since February 2009. The authors have published work on the threats they have identified [3]. The VIKING group has not published their models yet. The project has funding through 2011 [4].

2.2 National SCADA Test Bed (NSTB)

NSTB is a U.S. program funded by the Department of Energy. NSTB is focusing on creating new control system technology that will have built in security, be scalable, and be cost effective. The new solutions should have little effect on the utility implementing the new control system.

Many projects are part of this nation-wide test bed. Partners in this project include national labs, universities, utility companies, and companies that design and manufacture

SCADA equipment. Each of the projects receive funding through the NSTB project. The NSTB project is funded from 2007- 2013 [5].

Due to its size, the NSTB has many resources. These resources include a Next-Generation Wireless Test Bed, a Power Grid Test Bed, a Cyber Security Test Bed, Control System Security Training Courses, Virtual Systems Environment, and specialized laboratories for Cryptography, Network Security, and Intelligent Infrastructure Research and Development. The resources are located at Sandia National Laboratory and Idaho National Laboratory [6].

2.3 CRUTIAL

CRUTIAL (CRitical UTility InfrastructurAL resilience) is a European project for the identification of critical points in control systems. CRUTIAL has a laboratory test bed, which focuses on the identity of critical aspects between the power system and the information systems. CRUTIAL is working on identifying the threats from cyber attacks on control systems.

The model uses Ethernet, TCP/IP, and UDP/IP protocols for the basic network behavior. The model is not using a commercial SCADA protocol for the data exchange but the data packet is based off a specific standard. The model is a very simplified version of the power system. Only the pieces that are important to the communication network are modeled with a high level of detail [7].

2.4 TRUST

TRUST (Team for Research in Ubiquitous Secure Technology) is a National Science Foundation (NSF) funded project [8]. The TRUST-SCADA experimental test bed was created to assess SCADA in realistic settings, provide solutions to vulnerabilities, test new solutions, and to provide an open-source design for a test bed. The TRUST-SCADA test bed has the following requirements: modularity, reconfigurability, remote access, and accurate modeling.

TRUST has some early results from their work. The prototype TRUST-SCADA test bed is implemented and includes a Stateflow for plant and controller modeling and uses Omnet++ for network modeling. The experiments that have been implemented are a model for a chemical plant, a robust controller, and Distributed Denial of Service (DDOS) network attacks. The future goals of this project are to develop additional experiments, develop more security attack models, and package the test bed to be used by other researchers on projects [9].

2.5 RINSE

Real-time Immersive Network Simulation Environment (RINSE) is a project at the University of Illinois Urbana-Champaign. RINSE is a large-scale network simulator. RINSE is being used with PowerWorld server to simulate the network traffic in a power system. PowerWorld is a program that can simulate the power grid and provide SCADA data. The SCADA data is used in the RINSE simulator to test the network. The RINSE simulator is able to allow users to change the simulation parameters in the middle of the simulations. This allows RINSE to be very useful in large simulations. RINSE is being used to evaluate attack scenarios on the communication network [2].

2.6 Interdependent Networks

Research about interdependent network failures was published in [10]. This paper uses mathematical models to describe how interdependent networks rely on each other. The paper describes general networks but uses the power grid and communication network as an example. In the paper, they find interdependent networks are worse than the individual network in terms of robustness and reliability [10]. This research does not include any type of simulation or real-time network study. The paper is purely based on the mathematical models. This thesis presents work that is a first step toward testing the impact of the interconnection between the power grid and the communications network using a more accurate simulative approach.

Chapter 3 - Protocols and Security Aspects

In this chapter, we present an overview of the security aspects of the communications network. The security of the communications network is very important. The common communications protocols are described and compared. In this work, we provide an overview of the security but in future work the security aspect can be incorporated into the simulations.

The reliability of the communication of SCADA systems is very important. SCADA is a control system and data repository system for systems like the power grid, water utility plants, and other large industrial systems. SCADA systems are able to react automatically to certain events, like changes in voltage level. SCADA systems are able to control the physical hardware of the systems [1]. SCADA systems are vital to how the power grid works.

These systems need to be resistant to accidental failures and intentional attacks. The layout for the rest of the chapter is as follows: first, the chapter discusses NERC CIP requirements. Then, the chapter discusses the security of the more popular older SCADA protocols. Next, the chapter describes newer protocols. Last, the chapter discusses the connection of the protocols to the Smart Grid initiative.

3.1 NERC CIP

North America Electric Reliability Corporation (NERC) Critical Infrastructure Program (CIP) approved the Cyber Security Standards on January 17, 2008. These standards are mandatory and enforced by federal law. Utilities that fail to implement these standards will have to face penalties and pay fines. This was the first standard that required utilities to implement physical and cyber security of their computer systems [11].

In 2006, there were many security vulnerabilities lists for the communications networks. One of the issues on the lists was the connection between the SCADA system and the general IT system of the utility. Some utilities did not separate the two parts very well. This can cause problems with the SCADA system if a user on the IT system accidently downloads a malicious file while doing normal internet browsing. Another main issue was the system administrators did not patch or upgrade the devices and software on the network at regular intervals. This means that vulnerabilities that others had discovered, fixed, and published were still an issue on

the system. This could allow attackers to gain access to the system. These two issues are very serious.

Another main security issue was the actual physical security of the communications networking and sensor devices. These devices were not even physically secure in some utilities. Many people had access to the devices, sometimes including even the public. NERC CIP's Cyber Security Standards will help and require utilities be able to identify and fix many security problems [11].

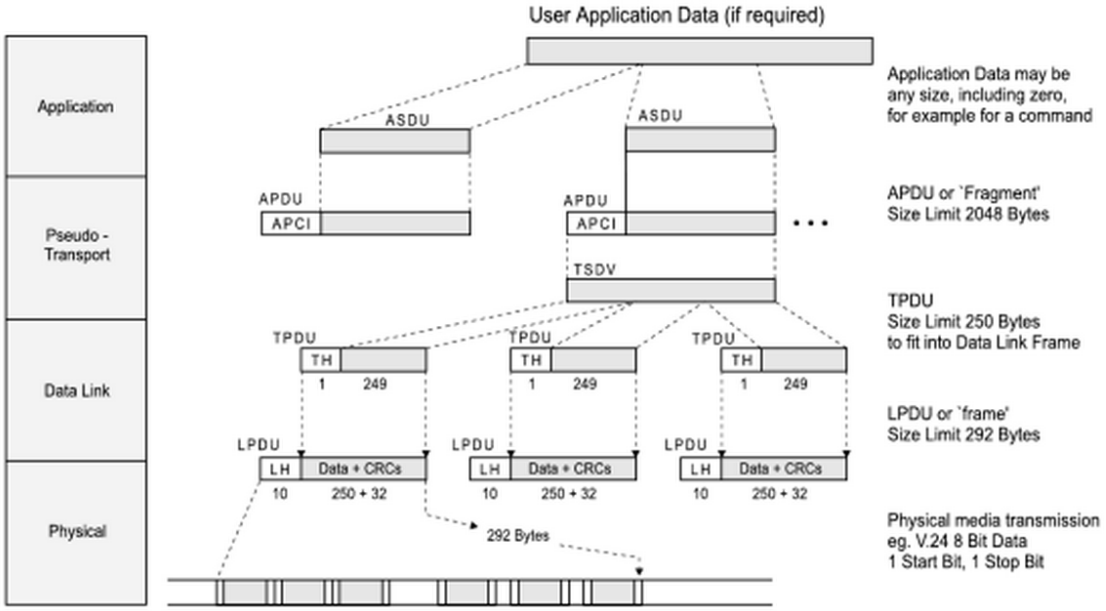
3.2 SCADA Communication Standards

Different types of SCADA systems use different communication protocols. Some of the protocols are proprietary and some are non-proprietary. Proprietary means the company owns the protocols and they do not release the details about the protocol outside of the company. Examples of proprietary protocols are GE Fanuc, Siemens Sinaut, Omron, Modbus RTU/ASCII, and Allen Bradley [12]. People outside of the company know little about these protocols because they are proprietary. Many protocols exist that are not proprietary and industry is moving towards these more open protocols. These include MODBUS X, Distributed Network Protocol (DNP), and IEC 60870 [12]. DNP3 and IEC 60870 are two very popular older protocols. IEC 61850 and IEC 62351 are newer protocols. In this section, I discuss the security aspects of each of these protocols.

3.2.1 Distributed Network Protocol 3

DNP3 is a commonly used protocol in the United States for SCADA power systems. DNP3 is a layered protocol. Figure 3.1, below, shows the layers of DNP3. DNP3 uses a simplified stack compared to the 7-layer OSI model. The application layer holds the data or control messages that need to be sent. The Pseudo-transport layer is included to handle large messages. This layer incorporates both the Transport layer and the Network layer from the OSI model. The Data link layer defines provides reliability of the information across the physical layer. The Physical layer defines how the protocol works on different physical mediums [17]. Figure 3.1 shows how the information is encapsulated in each layer.

Figure 3.1 DNP3 Layers from [17]



However, DNP3 does not provide good security features. DNP3 does implement Transport Layer Security (TLS) when used along with TCP/IP [13]. TLS can provide confidentiality, integrity, and authentication of one or both participants in the communication [14]. The problem is the transport layer may not be the same across every hop, rendering TLS unsafe. Alone, DNP3 has risks of different types of attacks against it. These attacks could be address-spoofing, modification of data, and replay of old messages [15]. Researchers have made many modifications to DNP3 to fix these issues and other security issues related to DNP3.

One approach of securing DNP3 is to apply Pretty Good Privacy (PGP). PGP can provide authentication, confidentiality, and non-repudiation to DNP3. Researchers added PGP to DNP3 in a way that does not require changes to the DNP3 specification. This allows devices not using the PGP security to be able to work on the network. PGP uses public keys to form a session key for use in communication. This allows encryption of the data to provide confidentiality. The sender creates a message digest from the data-link layer frame to provide integrity to the message. The main issues with PGP are that it is not extremely secure and that the use of cryptography adds a delay to each message [13].

Another approach is to use DNPSec. One main difference from the PGP approach is that DNPSec changes how DNP3 works so it is not as easy to implement. DNPSec provides

assurance that the recipient received it and an attacker cannot replay the message. DNPSec also provides integrity of the network headers and confidentiality assurances. A message authentication code, either using MD5 or SHA, is included in the packet to provide integrity. DNPSec uses shared session keys for the encryption. The system creates session keys during the initial configuration of the system. This only works due to the very static nature of SCADA systems. The system creates new session keys when needed. DNPSec does not suffer from performance degradation as much as the PGP approach. Therefore, DNPSec has a minimal effect on the overall delivery time of packets [16].

3.2.2 IEC 60870

IEC 60870 is a commonly used protocol in Europe for power grid systems. IEC 60870 can work over Ethernet and serial. The designers of the protocol did not design the protocol with any security features expressly stated. The specific part of this protocol that deals with SCADA systems is IEC 60870-5-101, also called T101, and IEC 60870-5-104, called T104. The T104 section deals with TCP/IP and the T101 section defines the serial communication [17]. See Section 3.2.4 on IEC 62351 for information on how researchers have added security to this protocol.

IEC 60870 is also a layered protocol. It uses a similar stack as DNP3 but does not included the Pseudo-transport layer. Figure 3.2 shows the layers used with version T101 over serial communication. T101 defines all of the layers in this case.

Figure 3.2 IEC 60870 T101 Layers from [17]

Layer	Source	Selections
User Process	IEC 60870-5-5	Application functions
Application	IEC 60870-5-4	Application information elements
	IEC 60870-5-3	ASDUs
Link	IEC 60870-5-2	Transmission procedures
	IEC 60870-5-1	Frame formats
Physical	ITU-T	Interface specification

Figure 3.3 shows the layers used with version T104. T104 uses the standard TCP/IP protocol suite for every layer below the application layer.

Figure 3.3 IEC 60870 T104 Layers adapted from [17]

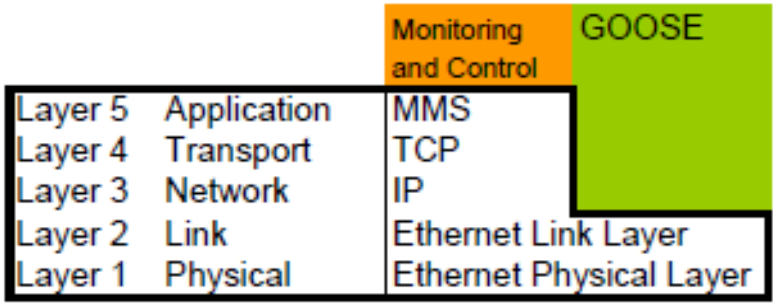
Layer	Source	Selections
User Process	IEC 60870-5-101	Application functions
Application	IEC 60870-5-101	ASDUs and Application Information Elements.
Transport	TCP / IP Transport and network protocol suite	
Network		
Link	Ethernet	
Physical		

3.2.3 IEC 61850

IEC 61850 is another layered protocol [18]. IEC 61850 has not been highly adopted in the US power grid system yet. This protocol will help utilities become compliant with the NERC CIP Cyber Security Standards. This protocol is becoming more widely used and seems to be becoming the protocol that will be used the most. IEC 61850 uses standardized names for components in the network. It uses XML-based Substation Configuration Language (SCL) to choose the names [18]. IEC 61850 does not specify any security. The creators of the protocol assumed that the protocol would be running on a safe network that is isolated from any outside influence and that all devices on the network are trusted [19]. However, this is not a realistic requirement. IEC 62351, in the next section, shows how it can secure IEC 61850.

Different message types in IEC 61850 have different protocol stacks. The monitoring and control messages are sent over MMS (Manufacturing Message Specification) [19]. These messages are in orange in Figure 3.4. GOOSE redefines Layers 3-5 and relies on the Ethernet Link Layer. GOOSE is in green in Figure 3.4. GOOSE is definition of peer-to-peer messages used for device automation [19].

Figure 3.4 IEC 61850 Layers



3.2.4 IEC 62351

IEC 62351 is a protocol that adds security aspects to IEC 61850, IEC 60870, and other protocols. IEC 62351 adds security in both the Transport Layer and the Application layer through MMS and TCP. This protocol is still under development and is not yet standardized. There are eight different parts to this protocol. The first two parts are descriptions of the general need for the protocol and definitions of terms. Sections 3, 4, and 5 are the more technical parts that relate to this research.

Part 3 concentrates on the mapping of IEC 61850 and IEC 60870 to TCP/IP. Part 4 maps these protocols to MMS. Devices use MMS to send SCADA data in a network. Both of these sections require the use of TLS (Transport Layer Security). The handling of certificates is performed using Certificate Revocation Lists (CRL). This is because Online Certificate Status Protocol (OCSP) has too much overhead and the networks have limited bandwidth [20].

Part 5 concentrates on serial communication with IEC 60870. This section defines how asymmetric cryptographic functions are used and how the keys are managed [20].

One form of MMS provides authentication at the application layer. The receiving party can authenticate each message received, but the receiving party cannot guarantee the integrity of the message. The other form of MMS provides integrity. MMS uses TLS over TCP. This provides the messages with authentication, confidentiality, and integrity at the transport layer. To make MMS more secure, the designer can combine these two forms to provide security features on both the application and the transport layer. The problem with this approach is that in the power grid communication systems TCP may not always be used depending on the underlying network structure, causing TLS not to be able to be implemented in the parts without

TCP. This would remove the security reassurances provided by TLS and make MMS only as secure as its first form. Three different approaches exist to solve this problem [20].

The first approach is to use HTTP Digest Authentication. This approach provides integrity end-to-end across the application layer. The two communicating parties will need to have an established shared secret. The two parties will use this shared secret to produce a MD5 checksum of each message or part of each message. Validating the checksum against the message will provide the integrity needed [20].

The second approach is to use H.235 security. This approach uses asymmetric cryptography to produce a shared secret between the two communicating parties. Then the two parties use the shared secret to produce a cryptographic hash of each message to ensure integrity. This approach is very similar to the first approach except it specifies how the two parties obtain the shared secret [20].

The third approach is to use XML security. This approach is specifically for web services. Utilities can use this for communication that has to take place over a large distance. An example of this is wind farm communication to the control center [20]. There are two different versions of XML security. The first is XML Signature that provides integrity. The second is XML Encryption that provides confidentiality. Both of these versions require keys and a key management system. XKMS was developed, which is a web service to handle the key distribution [21]. Both of these versions can be used together to provide the security. This security includes privacy, integrity, and non-repudiation [20].

Of these three, [20] suggests the second approach is the best one. This is because H.235 defines how to establish the shared secret and it is not based on web services. IEC 62351 allows devices in the power grid communication system to communicate securely.

3.2.5 Need for Improvement

SCADA systems need protocols designed from the beginning with security measures. The non-proprietary protocols are available in books and on the web for study. This poses a higher-level threat because now anyone can know the format of the messages sent and exactly how the devices send the messages. New protocols need to be developed and tested. These protocols need to rely on valid cryptography-based security not just security based on obscurity [22].

3.3 Connection to the Smart Grid

This section explains how improving the security and reliability of the power communication systems will help the Smart Grid effort. In addition, this section describes the groups that need to support the effort of improving of the communications systems.

3.3.1 Improvements

Smart Grid is the concept of adding advanced technology to the power grid. This includes adding better control methods, renewable energy sources, advanced sensors, and smart appliances to the grid. As consumers add the new smart applications, the utilities will have more control over the system. This can pose security issues if attackers compromise the control system. Improving the security of the systems will help ensure this does not happen.

The addition of distributed renewable energy sources requires a more advanced control of the power system. Improving the reliability and speed of the systems can help make this a reality. To make the grid a smarter grid, the utilities need to improve the communication system [23].

3.3.2 Supporting Groups

Many different groups of people need to support the improvement of communication systems. One major group is researchers. Researchers need to work on developing ways to improve the systems. Universities and national labs should be a big part of this research. The governments should support this initiative and help fund projects. In addition, companies that produce SCADA equipment and other networking equipment need to support increasing the reliability and security of SCADA systems.

Utilities are the most important group that needs to support improving of the systems. The utilities need to be willing to both support and implement projects that help increase the security and robustness of their communication systems.

3.4 Summary

This chapter has presented an overview of protocol used in the communications network of the power grid and the security of the communication systems of the power grid. The reliability of the communication in the network is very important. The communication systems are vital to how the power grid works. The protocols that researchers have developed for

SCADA systems have not been highly focused on security. The system needs to be resilient to accidental failures and intentional attack. Utilities are using IEC 61850 and IEC 62351 more as the Smart Grid is growing. These two protocols have the appropriate security standards for now, but in the future researchers need to develop protocols with security in mind from the beginning.

Chapter 4 - Simulator

To date, the efforts listed in Chapter 2, have not included simulations to investigate the effects of topology on the communications network metrics. To get quantifiable results, our research has created a simulator program to demonstrate the impact of topology on delay and lost packets. We will be studying the communications network that is represented in Figure 1.1. The program simulates layer 3 routing in the communications network. The buffers in the simulation program are modeled as layer 2.

The simulation model is written in C++ and models the components of the communications network. The simulation results provide insight on how to design the communications network in order for the system to be robust from failures. We are using the simulation model to evaluate the interdependency between the communications network and the power grid. The simulation results provide insight on how to design the network in order for the system to be robust from failures. The simulator is simplified from the large, general commercial simulators. This allows the simulator to be focused on this particular application. With this simplification, we are able to provide ease of use and correctness in our simulations.

The simulator will model different devices that are found in the typical communications network for the power grid. The sensors and data collection devices are modeled as nodes in the network. The nodes generate periodic traffic that represents the devices taking measurements at set time intervals. The routers in the communication network are modeled in the simulation program. The routers in the simulation program have basic functionality and can record statistics, which included buffer utilization, queuing delay, lost packets, and packet count.

4.1 Program Structure

The program is object-oriented with classes representing different parts of a communciations network. Figure 4.1, below, shows the UML diagram of the program structure.

Figure 4.1 UML Class Diagram

Each box in the diagram represents a class in the program. The classes have the following information displayed: Name, Attributes, and Functions. The lines between the boxes represent how the classes are related.

The Message class represents packets of information in the network. The Message objects hold the information that is being sent through the network. These objects also include the label-switched path details; see the intelligent rerouting section 4.3.1. There are many Message objects in each simulation. Message objects are created in each Node object or Router object.

The Node class represents sensors in the network. This class generates data and sends data out in the form of Message objects. The Node objects can have one interface that can be connected to a Router object. There are many Node objects in the simulations, each individually configurable. The Node objects can collect data and statistics about the network performance.

The DatabaseNode class is a specialized Node Class. This class inherits all of the Node class's attributes and functions. In addition to the Node Class functionality, the DatabaseNode is able to reply to received Message objects. This simulates control messages in the network. There is only one to a few DatabaseNode objects in a simulation.

The Router class represents the network routers in the system. The Router objects forward Message objects toward the DatabaseNode objects. Router objects are able to detect missing links and generate rerouting Message objects to send to Node objects. Router objects keep track of statistics, for example; buffer fullness and discarded Message objects.

The Interface class represents the network interface on routers and sensors. This class holds information about the links in the network. Each Interface object has a Buffer object. The Buffer objects are able to hold Message objects.

4.2 Initialization

This section describes how the network simulation program is used. First, input the network structure into the K-shortest Path algorithm from [24] to obtain the paths from each node to the control center. The K-shortest Path algorithm uses an un-weighted approach to generated the shortest paths based on the number of hops in between two nodes. This creates a file to be used by the simulation program. We call this the ShortestPath file. The ShortestPath file contains a list of routes that is used for sending data in the network. The network simulator

then chooses which paths to use initially to send the packets through. This is based off which is the shortest path, but it randomly decides between paths that have the same length.

Upon running the simulation program, it asks for multiple file names:

- Data Output file– the name of the file that the data will be stored in. (See example in Appendix A)
- Statistics Output file – the name of the file that the statistics will be stored in. (See example in Appendix B)
- Router file – the name of the file containing a list of the routers and their buffer size and clock speed. (See example in Appendix C)
- Node file – the name of the file containing a list of the nodes/sensors in the network, this file includes the node name, the connected router, the type of node, the frequency of data generated, the data size and the controlling database. (See example in Appendix D)
- ShortestPath file – a file containing a list of usable routes. (See example in Appendix E)

The simulation program uses the files to create and setup the communications network structure. Once this is initialized, the simulation program starts running. The program will end, displaying an error message, if the communications network setup will not allow any of the nodes to send any data.

4.3 Network Operation

This section describes how researchers can use the simulator program to simulate a real-world communications network. The program sends message objects through a series of node and router objects to simulate network traffic. The parameters can be changed to allow the message to be sent more frequently and to be different sizes. These parameters can be changed to represent a wide variety of network specifications. In the simulator, we assume the network traffic is deterministic, each node sending data periodically at constant rate to the control center. This represents messages from different types of sensors that could be connected to the communications network. The network represented by the simulator can be quite large and have many more specifications set than the ones used in this research work. The size of the network

that the simulation program can handle is limited by processing power, the larger the network the slower the simulations. This can be mitigated by using higher-powered computers.

Links in the communications network can be broken to simulate real world failure. This allows the researcher using the program to be able to study the effects of the failure with different topologies or parameters. The simulation program can also perform two other optional features. The next two sections describe these optional features.

4.3.1 Intelligent Rerouting

The simulator has the ability to do intelligent rerouting if a link is broken. This rerouting is based on multi-protocol label switching (MPLS). MPLS was chosen because it is the standard used by some power companies to implement their communication network and it has flexibility in performing fast operations. MPLS is a protocol works with many different protocols including Internet Protocol (IP). MPLS adds labels to IP headers that define how the packet will be forwarded. MPLS can provided quality of service constraints and is scalable.

MPLS can also perform Traffic Engineering. MPLS is able to reroute traffic through links based not only on the shortest path algorithm. It knows when a link is congested and can then reroute all or some of the packets along routes. These new routes may not be the shortest paths, but may have less congestion on them. This can reduce buffer overflow thus reducing the number of packets dropped in the communications network [25].

In the simulation program, each message is assigned a path to follow. This equates to the label for the packet. The packet will follow this route. If there is a buffer overflow, a message will be sent to the source node of the packet. This message will suggest a change of the label to the node. This allows for congestion avoidance through the Traffic Engineering aspects of MPLS. If a link is completely lost, a message will be sent back to the source node forcing a change to the label.

In the Chapter 5, I describe how the communications network reacts when MPLS is enabled and disabled.

4.3.2 Multiple Databases

The communications network topology can include multiple databases. Nodes can be configured to send data to one or several databases. This can be beneficial for reliability of the

communications network. If the path to one database is broken, the node can still record its data in other databases.

4.4 Output

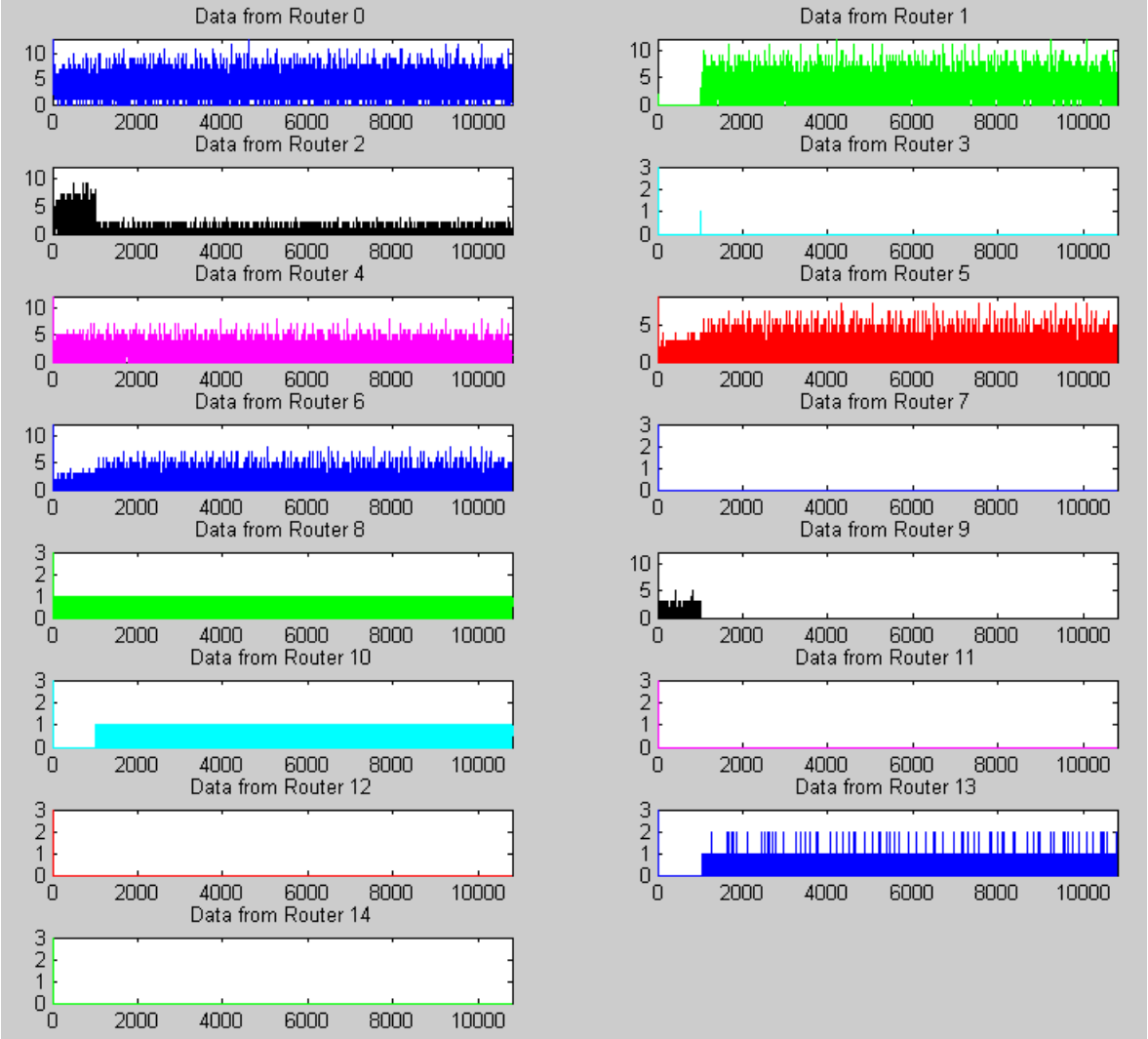
This section describes the output the program generates. Two different files are generated: a data file and a statistics file.

4.4.1 Data File

The data file consists of an array of values representing the number of packets in the most filled buffer in each router. See Appendix A for an example data file. This data file can be graphed with a MATLAB program to display the congestion in each router. See Appendix F for the MATLAB Script.

See Figure 4.2 for an example graph. In this simulation, a link was failed at t = 1000. In the graph for 'Data from Router 2' the data in the buffer decreases at t=1000 and redistributes to Routers 1, 5, 6, 10, 13. This is logical because the link failed was the link between Router 2 and the database. This caused the data to reroute intelligently through other routers to be still able to reach the database.

Figure 4.2 Buffer Usage in Simulation using Topology 1 (shown in Figure 5.1)



4.4.2 Statistics File

The statistics file holds more information than just buffer usage. It records statistics including:

- Links removed
- Total number of packets lost in each router
- Total number of packets received by each router
- Maximum buffer fullness in each router
- Average buffer utilization in each router

- Total number of packets received by databases
- Total number of packets each node receives
- Average packet delay
- Number of nodes disconnected from their respective databases

These statistics will be used to evaluate the performance, reliability, and robustness of the communications networks. See Appendix C for an example Statistics File.

The output files will allow us to evaluate the network performance. This evaluation will help us determine how each topology performs. With the output files, we are able to generate graphs that explain the network performance. The different features of the simulation program will help us be able to configure the simulation network to match the network we are using.

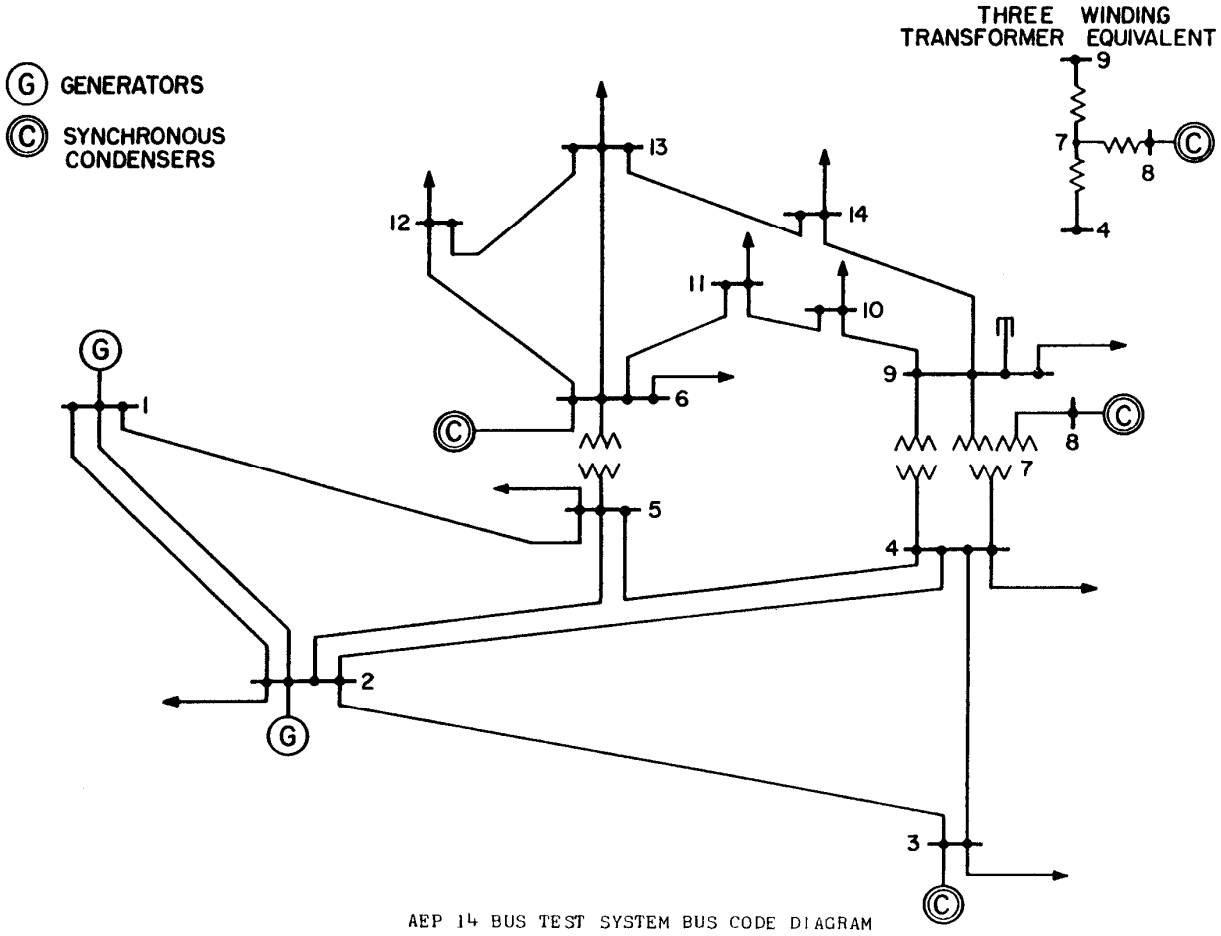
Chapter 5 - Simulations and Results

This chapter describes the research performed using the communications network simulation program from Chapter 4.

5.1 Topology

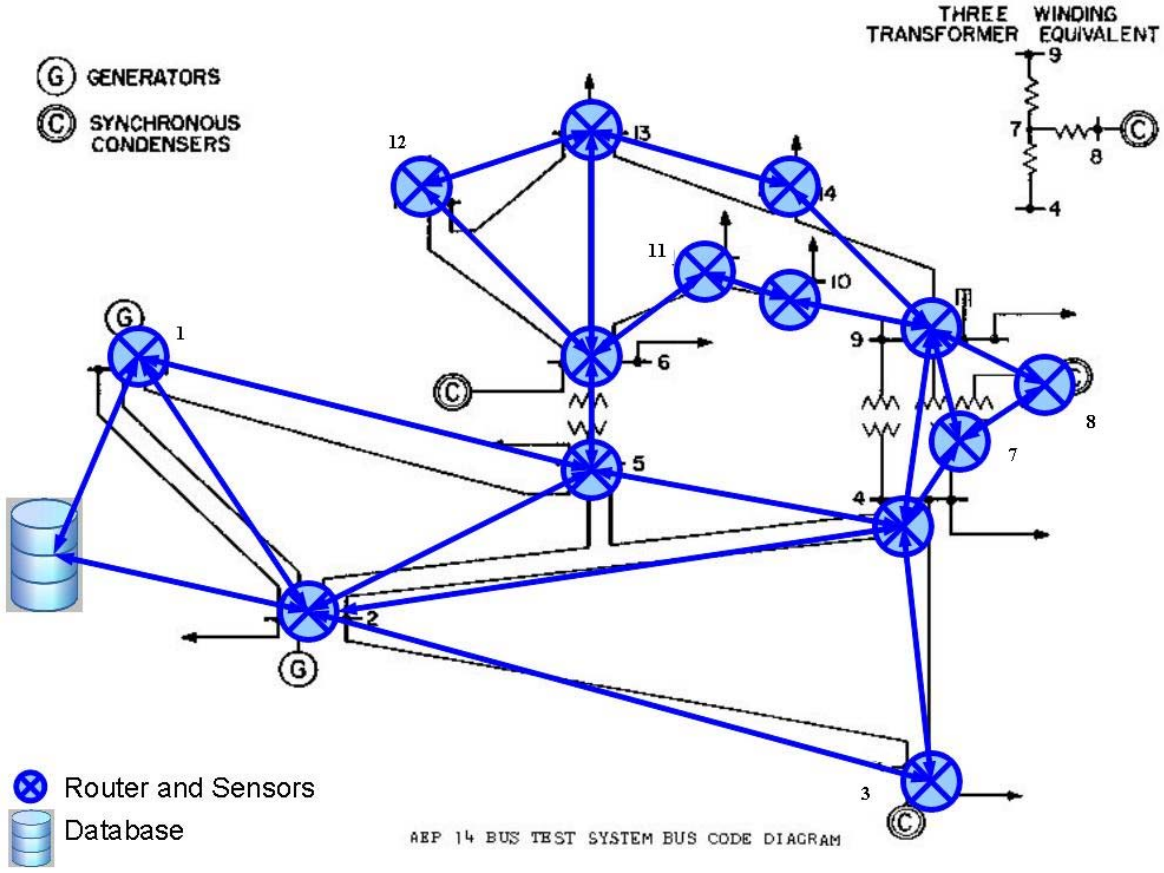
In this research, three topologies are used. The models for the simulation are based on the IEEE Test Case Model diagrams [26]. The 14-Node diagram, Figure 5.1, is below:

Figure 5.1 IEEE 14 Node Test Case Power Grid Diagram from [26]



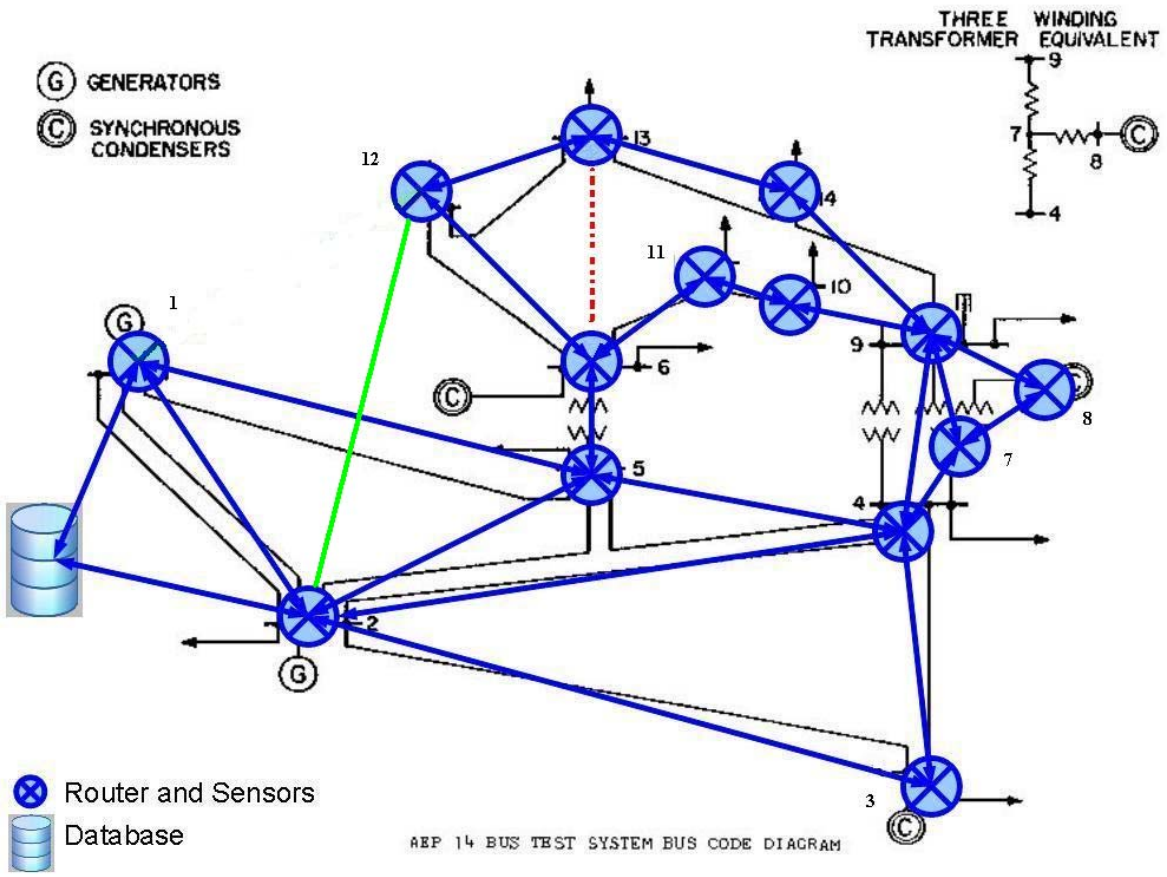
For the first topology, the nodes of the simulation model represent each node in the IEEE Power Flow Model. The links in the communications network follow the links in the power grid exactly. We assume the control center is located at the central generation station. See Figure 5.2, the diagram of the 14-node representation below.

Figure 5.2 Communications Network Topology 1 adapted to match power flow model[26]



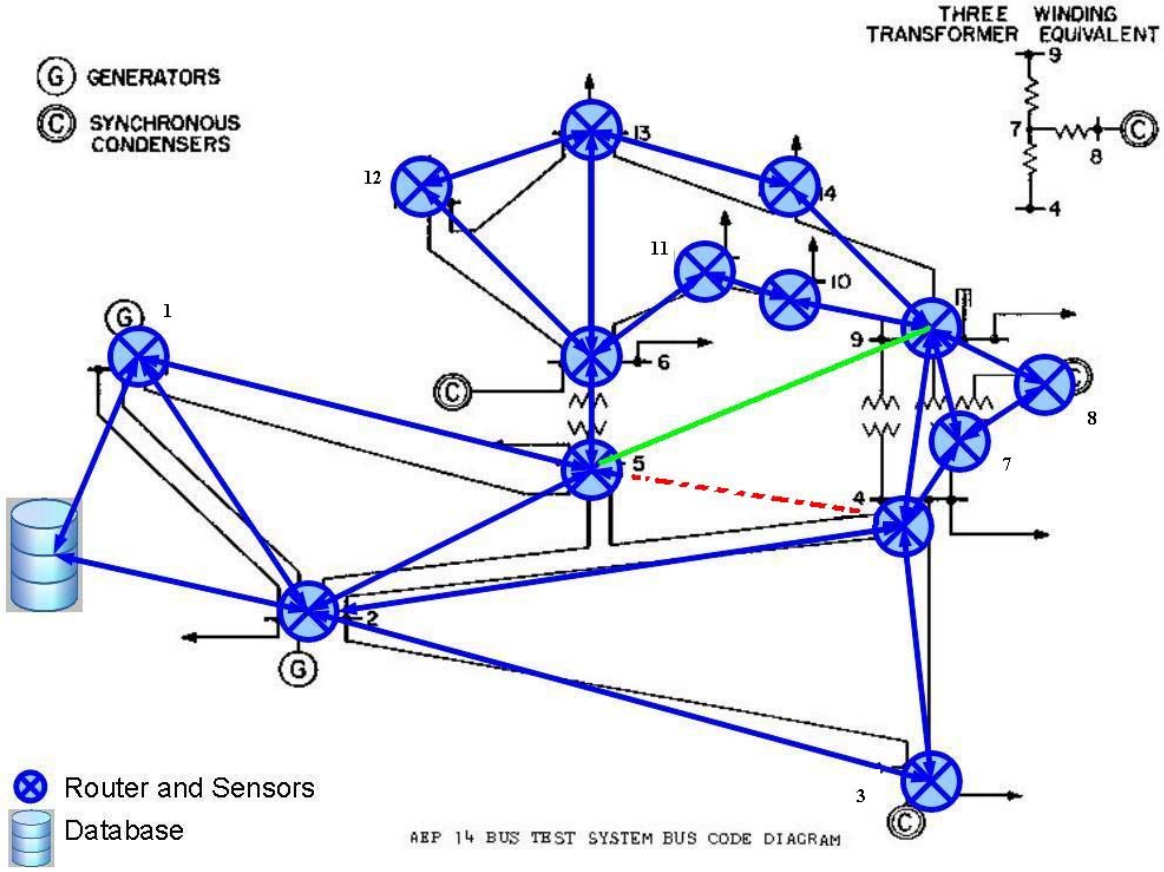
The next step is to evaluate different configurations of this communications network. The goal of this setup is to find the optimal network configurations to increase reliability and robustness of the SCADA system. Below, Figures 5.3 and 5.4 show two additional topologies used in the simulations. The green solid line is the added link, whereas the red dotted line is the link removed.

Figure 5.3 Communications Network Topology 2 modified from Figure 5.2



The total number of links and routers were kept constant due to the increased cost associated with the addition of them. The two additional cases were chosen to represent low-cost changes that could be incorporated into the communication network. Preliminary simulations were completed to evaluate which links to change. We chose these two because they were good examples of the average cases.

Figure 5.4 Communications Network Topology 3 modified from Figure 5.2



In each topology, we assume the network traffic has the same initial parameters. Each node is set to send traffic at the same interval and set to send the same size data packet. The data size parameter is set to equal 200 for each node. We also assume the link capacities for each link that are common in between the topologies are the same. This will allow us to compare the network performances between the three different topologies.

Below is table showing the input parameters for each router. These parameters are kept constant for each simulation.

Table 5.1 Router Parameters for the Simulations

Router Name	BufferSize (kB)	ClockSpeed (MHz)
1	600	800
2	600	800
3	100	400
4	100	400
5	200	600
6	200	400
7	100	400
8	100	400
9	100	400
10	100	400
11	100	400
12	100	400
13	100	400
14	100	400

The parameters are chosen based an average of real routers that could be used in the power grid communication systems. The core routers were set up to be larger than the peripheral routers.

5.2 Simulation Results

This section explains the different simulations and results. The first subsection evaluates the three different topologies and finds important links in them. The second two subsections use failure scenarios and evaluate the need for the intelligent rerouting implementation.

5.2.1 Delay Comparisons with Single Link Failures with Intelligent Rerouting

In this scenario, single links are failed at the same time in the simulation. This is evaluated for each topology. The communications network was enabled to reroute when congestion was detected. The following graphs show the delay in each topology for select single link failures. We chose the single link failures to represent the core of the communications network.

Figure 5.5 Delay in links for Topology 1

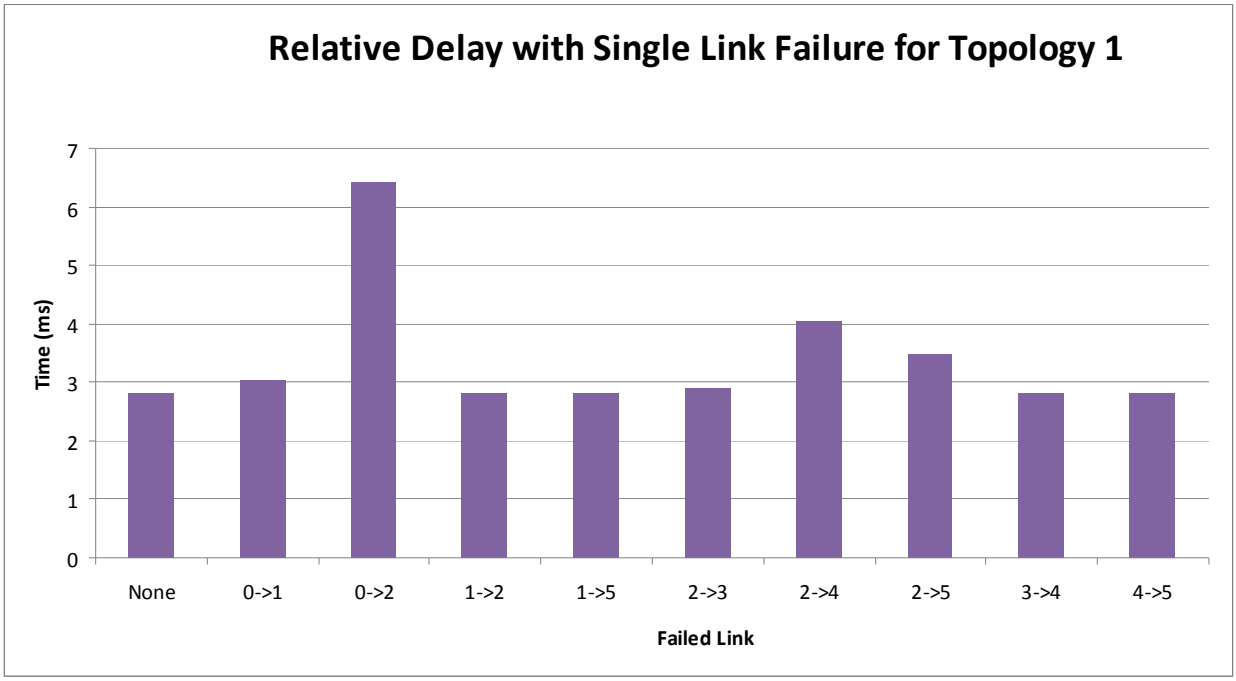


Figure 5.5 shows the average delay per packet in the communications network with single failed links in Topology 1. Link 0→2 generates the most delay; this means link 0→2 is an important link. By the same measure, link 2→4 is the second most important link.

Figure 5.6 Delay in links for Topology 2

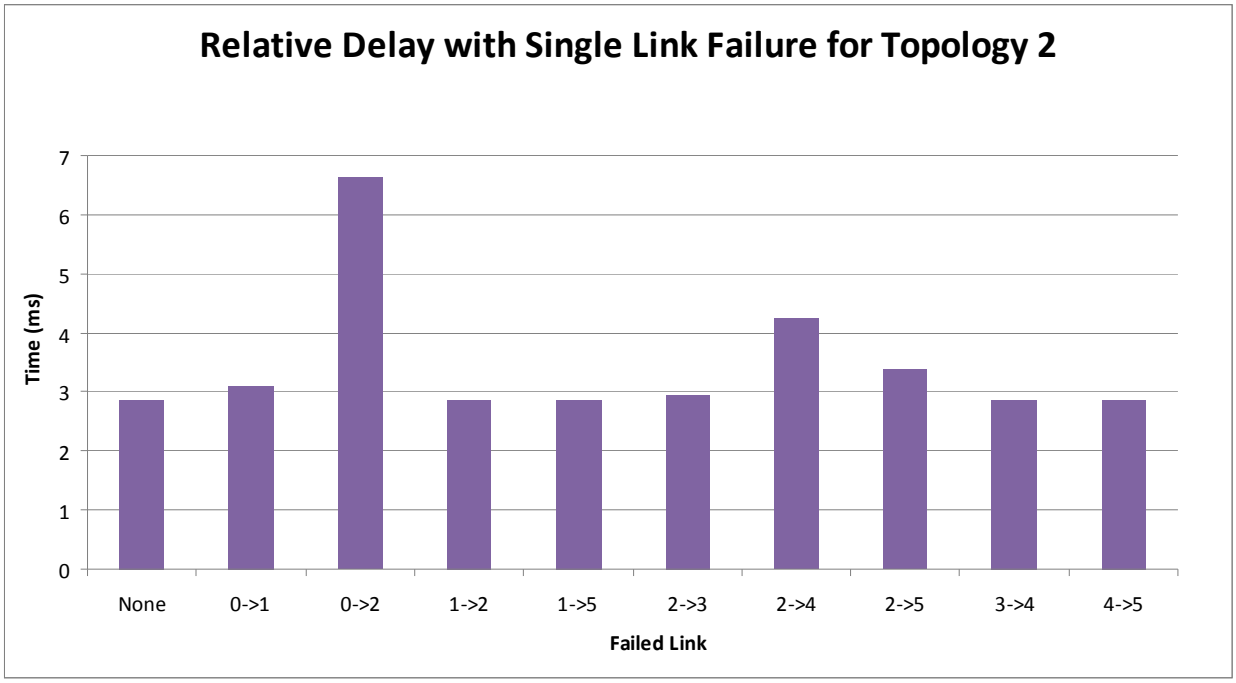
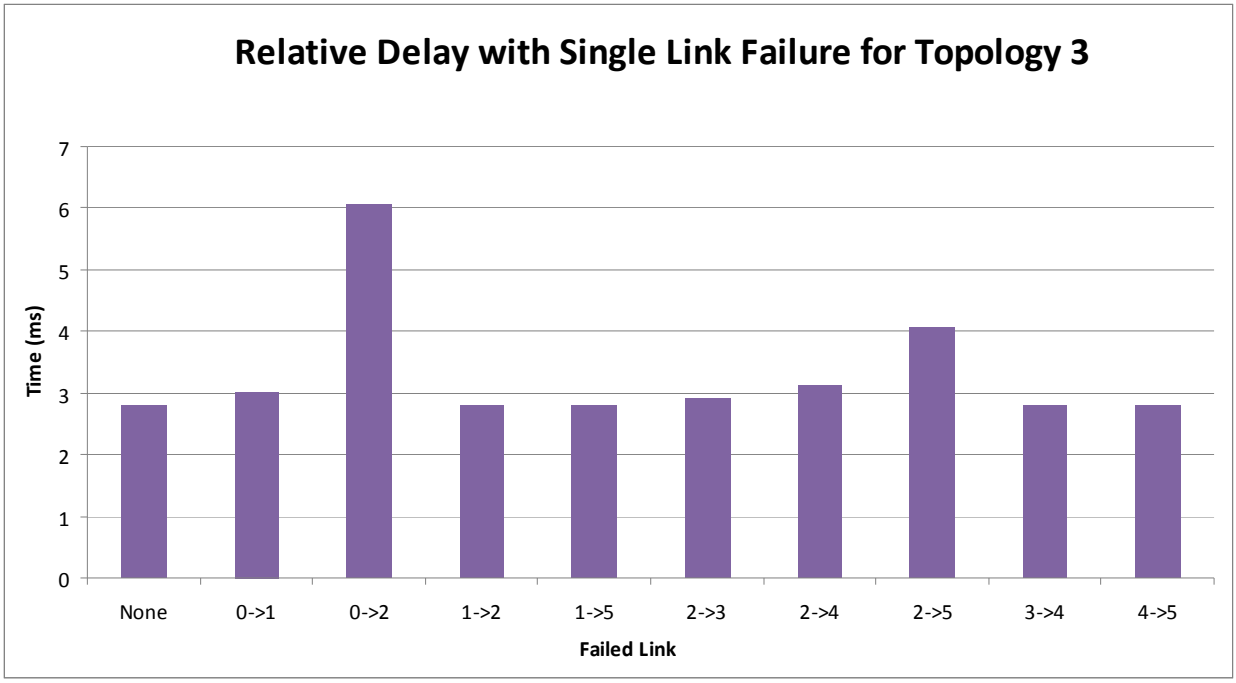


Figure 5.6 shows the similar results as Topology 1, the order of importance of the links remains the same. This means the difference in the importance of links between the two topologies is not very significant.

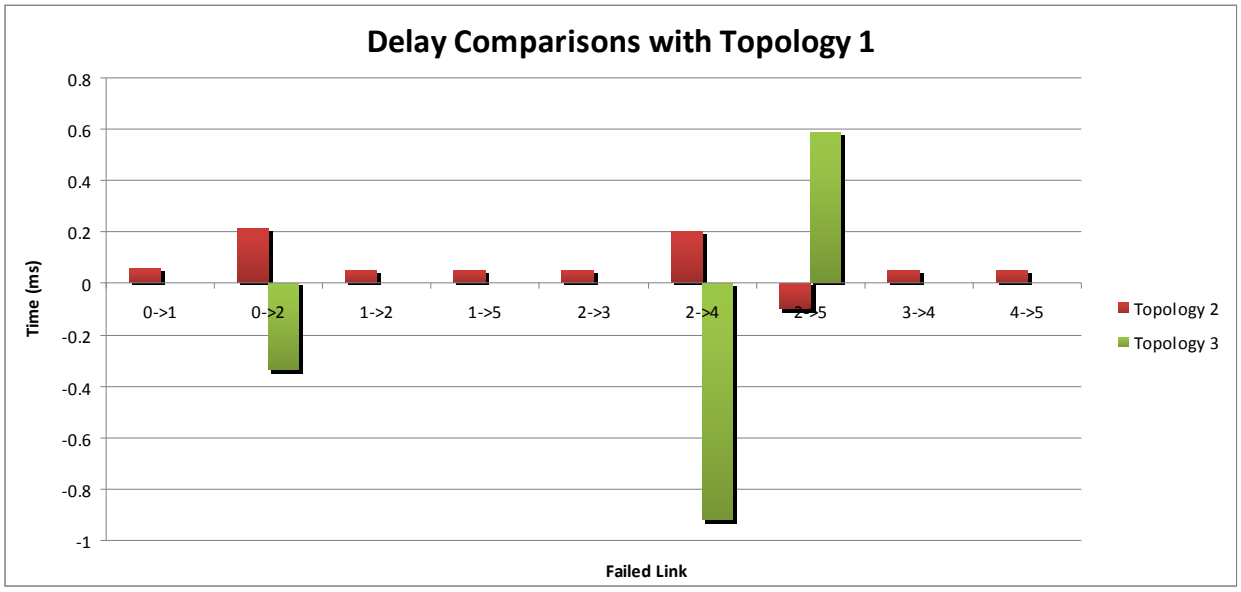
Figure 5.7 Delay in links for Topology 3



For Topology 3, link 0→2 is still important. The difference is that link 2→5 has become more important than link 2→4. This shows that Topology 3 has significant differences in how the traffic flows through it compared to topology 1.

Figure 5.8 shows the previous graphs combined. This graph shows the relative difference between the delays in each single failure compared to the same failure in Topology 1. This graph shows that failing links 0→2, 2→4, and 2→5 have the largest variations in the delays between topologies

Figure 5.8 Delay in links compared to Topology 1



The single link failures with rerouting do not cause any nodes to lose connectivity with the database. This simulation was designed to evaluate the importance of the links in each topology. In the next two sections, failure scenarios are used. These scenarios are roughly based off the findings from this section.

5.2.2 Failure Scenarios without Intelligent Rerouting

Table 5.2 shows the different failures that are simulated in both this section and in the next section. These scenarios were chosen to show different ways the communications network could be broken. These scenarios were chosen based off the single link failure from the previous section. These scenarios are just a subset of possible scenarios that could have been chosen. For larger communications networks, this test case would need to be larger. To choose the larger test case set, analysis of single link failures would need to be completed and analyzed for the larger topologies.

Table 5.2 Failure Scenarios

Scenario Name	F0	F1	F2	F3	F4	F5	F6
Link(s) Failed	None	0 → 2	2 → 5	2 → 3 2 → 4	0 → 1	0 → 1 2 → 4	1 → 5 1 → 2 2 → 5

In this section, the simulations are performed without any rerouting. This causes the nodes to lose contact with the database. Table 5.3 shows the nodes that lost communication links with the database. The shortest path algorithm, described in section 4.3.1, chose the paths the data initially follows.

Table 5.3 Disconnected nodes due to failure without rerouting algorithm

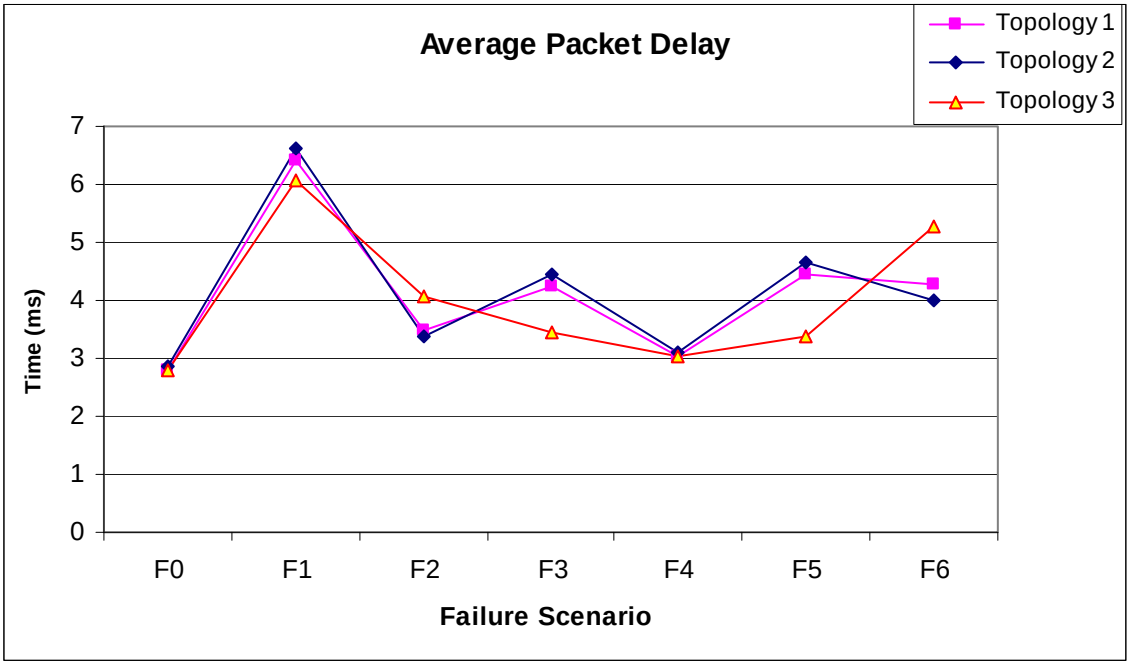
Scenario Name	F0	F1	F2	F3	F4	F5	F6
Topology 1	None	2, 3, 4, 6, 7, 8, 9, 10, 12, 14	6, 12	3, 4, 7, 8, 9, 10, 14	1, 5, 11, 13	1, 4, 5, 7, 8, 9, 10, 11, 13 14	5, 6, 11, 12, 13
Topology 2	None	2,3,4,6,7,8, 9,10,11, 13,14	6, 11	7, 8, 9, 10, 13, 14	1, 5, 12	1, 4, 5, 7, 8, 9, 10, 12, 13, 14	5, 6, 11, 12
Topology 3	None	2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14	6, 8, 9, 10, 11, 12, 13, 14	3, 4, 7	1, 5	1, 4, 5, 7	5, 6, 8, 9, 10, 11, 12, 13, 14

Table 5.2 shows that many nodes were disconnected from the communications network. Many nodes lose the connectivity to the database because they do not have the ability to reroute. This shows the need for the intelligent rerouting algorithm to be implemented.

5.2.3 Failure Scenarios with Intelligent Rerouting

This subsection describes the results with the rerouting algorithm. In this section, all of the nodes retain connectivity with the database. The delay and packet loss through the communications network are described. This simulation uses the Failure Scenarios in Table 5.1 with each of the three topologies from Section 5.1. Figure 5.9 shows the average packet delay through the communications network for each failure scenario in each topology.

Figure 5.9 Average Packet Delay

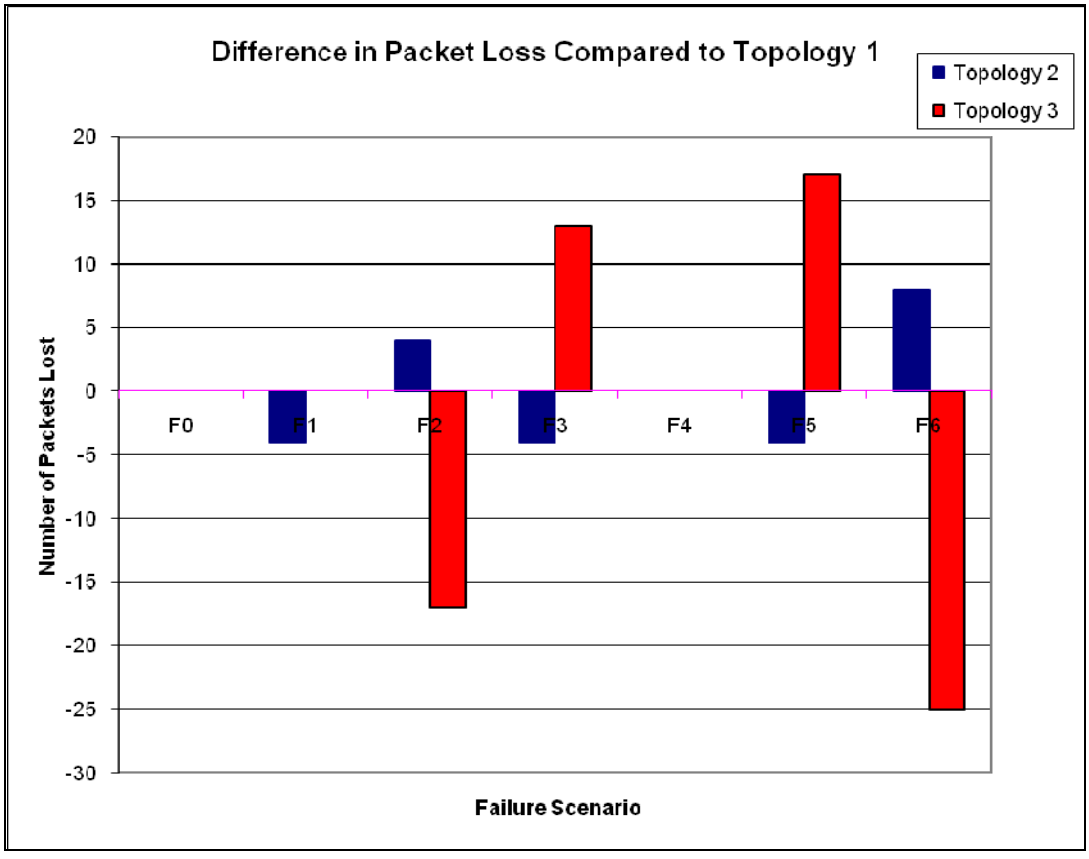


Topology 1, in pink, is the topology that exactly matched the power grid. Topology 3, in yellow, seems to have the least delay in the majority of the scenarios. This shows that Topology 3 could be the better topology than either Topology 1 or Topology 2 for this communications network. Topology 3 shows an overall decrease in average delay by 0.095 ms compared to Topology 1. The worst case shows Topology 3 increasing the delay by 0.99 ms compared to

Topology 1. Topology 2 shows an overall increase in average delay of 0.061 compared to Topology 1. The worst case shows Topology 2 increasing the delay by 0.23 ms compared to Topology 1.

Figure 5.10 shows the number of packets lost in each simulation compared to Topology 1. The simulations for F0 show no packet loss because there were not any communications network failures. The packet loss for each failure scenario seems to be similar across the different topologies. Failure scenario F5 has the greatest packet loss in all three topologies. This could mean the links from 1→0 and 2→4 have significant traffic in all three topologies. Failure scenarios F6 and F2 show cases in which Topology 3 has less packet loss than the other topologies.

Figure 5.10 Packet Loss



This simulation shows the effects of the rerouting algorithm in the communications network. As links fail, the rerouting algorithm is able to choose new paths for the packets,

allowing the data to still be received by the database. The communications networks see increased delay because of this rerouting.

Chapter 6 - Conclusion

This chapter discusses the results of the simulation program, connection of the results to the power grid, and the future work on this project. This thesis presented a simulator program that can be used to evaluate the communication networks of the power grid. We had two main contributions in this paper. The first contribution is the development of the network simulator. The second main contribution is the results from the simulations.

6.1 Relation of the Results to Power Grid

The results of the previous simulations show that the topology of the communications network is important. The topology that exactly matches the power grid topology is not necessarily always the best. The communications network needs to be thoroughly researched and evaluated before being implemented or changed in the power grid systems.

It is very critical to keep the delay in the communications network at a minimum. In [27], the cascading effect on power grid networks from failures was studied. [27] describes how a mitigation strategy could be used to reduce the failures in the power grid. The mitigation strategy consists of reducing the load in a portion of the grid to stop the cascading failure of the power grid. This mitigation strategy needs to be communicated across the communications network in a very short time for it to be successful. If the control center is unable to receive the information from the substation or unable to send out the information to the nodes quickly it does not matter if there was a mitigation plan because it would be of little use.

The topology of the communications network is very important to design correctly. The simulator program can help initially evaluate different topologies proposed for the communications networks.

6.2 Future Work

This section describes future work that a researcher could continue in the project.

6.2.1 More complex simulation

One sub-project could be doing complex simulations using the simulator. IEEE has published larger test cases that could be used. In addition, the researcher could implement real

world power grid networks and their communications networks. This could provide insight into how efficient the current SCADA systems are and ways in which the systems could be improved.

6.2.2 Connecting the simulators

The communications network simulator could be connected to the simulator designed in [27] or other commercial power grid simulators. This would provide realistic data sizes and content to the communications network. The simulator in [27] can provide the data and destination for the messages in the communications network. The network simulator can provide the mitigation information to the nodes in the power grid simulator. This could be a way to study how the delays in the communications network could be detrimental to the reliability of the whole system.

6.2.3 More realistic simulation

A more realistic next step of this research is to implement a lab with the actual equipment used in the industry. The Smart Grid lab is described in Appendix G.

Bibliography

[1] Daneels ,A.; Salter, S., "What is SCADA?" in International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, Trieste, Italy, pp. 339-343.

[2] Davis, C.M.; Tate, J.E.; Okhravi, H.; Grier, C.; Overbye, T.J.; Nicol, D., "SCADA Cyber Security Testbed Development," Power Symposium, 2006. NAPS 2006. 38th North American, pp.483-488, 17-19 Sept. 2006.

[3]Giani, A.; Satry, S.; Johansson, K.; Sanberg, H., "The VIKING Project: An Initiative on Resilient Control of Power Networks" IEEE International Symposium on Resilient Control Systems, Idaho Falls, ID, USA, 2009.

[4] VIKING consortium (2010, March 23) *The Viking Project* [ONLINE]. Available: http://www.vikingproject.eu/

[5] US Department of Energy: Office of Electricity Deliver and Energy Reliability, "National SCADA Test Bed Program: Multi-Year plan FY2008-2013," Jan 2008.

[6] Idaho National Laboratory, "National SCADA Test Bed: Fact Sheet," http://www.inl.gov/scada/, 2007.

[7]Dondossola, G.; Garrone, F.; Szanto, J.; Fiorenza, G.; "Emerging Information Technology Scenarios for the Control and Management of the Distribution Grid," in *19th International Conference on Electricy Distibution,* Vienna, 2007.

[8] Giani, A.; Karsai, G.; Roosta, T.; Shah, A.; Sinopoli, B.; Wiley, J., "A testbed for secure and robust SCADA systems," *SIGBED Rev.* 5, 2, Article 4, July 2008.

[9]Karsai, G., "TRUST for SCADA: A Simulation-Based Experimental Platform". Presentation, 29, November, 2009.

[10] Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, E.; Havlin, S., "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, pp. 1025, 2010.

[11] Pollet, J., "The Past, Present, and Future of Securing Electric Power Systems," *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on* System Sciences, pp.1-7, 5-8 Jan. 2009.

[12] Kalapatapu, R., "SCADA Protocols and Communication Trends" in ISA EXPO, 2004.

[13] Mander, T.; Wang, L.; Cheung, R.; Nabhani, F., "Apapting the Pretty Good Privacy Security Style to Power System Distributed Network Protocol" in *Large Engineering Systems Conference on Power Engineering,* 2006, pp 79-83.

[14] Peterson, L.; Davie, B., "Computer Networks: A Systems Approach." San Francisco: Morgan Kaufmann Publishers, 2007.

[15] Gilchrist, G., "Secure Authentication for DNP3" in *Power and Energy Society General Meeting- Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp 1-3.

[16] Majdalawieh, M.; Parisi-Presicce, F.; Wijesekera, D., "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework" in *Advances in Computer, Information, and Systems Sciences, and Engineering,* 2006, pp 227-234.

[17] Clarke, G.; Reynders, D., *Practical Modern SCADA Protocols.* Oxford: Newnes, 2004.

[18] Klein, S.A., "Security, cost, and operational benefits of EC-61850," *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE* , pp.1-3, 20-24 July 2008.

[19] Montignies, P.; Angays, P.; Guise, L., "Is there a value in deploying IEC 61850 communication into oil & gas EMCS?," *PCIC Europe, 2009. PCIC EUROPE '09. Conference Record* , pp.103-112, 26-28 May 2009.

[20] Fries, S.; Hof, H.J.; Seewald, M., "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments," *Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on* , pp.135-142, 9-15 May 2010.

[21] Nordbotten, N.A. , "XML and Web Services Security Standards," *Communications Surveys & Tutorials, IEEE* , vol.11, no.3, pp.4-21, 3rd Quarter 2009.

[22] Cleveland, F.M., "IEC 62351-7: communications and information management technologies -network and system management in power system operations," *Transmission and Distribution Conference and Exposition, 2008. T&D. IEEE/PES* , pp.1-4, 21-24 April 2008.

[23] Rahman, S., "Smart Grid Expectations: what will make it a reality," IEEE Power & Energy Magazine, September/October 2009.

[24] Qi, Y., (2010, October 5) *K-shortest paths* [ONLINE] Available: http://code.google.com/p/k-shortest-paths/

[25] Porwal, M.K.; Yadav, A.; Charhate, S.V., "Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic Distribution in OSPF and MPLS," Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference on, pp.187-192, 16-18 July 2008.

[26] UW Electrical Engineering, *Power Systems Test Case Archive* [ONLINE] Available: http://www.ee.washington.edu/research/pstca/

[27] Pahwa, S., "Topological Analysis and Mitigation Strategies for Cascading Failures in Power Grid Networks," M.S. thesis, ECE, KSU, Manhattan, KS 2010.

[28] Gordon, M.; Shahidehpour, M., "A Living Laboratory [The Business Scene]," Power and Energy Magazine, IEEE , vol.9, no.1, pp.18-98, Jan.-Feb. 2011.

[29] Department of Electrical and Computer Engineering (2011, March 6) *IIT Establishes $12.6 Million Smart Grid Training Center* [ONLINE] Available: www.iit.edu/engineering/ece/news/

[30] Ali, I.; Thomas, M.S., "GOOSE based Protection Sscheme Implementation & Testing in Laboratory," 2011 IEEE PES Innovative Smart Grid Technologies Conference, Jan. 2011.

[31] Mohammed, O.A.; Nayeem, M.A.; Kaviani, A.K., "A laboratory based microgrid and distributed generation infrastructure for studying connectivity issues to operational power systems," Power and Energy Society General Meeting, 2010 IEEE , vol., no., pp.1-6, 25-29 July 2010.

[32] Choi, S.; Kim, B.; Cokkinides, G.J.; Meliopoulos, A. P. S., "Autonomous state estimation for the smart grid - laboratory implementation,"Transmission and Distribution Conference and Exposition, 2010 IEEE PES , vol., no., pp.1-8, 19-22 April 2010.

[33] Kezunovic, M.; , "Teaching the smart grid fundamentals using modeling, simulation, and hands-on laboratory experiments," Power and Energy Society General Meeting, 2010 IEEE , vol., no., pp.1-6, 25-29 July 2010.

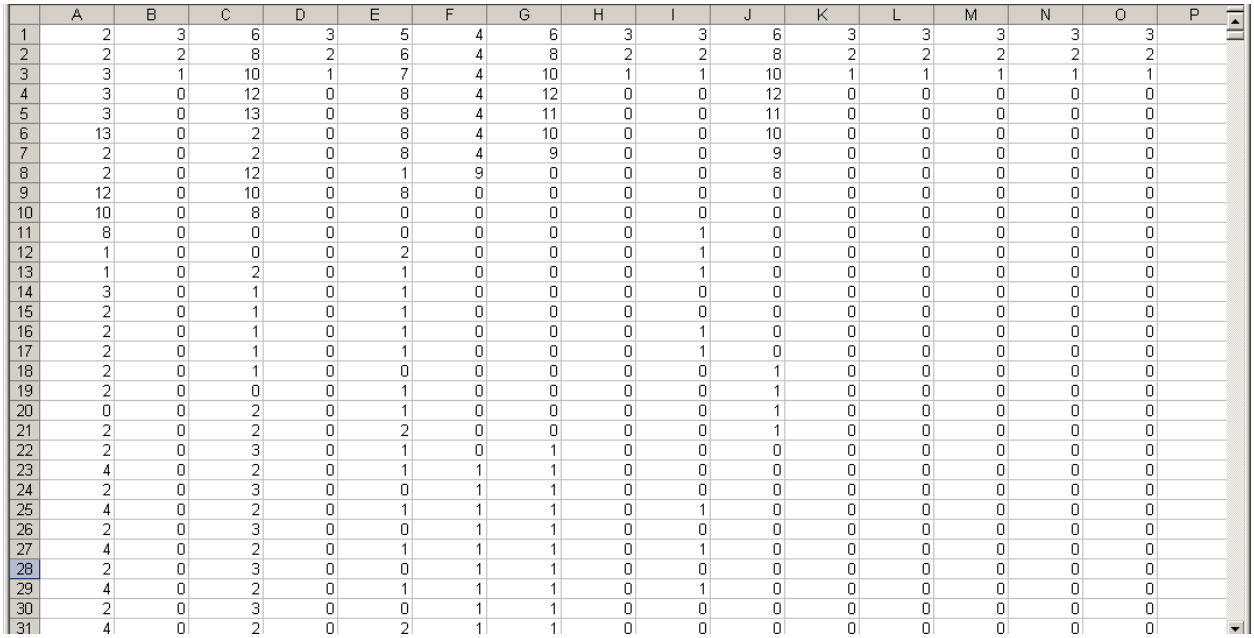
[34] Dutta, P., (2011 March 31). *Smart Energy Campus Initiative* [ONLINE] Available: http://epipc01.tamu.edu/seci/index.html

[35] Reddi, R.M.; Srivastava, A.K , "Real time test bed development for power system operation, control and cyber security," North American Power Symposium (NAPS), 2010 , vol., no., pp.1-6, 26-28 Sept. 2010.

[36] Srivastava, A.K., [ONLINE] Available: http://school.eecs.wsu.edu/node/909

Appendix A - Data File

Figure A.1 Example Data File



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	6	3	5	4	6	3	3	6	3	3	3	3	3	
2	2	2	8	2	6	4	8	2	2	8	2	2	2	2	2	
3	3	1	10	1	7	4	10	1	1	10	1	1	1	1	1	
4	3	0	12	0	8	4	12	0	0	12	0	0	0	0	0	
5	3	0	13	0	8	4	11	0	0	11	0	0	0	0	0	
6	13	0	2	0	8	4	10	0	0	10	0	0	0	0	0	
7	2	0	2	0	8	4	9	0	0	9	0	0	0	0	0	
8	2	0	12	0	1	9	0	0	0	8	0	0	0	0	0	
9	12	0	10	0	8	0	0	0	0	0	0	0	0	0	0	
10	10	0	8	0	0	0	0	0	0	0	0	0	0	0	0	
11	8	0	0	0	0	0	0	0	1	0	0	0	0	0	0	
12	1	0	0	0	2	0	0	0	1	0	0	0	0	0	0	
13	1	0	2	0	1	0	0	0	1	0	0	0	0	0	0	
14	3	0	1	0	1	0	0	0	0	0	0	0	0	0	0	
15	2	0	1	0	1	0	0	0	0	0	0	0	0	0	0	
16	2	0	1	0	1	0	0	0	1	0	0	0	0	0	0	
17	2	0	1	0	1	0	0	0	1	0	0	0	0	0	0	
18	2	0	1	0	0	0	0	0	0	1	0	0	0	0	0	
19	2	0	0	0	1	0	0	0	0	1	0	0	0	0	0	
20	0	0	2	0	1	0	0	0	0	1	0	0	0	0	0	
21	2	0	2	0	2	0	0	0	0	1	0	0	0	0	0	
22	2	0	3	0	1	0	1	0	0	0	0	0	0	0	0	
23	4	0	2	0	1	1	1	0	0	0	0	0	0	0	0	
24	2	0	3	0	0	1	1	0	0	0	0	0	0	0	0	
25	4	0	2	0	1	1	1	0	1	0	0	0	0	0	0	
26	2	0	3	0	0	1	1	0	0	0	0	0	0	0	0	
27	4	0	2	0	1	1	1	0	1	0	0	0	0	0	0	
28	2	0	3	0	0	1	1	0	0	0	0	0	0	0	0	
29	4	0	2	0	1	1	1	0	1	0	0	0	0	0	0	
30	2	0	3	0	0	1	1	0	0	0	0	0	0	0	0	
31	4	0	2	0	2	1	1	0	0	0	0	0	0	0	0	

This is a partial part of the output data file. Each value represents the number of packets in each router and the database.

Appendix B - Statistics File

DataFileName.txt
RouterFileName.txt
NodeFileName.txt
Database Name: N0
ShortestPathFileName.txt

Starting Simulation
Router 0 has 0 errors
    and received 57707 messages
    which is a 0% failure rate.
    and has 1.625% of buffer filled at maximum
    and has 0.334005% of buffer filled on average

Router 1 has 0 errors
    and received 6970 messages
    which is a 0% failure rate.
    and has 0.666667% of buffer filled at maximum
    and has 9.25926e-005% of buffer filled on average

Router 2 has 0 errors
    and received 50737 messages
    which is a 0% failure rate.
    and has 2.16667% of buffer filled at maximum
    and has 0.351435% of buffer filled on average

Router 3 has 0 errors
    and received 4230 messages
    which is a 0% failure rate.
    and has 4% of buffer filled at maximum
    and has 0.000555556% of buffer filled on average

Router 4 has 0 errors
    and received 25581 messages
    which is a 0% failure rate.
    and has 8% of buffer filled at maximum
    and has 1.02426% of buffer filled on average

Router 5 has 0 errors
    and received 15664 messages
    which is a 0% failure rate.
    and has 4.5% of buffer filled at maximum
    and has 0.293241% of buffer filled on average

Router 6 has 0 errors
    and received 12626 messages
    which is a 0% failure rate.
    and has 6% of buffer filled at maximum
    and has 0.233056% of buffer filled on average

Router 7 has 0 errors
    and received 2372 messages
    which is a 0% failure rate.

and has 4% of buffer filled at maximum
and has 0.000555556% of buffer filled on average

Router 8 has 0 errors
and received 6478 messages
which is a 0% failure rate.
and has 4% of buffer filled at maximum
and has 0.259259% of buffer filled on average

Router 9 has 0 errors
and received 19673 messages
which is a 0% failure rate.
and has 12% of buffer filled at maximum
and has 0.339444% of buffer filled on average

Router 10 has 0 errors
and received 4689 messages
which is a 0% failure rate.
and has 4% of buffer filled at maximum
and has 0.000555556% of buffer filled on average

Router 11 has 0 errors
and received 3852 messages
which is a 0% failure rate.
and has 4% of buffer filled at maximum
and has 0.000555556% of buffer filled on average

Router 12 has 0 errors
and received 3268 messages
which is a 0% failure rate.
and has 4% of buffer filled at maximum
and has 0.000555556% of buffer filled on average

Router 13 has 0 errors
and received 2840 messages
which is a 0% failure rate.
and has 4% of buffer filled at maximum
and has 0.000555556% of buffer filled on average

Router 14 has 0 errors
and received 2510 messages
which is a 0% failure rate.
and has 4% of buffer filled at maximum
and has 0.000555556% of buffer filled on average

Node N1 has received 982 messages
Node N2 has received 900 messages
Node N3 has received 831 messages
Node N4 has received 772 messages
Node N5 has received 720 messages
Node N6 has received 675 messages
Node N7 has received 636 messages
Node N8 has received 600 messages
Node N9 has received 569 messages

Node N10 has received 540 messages
Node N11 has received 515 messages
Node N12 has received 491 messages
Node N13 has received 470 messages
Node N14 has received 450 messages
Node N15 has received 432 messages
Node N16 has received 416 messages
Node N17 has received 400 messages
Node N18 has received 386 messages
Node N19 has received 373 messages
Node N20 has received 360 messages
Node N21 has received 349 messages
Node N22 has received 338 messages
Node N23 has received 328 messages
Node N24 has received 318 messages
Node N25 has received 309 messages
Node N26 has received 300 messages
Node N27 has received 292 messages
Node N28 has received 285 messages
Node N29 has received 277 messages
Node N30 has received 1080 messages
Node N31 has received 982 messages
Node N32 has received 900 messages
Node N33 has received 831 messages
Node N34 has received 772 messages
Node N35 has received 720 messages
Node N36 has received 675 messages
Node N37 has received 635 messages
Node N38 has received 600 messages
Node N39 has received 569 messages
Node N40 has received 540 messages
Node N41 has received 515 messages
Node N42 has received 491 messages
Node N43 has received 470 messages
Node N44 has received 450 messages
Node N45 has received 432 messages
Node N46 has received 416 messages
Node N47 has received 400 messages
Node N48 has received 386 messages
Node N49 has received 373 messages
Node N50 has received 360 messages
Node N51 has received 349 messages
Node N52 has received 338 messages
Node N53 has received 328 messages
Node N54 has received 318 messages
Node N55 has received 309 messages
Node N56 has received 300 messages
Node N0 has received 28854 messages
Total Sent by all nodes: 28854
Total Received by all databases: 28854
Total Received by all : 57707
Average Packet delay: 1.40416
Total number nodes disconnected from their database: 0

Appendix C - Router File

15

format is: RouterName BufferSize ClockSpeed (MHz)

0 800 1600

1 600 800

2 600 800

3 100 400

4 100 400

5 200 600

6 200 400

7 100 400

8 100 400

9 100 400

10 100 400

11 100 400

12 100 400

13 100 400

14 100 400

Appendix D - Node File

N0 0 10 0 200 N0
N1 1 10 1 200 N0
N2 1 10 1 200 N0
N3 1 10 1 200 N0
N4 1 10 1 200 N0
N5 2 10 1 200 N0
N6 2 10 1 200 N0
N7 2 10 1 200 N0
N8 2 10 1 200 N0
N9 3 10 1 200 N0
N10 3 10 1 200 N0
N11 3 10 1 200 N0
N12 3 10 1 200 N0
N13 4 10 1 200 N0
N14 4 10 1 200 N0
N15 4 10 1 200 N0
N16 4 10 1 200 N0
N17 5 10 1 200 N0
N18 5 10 1 200 N0
N19 5 10 1 200 N0
N20 5 10 1 200 N0
N21 6 10 1 200 N0
N22 6 10 1 200 N0
N23 6 10 1 200 N0
N24 6 10 1 200 N0
N25 7 10 1 200 N0
N26 7 10 1 200 N0
N27 7 10 1 200 N0
N28 7 10 1 200 N0
N29 8 10 1 200 N0
N30 8 10 1 200 N0
N31 8 10 1 200 N0
N32 8 10 1 200 N0
N33 9 10 1 200 N0
N34 9 10 1 200 N0
N35 9 10 1 200 N0
N36 9 10 1 200 N0
N37 10 10 1 200 N0
N38 10 10 1 200 N0

.

.

.

Appendix E - Shortest Path File

1, 0
1, 2, 0
1, 5, 2, 0
1, 5, 4, 2, 0
1, 5, 4, 3, 2, 0
1, 5, 6, 11, 10, 9, 4, 2, 0
1, 5, 6, 13, 14, 9, 4, 2, 0
1, 5, 6, 11, 10, 9, 4, 3, 2, 0
1, 5, 6, 12, 13, 14, 9, 4, 2, 0
1, 5, 6, 13, 14, 9, 4, 3, 2, 0
2, 0
2, 1, 0
2, 5, 1, 0
2, 4, 5, 1, 0
2, 3, 4, 5, 1, 0
2, 4, 9, 14, 13, 6, 5, 1, 0
2, 4, 9, 10, 11, 6, 5, 1, 0
2, 3, 4, 9, 14, 13, 6, 5, 1, 0
2, 4, 9, 14, 13, 12, 6, 5, 1, 0
2, 3, 4, 9, 10, 11, 6, 5, 1, 0
3, 2, 0
3, 4, 2, 0
3, 2, 1, 0
3, 4, 5, 2, 0
3, 4, 5, 1, 0
3, 4, 2, 1, 0
3, 2, 5, 1, 0
3, 4, 5, 1, 2, 0
3, 2, 4, 5, 1, 0
3, 4, 2, 5, 1, 0
4, 2, 0
4, 5, 2, 0
4, 5, 1, 0
4, 3, 2, 0
4, 2, 1, 0
4, 2, 5, 1, 0
4, 5, 1, 2, 0
4, 5, 2, 1, 0

.

.

.

Appendix F - MATLAB Script

```
figure(5)
A=load('Remove_0_2_at1000.txt');
[x,y]=size(A);
colors=['b' 'g' 'k' 'c' 'm' 'r' 'b' 'g' 'k' 'c' 'm' 'r' 'b' 'g' 'k' 'c' 'm'
'r'];
for i=1:1:floor(y/2)
    subplot(ceil(y/2),2,i);
    plot(A(:,i),colors(i));
    xlim([0 x]);
    ylim([0 max(max(A(:,i)))]);
    t=sprintf('Data from Router %d', i-1);
    title(t)

end

for i=1:1:ceil(y/2)
    subplot(ceil(y/2),2,i+floor(y/2));
    plot(A(:,i+floor(y/2)),colors(i));
    xlim([0 x]);
    ylim([0 max(max(A(:,i+floor(y/2))))]);
    t=sprintf('Data from Router %d', i+floor(y/2)-1);
    title(t)

end
```

Appendix G - Smart Grid Lab

Burns and McDonnell has collaborated with the Electrical and Computer Engineering (ECE) department at Kansas State University (K-State) to develop a Smart Grid Lab. This lab will be located inside of the ECE department and the lab is currently in the planning stages. The next few sections discuss the plans for the lab and other related labs. The Smart Grid Lab is a natural extension from using simulators to study the communication network and the power grid. The lab will provide results that are more realistic and will be able to teach students about how the systems actually work.

G.1 Lab Goals

The goal of the lab is to provide a hands-on learning environment for students in the ECE department. This lab will be applicable to students in both the networking emphasis and the power emphasis in the ECE department. The networking students will be able to use the lab to perform basic networking exercises during their beginning courses. With some additional coursework, the students will be able to perform complex network simulations using real world equipment. The power students will be able to learn about how the power grid is changing. They will be able to enter into industry with real world experience on the Smart Grid and how the networking side of the power grid works.

G.2 Related Labs

This section describes Smart Grid labs found at other universities. The amount of information varies between the universities. This section will provide the information found in research papers and from online resources.

G.2.1 Illinois Institute of Technology

Illinois Institute of Technology (IIT) is creating a Smart Grid Education and Workforce-Training Center. This program is aimed at educating utilities, corporations, veterans, K-12 students, community college students, labor unions, educators, and university students. This lab is funded in part by the DOE (Department of Energy) and has a total funding amount of more than $12.6 million [28]. IIT started the lab in January of 2011. The funds allow three years to complete the design and implementation of the lab. Then, the funds allow for three more years

of operational support. After the initial six years, the lab will be supported by membership fees [29].

The lab will provide different levels of education about the Smart Grid. The fundamental level will be focused on K-12 and community college students. These students will learn about basic electrical theory and Smart Grid fundamentals. The applied level will be for industry personnel and others with prior knowledge of power systems. They will learn about the new technology and other new skills to keep them employable. The last level is the advanced level. This is focused towards university students seeking bachelor degrees or higher [28]. As of this time, no more information about the lab is available.

G.2.2 Jamia Millia Islamia University

Jamia Millia Islamia University is in New Delhi, India. This lab was designed to study IEC 61850. The lab demonstrates the peer-to-peer communication of the GOOSE message model. The lab setup was described in [30]. Figure G.1 shows the schematic of the lab.

Figure G.1 Jamia Millia Laboratory schematic from [30]

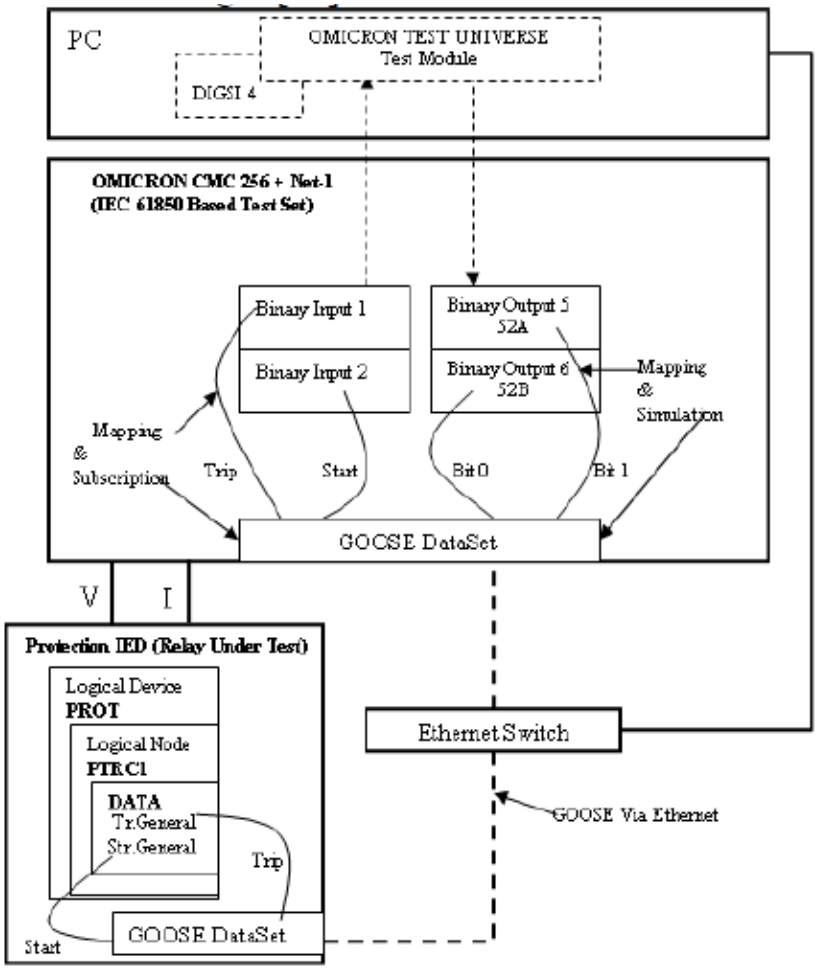


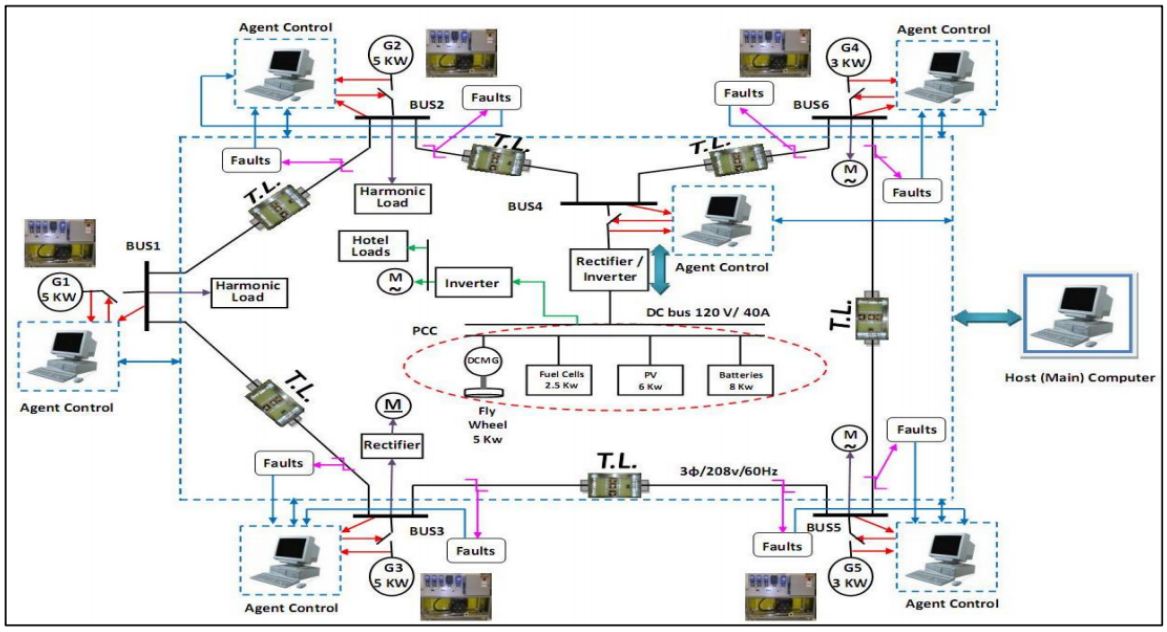
Figure G.1 shows the software being used, DIGSI 4, in the top box; the OMICRON test set in the next box, the power grid equipment in the bottom left box and the Ethernet switch in the bottom right [30]. Figure G.2 is the actual lab and the equipment described in Figure G.2.

Figure G.2 Jamia Millia Laboratory picture from [30]

G.2.3 Florida International University

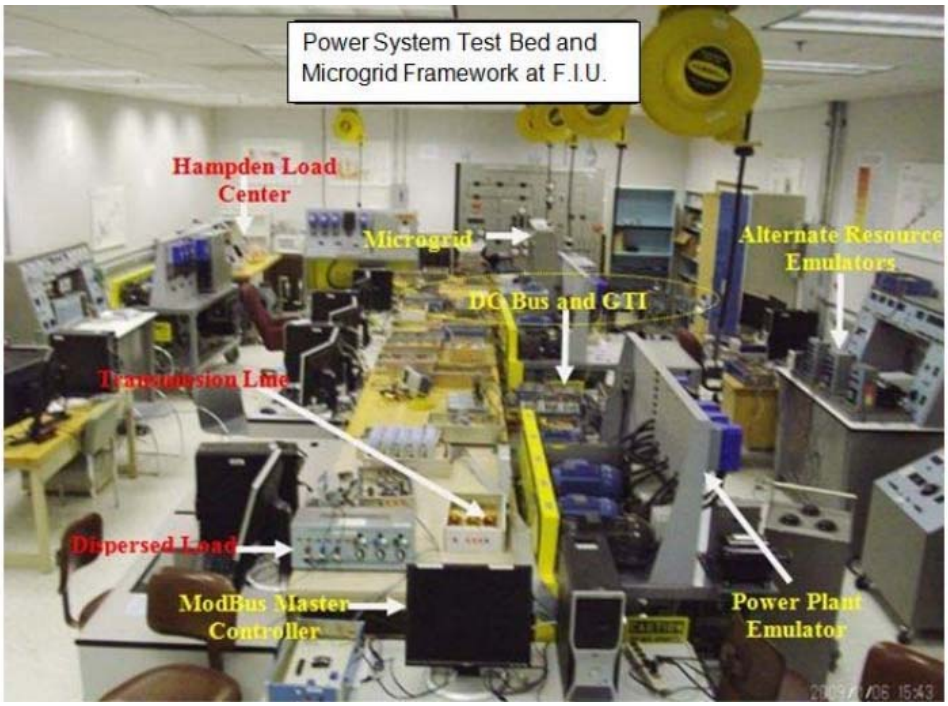
Florida International University has a lab designed to study distributed generation and connectivity issues. The information published in [31] discusses the lab being used to simulate mostly the power side of the grid. Reference [31] states the research on the communication network will soon be published. Figure G.3 shows the schematic of the lab.

Figure G.3 Florida International University Laboratory Schematic from [31]



This schematic shows mostly the power grid implementation and simulation control. Figure G.4 shows a picture of the lab.

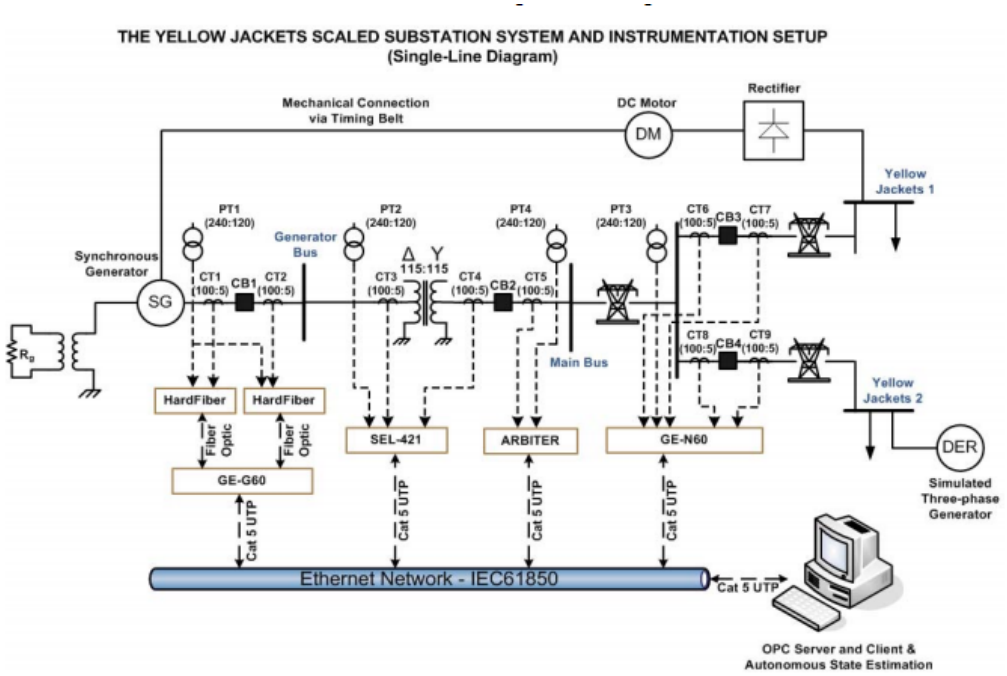
Figure G.4 Florida International University Laboratory picture from [31]



G.2.4 Georgia Institute of Technology

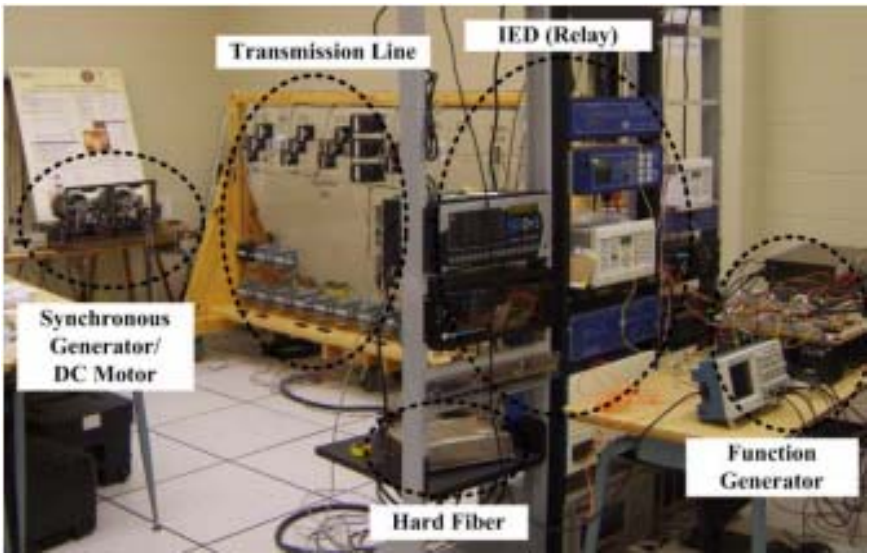
Georgia Institute of Technology is implementing a Smart Grid lab into their currently existing power grid lab. They are testing interoperability between different hardware. They have General Electric (GE), Schweitzer Engineering Laboratories (SEL), Beckwith, and Arbiter equipment installed in their lab. Their lab is a 1:1000 scaled model of an actual power grid network. They are also studying distributed generation in this lab [32]. Figures G.4 and G.5 are the schematic drawing of their lab and a picture of the lab setup.

Figure G.5 Georgia Institute of Technology Laboratory Schematic from [32]



The Smart Grid equipment, GE-G60, SEL-421, ARBITER, and GE-N60, can be seen in the middle of Figure G.5. The lab is using IEC61850 over Ethernet for their network communication. In Figure G.6, you can see the SEL equipment in the rack on the right; they are the blue devices.

Figure G.6 Georgia Institute of Technology Laboratory picture from [32]



G.2.5 Texas A&M

Texas A&M has many different power lab setups. The relay test lab focuses on the new Smart Grid effort. This lab tests equipment that is vital to the Smart Grid effort. Texas A&M's professors are teaching their students about the power grid communication [33]. Figure G.7 is a picture of the relay test lab.

Figure G.7 Texas A&M Relay test lab from [33]

They are working on creating a campus-wide Smart Grid. They plan to include electric vehicle charging stations and alternative energy sources. They also plan to make large computer labs that run from DC energy sources to increase efficiency [34].

G.2.6 Washington State University

Washington State University has developed *SmartGridLab*, which is a test bed for research on the Smart Grid protocols and devices. This test bed was designed alongside a power grid network. This test bed can use conventional power or alternative energy power sources to run. The test bed has four main parts: an information network, a generation model, a user model, and an intelligent control center.

G.2.7 Mississippi State University

Mississippi State University (MSU) has developed a Real Time Test Bed for Power System Operation, Control, and Cyber Security. MSU has GE and SEL equipment in their lab. LABVIEW is used to gather the data from the test bed and displays the results [35]. Figure G.8 is a diagram of the architecture of the test bed.

Figure G.8 Mississippi State University Test Bed Diagram from [35]

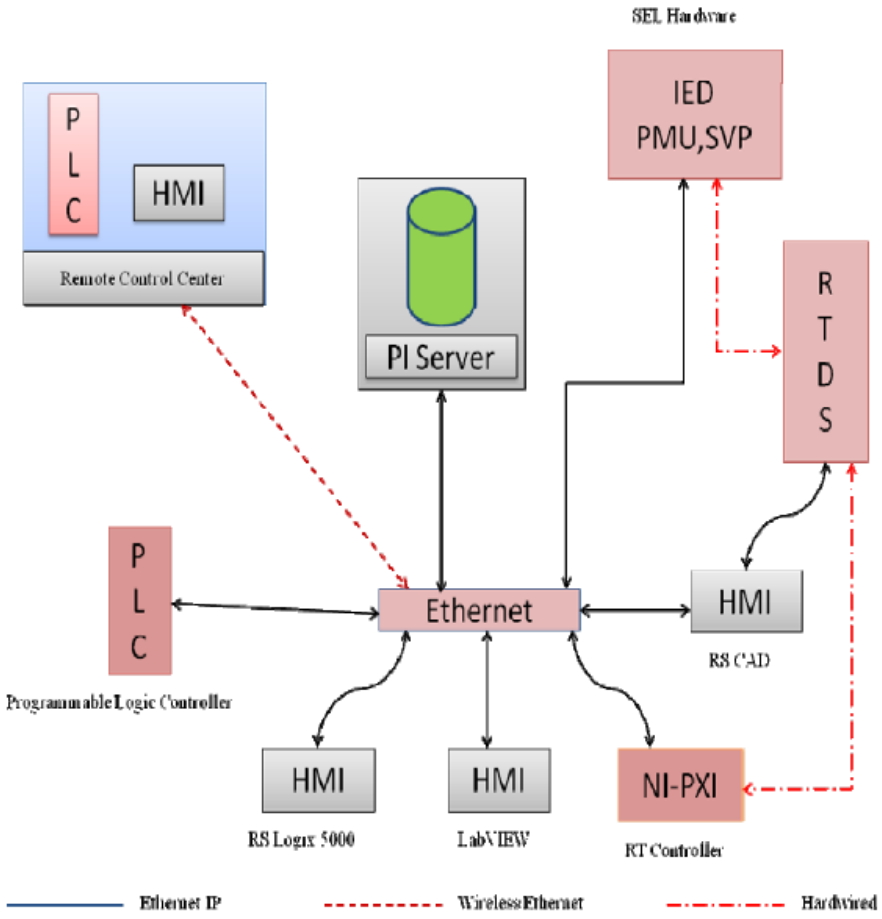


Figure G.8 shows SEL equipment being used with LABVIEW being used for the Human Machine Interface (HMI). This network is able to gather data in real-time [35]. The main professor previously working on this at MSU has moved to Washington State University [36].

G.3 Lab Setup

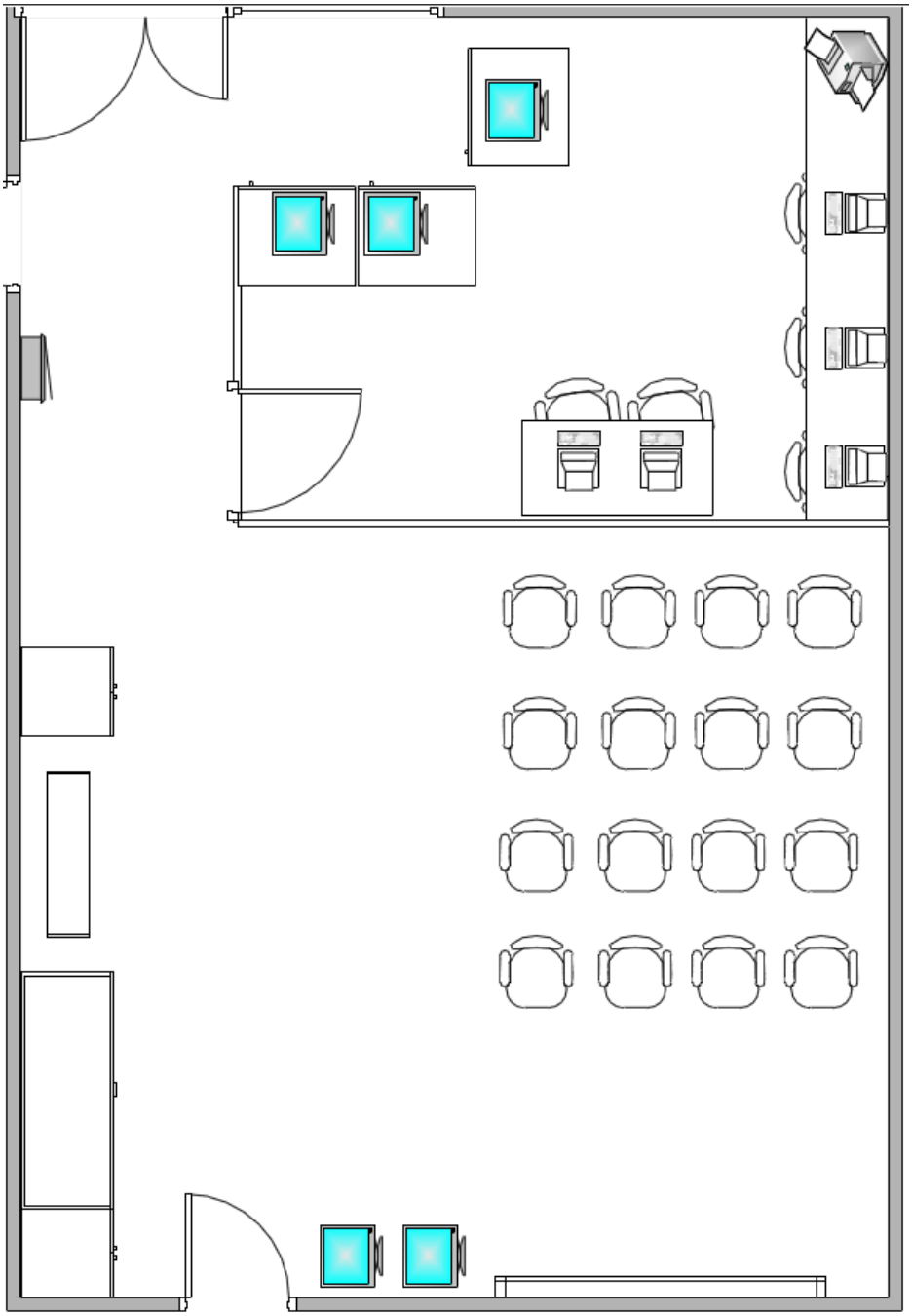
The proposed lab setup is based off the Burns and McDonnell lab. Some of the other related labs have some influence. The follow sections describe different parts of the lab.

G.3.1 Room Size and Setup

The lab will be located inside the ECE department on the second floor of the engineering building on the K-State campus. The room allocated is approximately 620 sq feet. The room has a large window on one side of it. This will allow prospective students and industry alumni to

tour the lab without having to enter the room. This can help with safety issues and security of the equipment. Below is a floor plan of the layout of the room.

Figure G.9 Floor Plan of Lab



The bottom right of the diagram shows a classroom portion that can be used for small classes. The storage area at the bottom left will be utilized to help keep the lab clean and safe. The server racks will be placed so the front side will be viewable from the window into the room. A cubicle-style panel will separate the classroom section from the work area behind the racks. The work area will be filled with wires and tools. This will increase the safety of the students in the lab. Workstations, on the top right of the diagram, are within the work area to allow research students to perform work in the lab.

G.3.2 Initial Lab Equipment

The funding for the lab is going to arrive at different times. The initial list of equipment is mostly from donations and discounted rates from companies. This plan will give the lab a chance to grow in the future when more donations are received. The proposed equipment is listed in the table below.

Table 6.1 Proposed Initial Lab Equipment

Cisco	805	Serial Router
Cisco	2960	Router
Cisco	5520	Edge Router
Cisco	CGH 100	Home Energy Controller
Cisco	CGR 2010	Connected Grid Router
Cisco	CGS 2520	Connected Grid Switch
Cisco		Building Mediator
Cisco		Building Mediator Manager
Cisco		R Series Racks
Cisco	3750	Switch
SEL	279	Reclosing Relay
SEL	351	Breaker Failure and Reclosing
SEL	421	Synchrophasor Measurement and Distance Relay in Conjunction with UPLC
SEL	1102	HMI Computer Data Concentrator
SEL	3351	HMI/61850 Data Converter

SEL	311L	Line Current Differential Protection
SEL	351S	Breaker Failure and Reclosing
SEL	487B	Bus Differential
SEL	321	Distance Relay

This equipment would allow students to start learning about the Smart Grid. The networking equipment included will allow students to start running simulations in the lab. The hope is to add more equipment later.

G.3.3 Future Lab Equipment

The lab will be expanded in the future. The equipment that is recommended to be added to the lab when the funding is available is listed in the table below. Additional equipment may be desired as the companies produce new models. The variety of different brands is helpful when teaching students. The students will have more career opportunities if they have more exposures to the different brands.

Table 6.2 Proposed Future Lab Equipment

ABB	2000R	Distribution Protection Unit
ABB	2000R	Transformer Protection Unit
Adtran	Netvanta 1224STR	Ethernet Switch
Alcatel-Lucent	7705	Alcatel-Lucent MPLS Router
Basler	BE1-951	Breaker Failure Relay
Check Point	EDGE Industrial	Firewall
Electro Ind.	Nexus 1250	Line Metering
Fujitsu	4100ES	SONET Transport
Garrettcom	DX800	Firewall
GarrettCom	Terminal Servers	Used for Transferring Serial Data Sources to Ethernet
GE	B30	Backup Bus differential

GE	Brick	Breaker 61850 Process Bus Module
GE	C30	Breaker Control, Breaker Failure and Reclosing
GE	D20 RTU	Remote Control and Monitoring of Substation Devices
GE	D60	Backup Distance Relaying
GE	JungleMUX	SONET Multiplexer
GE	N60	Synchrophasor Measurement and Protection
GE	T60	Transformer Management Relay
ION	7650	Smart Meter with IEC 61850 Software
ION	8600A	Smart Meter with PQ Software
MOXA	IKS-6726	Ethernet Switch
Netguardian	832A	Alarm Remote
Novatech	Orion LX	Data Concentrator
Pulsar	UPLC	Universal Power Line Carrier, Transmitter and Receiver
Ruggedcom	RSG2100	Ethernet Switch
Satec	PM172E	Metering
SEL	451	Synchrophasor Measurement and Protection
SEL	734	Line Metering
SEL	2407	IRIG-B Satellite Clock
SEL	311L	Line Current Differential Protection
SEL	351S	Breaker Failure and Reclosing
SEL	2032	Communication Processor

The equipment in the list is used in the utility industry. The lab may not be able to have all the equipment on the list due to costs. However, the more equipment the lab has the more beneficial it will be.