Simulation of the Effect of False Data Injection Attacks on SCADA Using Offline EMT Simulation

A Thesis

Presented in Partial Fulfilment of the Requirements for the

Degree of Master of Science

with a

Major in Computer Engineering

in the

College of Graduate Studies

University of Idaho

by

Kaushik Lingaraju

Major Professor: Brian K. Johnson, Ph.D., P.E.

Committee Members: Yacine Chakhchoukh, Ph.D.; Hangtian Lei, Ph.D.

Department Administrator: Joseph D. Law, Ph.D., P.E.

August 2020

Authorization to Submit Thesis

This thesis of Kaushik Lingaraju, submitted for the degree of Master of Science with a Major in Computer Engineering and titled “Simulation of the Effect of False Data Injection Attacks on SCADA Using Offline EMT Simulation,” has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor ________________________________ Date ______________
Brian K. Johnson, Ph.D.

Committee
Members ________________________________ Date ______________
Yacine Chakhchoukh, Ph.D.

________________________________ Date ______________
Hangtian Lei, Ph.D.

Department
Administrator ________________________________ Date ______________
Joseph D. Law, Ph.D.

Abstract

Transient stability simulation is a critical task for validating dynamic models of the power grid. However, transient stability programs do not model the behavior of the supervisory control and data acquisition (SCADA) measurements. We propose an off-line method for performing dynamic power system simulations in an electromagnetic transients (EMT) program with a model of the SCADA systems to allow preliminary study of the grid in the presence of cyber-attacks. Simulations are executed in PowerWorld and PSCAD/EMTDC to first validate the EMTDC model and then use EMTDC to study the impact on the grid of cyber-attacks. Studies are performed on a version of the IEEE 14-bus system modified to mimic modern power system operation. To get effective measurements for state estimation, SCADA polling is reproduced in the EMT simulation at a controlled sampling frequency. The results of a case with a tripped line and case with injection of false data caused by cyber-attacks are presented and analyzed. The approach can be used for preliminary studies prior to use an hardware-in-the-loop simulation studies as well as for classroom study of SCADA and industrial control systems. This thesis describes modeling and validation efforts related to implementing a real-time hardware-in-the-loop model of the IEEE 14-bus system.

Acknowledgements

I would like to express my deepest appreciation to my advisor Professor Brian K. Johnson for his encouragement, support, guidance, help, patience and valuable suggestions during this research. My appreciation is extended to the committee members, Dr. Yacine Chakhchoukh, Dr. Hangtian Lei for their valuable time and effort in reviewing this thesis. I am also thankful to my fellow students, faculty and staff of the ECE department who have been part of my Master's Degree completion. Last but not the least, I would like to thank my family and friends, for their unwavering belief in me throughout my personal and academic life. I would not be able to attain this position in my studies if not for their motivation and support.

Dedication

I dedicate this work to the soul of my father Lingaraju and my mother Shantha B.K. for all their love, support, prayers, caring and sacrifices for educating and preparing me for my future. This work is also dedicated to my brother Karthik Lingaraju and my other family members Shivaram, Mangamma, Sunanda, Thimmegowda, Srivatsa, Aradhana, who have always loved me unconditionally and whose good examples have taught me to work hard for the things that I aspire to achieve.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMI	Advanced Metering Infrastructures
CPS	Cyber Physical System
CSMF	Continuous System Model Functions
DNP	Distributed Network Protocol
DOE	Department of Energy
DOS	Denial of Service
DSA	Dynamic Security Analysis
DSE	Dynamic State Estimator
EMS	Energy Management System
FDI	False Data Injection
GOOSE	Generic Object Oriented Substation Events
IED	Intelligent Electronic Devices
IT	Information Technology
NERC	North American Electrical Reliability Corporation
NSTB	National SCADA Test Bed
OT	Operational Technology
PMU	Phasor Measurement Unit
RTAC	Real Time Automation Controller
RTDS	Real Time Digital Simulator
RTU	Remote Terminal Unit

SCADA	Supervisory Control and Data Acquistion
SSE	Static State Estimator
TVM	Timed Vector Measurement

CHAPTER 1

Introduction

A comprehensive analysis of a power system with communication based protection and control can only be carried out by co-simulation of the power system and the data communication network [1].

Until the last decade, research related power systems planning and operation has concentrated on improving system performance with respect to sudden load changes and faults due to equipment failures or localized weather events to improve reliability of operation. Researcher have recently began to study the resilience of power systems to extreme events such as hurricanes, major storms, floods, fires and cyber-attacks. Supervisory control and data acquistion (SCADA) systems have long used communication technologies. Growing use of information technologies (IT) in externally connected utility enterprise networks has led to coupling between the internal operation technology (OT) networks and the IT networks. For example, the connectivity of SCADA systems and enterprise networks improves business visibility and efficiency, but it makes SCADA systems more vulnerable to cyber-attacks. According to the 2003-2006 data from Eric Byres, 49% of cyber-attacks at industrial control systems are launched via connected enterprise networks [2]. One highly publicized example is Stuxnet, which attacked an industrial control system by infecting those organization networks that interact with the target [3].

In 2006, the US Department of Energy (DOE) published “Roadmap to secure control systems in the energy sector” (updated in 2011) [2]. Much effort has been made to secure power facilities around the world. The DOE National SCADA Test Bed (NSTB) Program, established in 2003, supports industry and government efforts to enhance cyber security of control systems in the energy sector. The North American Electrical Reliability Corporation (NERC) standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operations of bulk electric system [2]. The International Electrotechnical Commission Technical Council

57 (IEC TC 57) has advanced the standard communication protocol security in IEC 62351 with stronger encryption and authentication mechanisms [4]. The US DOE has recognized seven properties required for the smart grid to satisfy future needs [5]. These necessities incorporate attack resistance, self-healing, consumer motivation, power quality, generation and storage accommodation, enabling markets, and asset optimization. While innovations such as phasor measurement units (PMUs), wide area measurement systems, substation automation, and advanced metering infrastructures (AMI) will help accomplish these targets, they likewise present an expanded reliance on cyber resources which may be vulnerable to attack [6]. The U.S. Government Accountability Office examinations concerning the grid's cyber infrastructure have scrutinized the sufficiency of the present security posture [7]. The NERC policy makers have examined these results and improved guidelines to uphold baseline cybersecurity endeavors all through the critical elements of the bulk power system. Moreover, recent developments have demonstrated attackers utilizing expanding advanced attacks against industrial control systems while various nations have recognized that cyber-attacks have focused on their critical infrastructures [6].

With the application of additional computing, sensing and control capability into the grid, the power system is transforming into a complex cyber physical system with possibly an improved efficiency in its operation [8]. However, potential cyber vulnerabilities are introduced by the multifunction intelligent devices communicating over multiple channels in system operation [9]. The measurements collected in real-time in the system can be targeted by attackers which could degrade the behavior of the power system, create financial losses, cause damage assets and even cause blackouts.

Measurement and control data is communicated using Supervisory Control and Data Acquisition (SCADA) units via remote terminal units (RTUs) to the control center [10, 11]. Other data is communicated using phasor measurements units (PMUs) [12, 13]. This means that communication technologies are essential for proper monitoring, operation and control of the power grid. The objective of these applications is to maintain system reliability, stability, security and economic operation using advanced control and protection based on fast real-time reliable communication [14]. Application of modern communication technologies in power industry has seen a significant increase. The data being collected in real-time is becoming significant which is very useful for both online control and for conducting detailed off-line simulation studies. The use of real-time simulation is gradually becoming an indispensable process before the introduction of new technologies to control power and voltage in power systems. With the reduced security margins due to the stress of increased intermittent generation from renewables and the competitive electricity markets, there is an increased need for dynamic security analysis (DSA) which can be performed by conducting a large number of simulations. One important tool of DSA is the transient stability analysis. The authors in [15] studied the impact of cyber-attacks targetting the controls of voltage support devices such as SVC and STATCOM. They showed the impact of attacks on voltage and angle stability. Reference [16] presents a test system developed with off-line simulation in PSCAD/EMTDC providing a playback simulator for relay testing. The authors in [17] develop an interface for an EMT program in order to permit multi-agent simulation of controls and protection. The communication component is implemented with PSCAD/EMTDC in a co-simulation set up. The co-simulator can incorporate communication delays and loss of packets and assess their impact on relays and controls of the power grid. The delay caused by cyber-attacks can affect the stability of power systems. The authors of [18] analyze the impact of network delays on transient stability. The transient analysis of cyber-attacks effects is conducted using a real time digital simulator (RTDS). Reference [19] analyzes the impact of cyber-attacks targeting active distribution systems on the transient stability of the overall power system. The authors in [20] analyze the impact of cyber-attacks on distributed transient stability control schemes and develop robust controls to limit the impact of these attacks. A common theme of the references described above is that the operational data impacting the transient stability of the system is vulnerable to cyber-attacks.

Both static state estimation (SSE) and dynamic state estimation (DSE) are vulnerable to cyber-attacks. While SSE is implemented in practice and is an important tool to perform the static security analysis (SSA), the dynamic state estimator will constitute an important monitoring tool in the presence of a large numbers of PMUs enabling an accurate dynamic security analysis while also mitigating some of the cyber vulnerabilities in SSE. When a false data injection (FDI) cyber-attacks corrupts the communicated SCADA or PMU measurements, the SSE and DSE can suffer from a degraded performance. Different authors proposed solutions based on data analytics such as [21] for SSE and [22, 23] for DSE. In [24], the vulnerability of state estimation is quantified in an index. The authors show a decrease in a cyber vulnerability index using a proposed solution against cyber-attacks. The solution applies the combination of remote measured SCADA and timed vector measurements (TVMs) data for state estimation.

The authors in [25] showed the impact of cyber-attacks such as denial of service attacks on communication assisted protection schemes. They proposed solutions against cyber-attacks based on enhancing and securing the communication. Reference [26] presents a modeling approach of power cyber-physical systems based on graphs. The approach considers the interactions between the cyber and physical systems and includes the dynamics of the whole system. A cyber secure optimal frequency regulation method is proposed in by enhancing the security of the communication network and hence the resiliency of the grid against cyber intruders. In order to simulate cyber-attacks and their cascading effects on the dynamics of the power grid, it is necessary to reproduce the real measured data using software tools.

As noted above, cyber-physical test beds are important to analyze methods to detect and mitigate cyber-attacks against OT systems, enhancing cyber-resilience of critical infrastructure without testing the methods on the real system. Test beds are also a valuable tool for university research and education. However, test beds built around hardware-in-the-loop simulation platforms are costly. This thesis explores lower cost options that are able to provide a reasonable approximation of the behavior of detailed test beds to use in senior and graduate level courses with distance education students. The platform can also be used for preliminary research before moving to a more realistic testbed.

1.1 Thesis Contribution and Roadmap

This thesis explores performing dynamic power system simulations in an electromagnetic transients (EMT) program with a model of the SCADA system to allow preliminary study in the presence of cyber-attacks. The primary contributions of this thesis are:

1) Implementing a modified version of the IEEE 14-bus system in PSCAD/EMTDC and validating it against a PowerWorld model.

2) Implement a polling based SCADA model in PSCAD/EMTDC to produce data for a static state estimator.

3) The approach is demonstrated using simulation results from normal and cyber-attack conditions in PSCAD/EMTDC.

4) The approach implemented here can be used for preliminary research studies prior to used closed loop testbeds and in courses exploring power system SCADA and control systems, especially for distance education students.

The rest of the thesis is organized as following. Chapter 2 presents a review of the literature related to cyber and physical attack scenarios along with an overview of SCADA systems. The test environment is introduced in Chapter 3, then the SCADA polling implemented on the IEEE 14-bus system in PSCAD/EMTDC is introduced with controlled sampling frequency in Chapter 4. Chapter 4 also presents an example of a cyber-attack on measurements. Chapter 5 describes efforts to implement DNP communication on a RTDS test bed. Conclusions and a discussion of future work are provided in Chapter 6.

CHAPTER 2

Background

2.1 Combined Cyber and Physical Attacks

Combined cyber-physical attacks, are also called blended attacks or cyber-physical attacks. As the name implies, blended attacks use a cyber-attack to amplify the impact of a physical attack, or a physical attack to increase the harm from a cyber-attack. NIST SP 800-82 Rev. 1, Guide to Industrial Control Systems Security, and ISA 99, Industrial Automation and Control Systems Security, provide additional resources for classifying vulnerabilities associated with cyber-physical attacks [27].

Classification of cyber-physical attacks:

- Physical attacks informed by cyber: The utilization of data accumulated by cyber-means permits an attacker to design and execute an improved or upgraded physical attack. For example, an attacker plots to destroy components inside a substation. However they don't know which substation or components would have the most effect. Collecting and analyzing unprotected data by cyber-means enable them to target a specific substation on a very congested transmission path with heavily loaded lines. This information allows their attack to have more impact.

- Cyber-attacks leveraging naturally occuring physical events or physical attacks: An advesary conducts a cyber-attack to increase the effects of a physical attack by either making the attack impact a larger area or interfering with restoration efforts (in this manner expanding the time span of the attack). Although the expression "adversary" is used, conventional failures could replace the physical attack. For example an adversary could modify protective relay settings and the incorrect settings could sit for months or years before a fault occurs on a transmission line. The tampered settings could permit the failure to cascade so it impacts a more extensive section of the grid.

- Use of a cybersystem to cause physical harm: For example an adversary utilizes a cyber system that controls physical equipment in such a way to cause equipment damage. An, adversary or a reckless operator could endeavor to turn on the natural gas inflow without an ignition source present. As the burner unit loads up with natural gas, the adversary could turn on ignition source, possibly causing a blast.

Cyber-physical attacks can significantly increase the area impacted and outcomes of an attack or increase the duration of the impacts by delaying or interfering with responses. However, good cyber, physical, and operational security can limit these effects. Defensive measures that can be utilized to limit the probability of effective cyber and physical attacks will likewise work to limit the effects of a cyber-physical attack. Security operators need to consider the two sorts of attacks and how they might be utilized together to create systems that are resilient to cyber-physical attacks. The utilization of NISTIR 7628 and other security standards and rules as a part of an organization wide risk management procedure can help reduce the cyber vulnerabilities and limit the effects of cyber-physical attacks [27].

2.2 Concept of SCADA Polling/Polling Behavior

Polling is a process for SCADA to acquire data. The remote terminal unit (RTU) obtains measurement data and waits for a data request. The transmission or distribution voltage, current, real and reactive power and other measurement are interfaced by using this RTU. The RTU responds to a polling request and submits data to the control center. It can also implement control actions based on commands from the operator. The polling can occur at a fixed time period (for example, every couple of seconds, minutes, hours, days, months or years). The polling period is set based on the rate at which data can vary, and more importantly, the rate at which a human operator can make actionable decisions on that data. However, the polling does not need to cover a case where autonomous devices can act without the need of a human operator. For example a protective relay can clear a fault in 50 to 100 ms. There is no need to poll fast enough to get this data to the operator. Depending on the design of the SCADA system, the RTU could submit an unsolicited message indicating a fault has occured, or wait to submit the information in response to a polling request. In most cases, waiting for the next polling cycle has little impact on the response to the fault. SCADA systems are the most widely used systems to provide situational awareness or data that can be used to estimate the state of the system to be estimated [28].

Supervisory Control and Data Acquisition (SCADA) systems are exposed to increased threats from cyber-attacks which threaten our critical infrastructure. SCADA collects measurements of real and reactive power and voltage magnitudes and communicates those to the control center every 30 seconds. The data is used at the energy management system (EMS) in order to monitor the system. The data delivered by the SCADA is noisy due to the communication and sensor measuring errors. The SCADA could also contain a few bad measurements or even large errors due to damaged or failed equipments. To reduce the impact of bad data the state estimators receive far more measurements than the minimum needed to determine the state, as well as executing bad data detection algorithms. A state estimator is executed at regular intervals, i.e. every several seconds to a few minutes. The state estimator uses the grid physical model, and estimates or fits an optimum state to the large amount of collected measurements. This is known as a static state estimation (SSE). SCADA systems are exposed to an increased vulnerability to cyber-attacks such as denial-of-service (DOS) and false data injection (FDI) types of attacks. The SCADA traffic exhibits steady and probable communication patterns because of the use of request-response communication in polling. The purpose of this polling behavior is to get a new sample at every specific time period and the values of the parameters will keep on updating. Each bus or substation parameter measurement is updated at every time step to the control center. Data is updated and copied into a file used as an input to the state estimator program.

CHAPTER 3

Test Environment

3.1 IEEE 14-Bus System

The IEEE 14-bus system [29] has 14 buses, 5 of which have generators connected, all at 138kV. Eleven of the buses have loads connected, with approximately 300 MW of total load. The generator at Bus 1 supplies 232 MW in base case, while the generator at Bus 2 supplies approximately 38 MW. The other generators supply only reactive power, acting as synchronous condensers. In the base case of the IEEE 14-bus system, there are no line current/power flow limits or generator output limits.

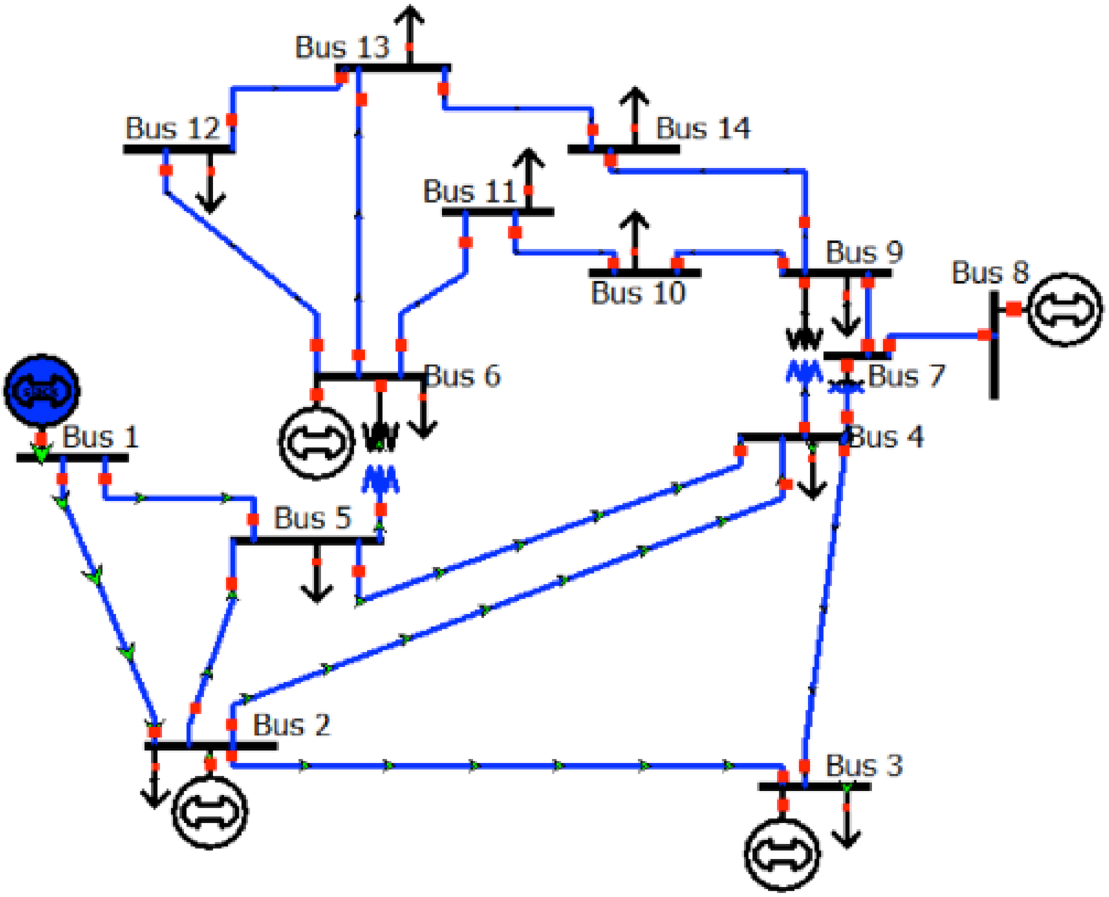


Figure 3.1: IEEE 14-Bus System Implemented in PowerWorld

The PowerWorld model of IEEE 14-bus system was modified as part of a research project to better align with a modern power system for conducting resilience research. This thesis will implement the modified system in PSCAD/EMTDC and validate the resulting model against the PowerWorld model. This chapter will analyze a set of test cases in PowerWorld to use as benchmarks for the testing the PSCAD/EMTDC model.

3.2 Modified Version of IEEE 14-Bus System

The default base case operating scenario isn't well aligned up with modern power system operation, so along these lines, the IEEE 14-bus system was modified as appears in Figure 3.2 to line up with current practice. The generator setpoints were modified to decrease the power supplied by the generator at Bus 1 and to have the generators at Buses 3, 6 and 8 supply part of the load. In addition the plants at Buses 2, 3 and 6 were modified to each have multiple generator units that are each loaded equally. This modification allows the system to model generator shedding through operator actions or remedial action scheme response in a more realistic fashion. Tables 3.1 through 3.3 show the comparison between the PowerWorld and PSCAD/EMTDC results of particular components in steady-state. All of the generators in Figure 3.2 are initially modeled in PSCAD/EMTDC as ideal sources and lines are modeled with constant impedance. The voltage source amplitudes and angles are determined based on the PowerWorld results.

The output power from the generators, power consumed by loads, power flows in transmission lines in modified IEEE 14-bus system in PSCAD/EMTDC are similar to the actual base case results in PowerWorld. The voltages are almost the same as well. The same topology, line parameters and loads were considered. Figure 3.3 and Figure 3.4 show the real power injected from generators and flowing in the transmission lines obtained with PowerWorld power flow solution and PSCAD/EMTDC. Both figures show roughly similar power supplied by generators and flowing in transmission lines.

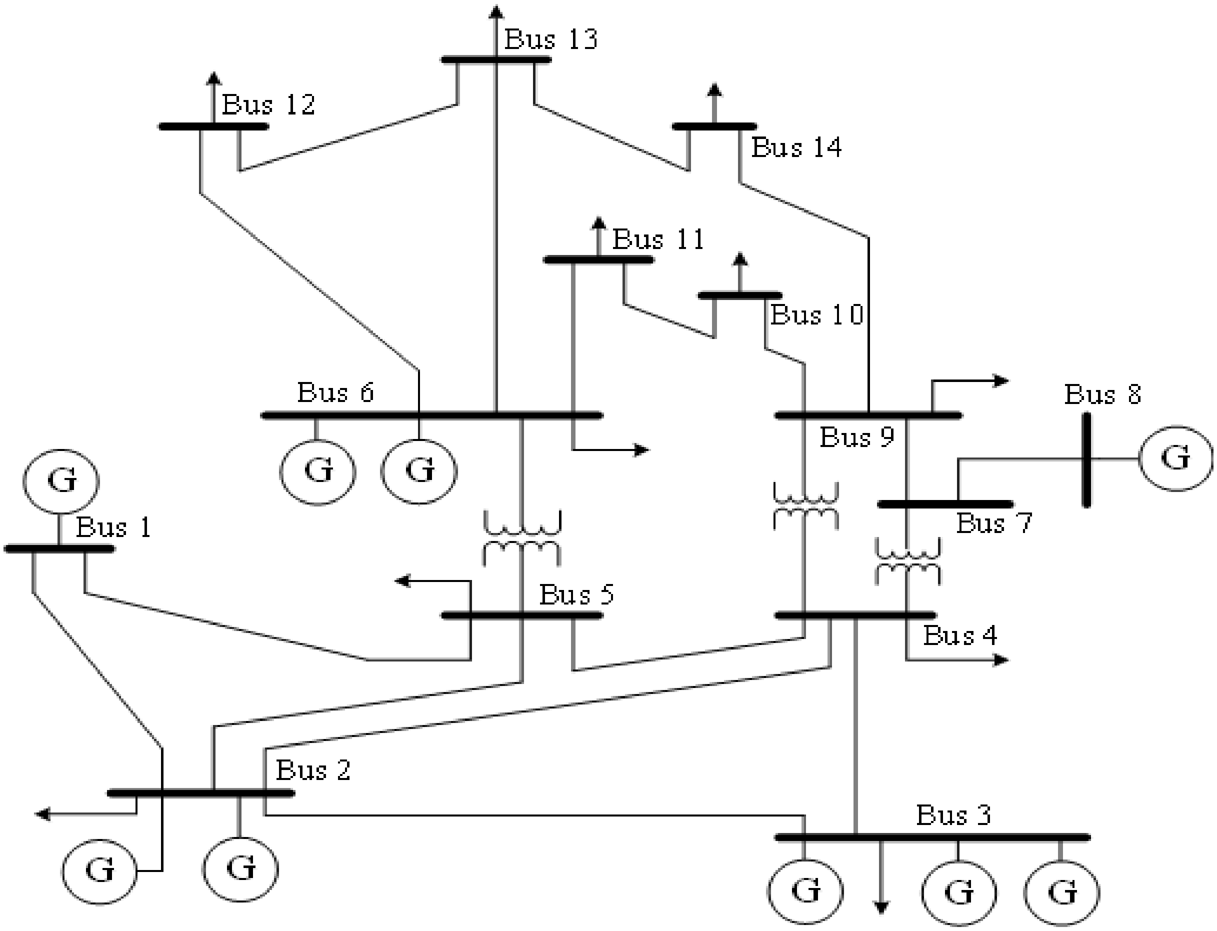
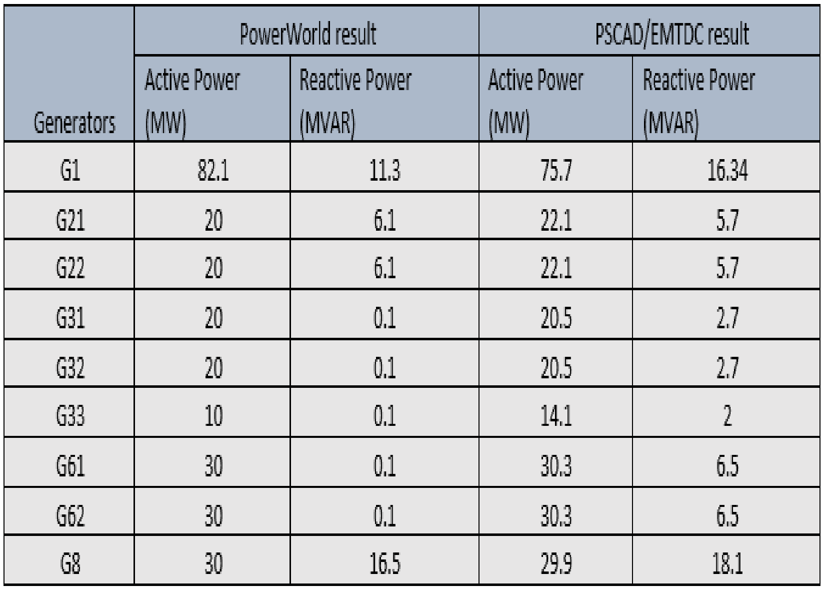


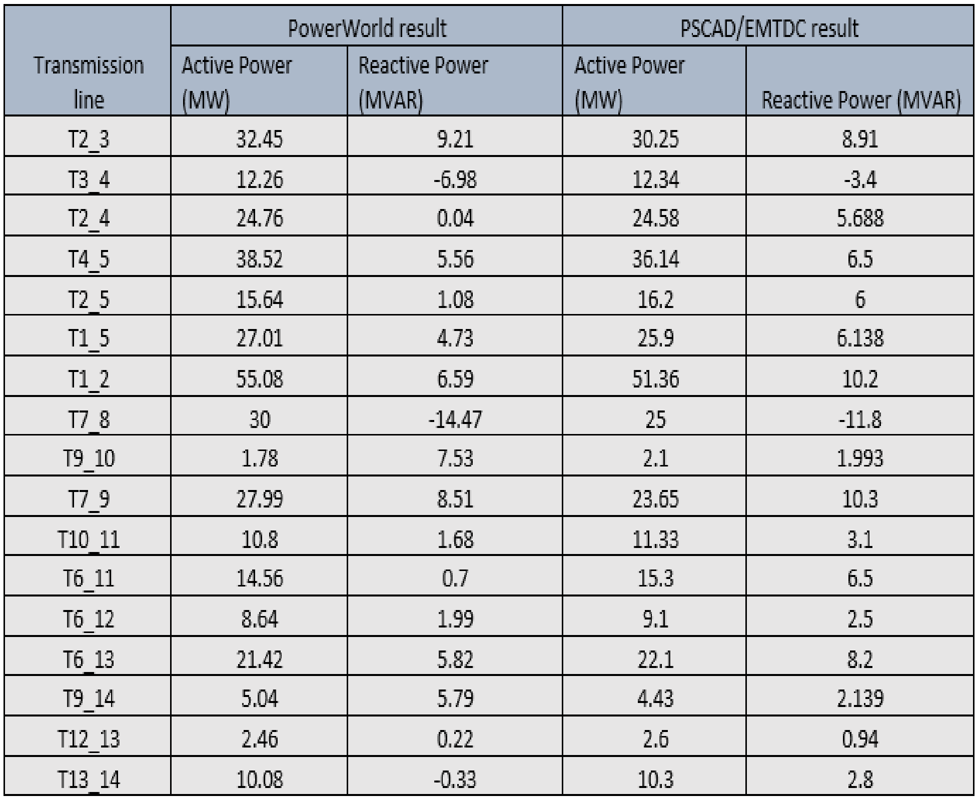
Figure 3.2: Modified Version of IEEE 14-Bus System

Table 3.1: Generator Power Flow for the Modified IEEE 14-Bus System at Steady-State



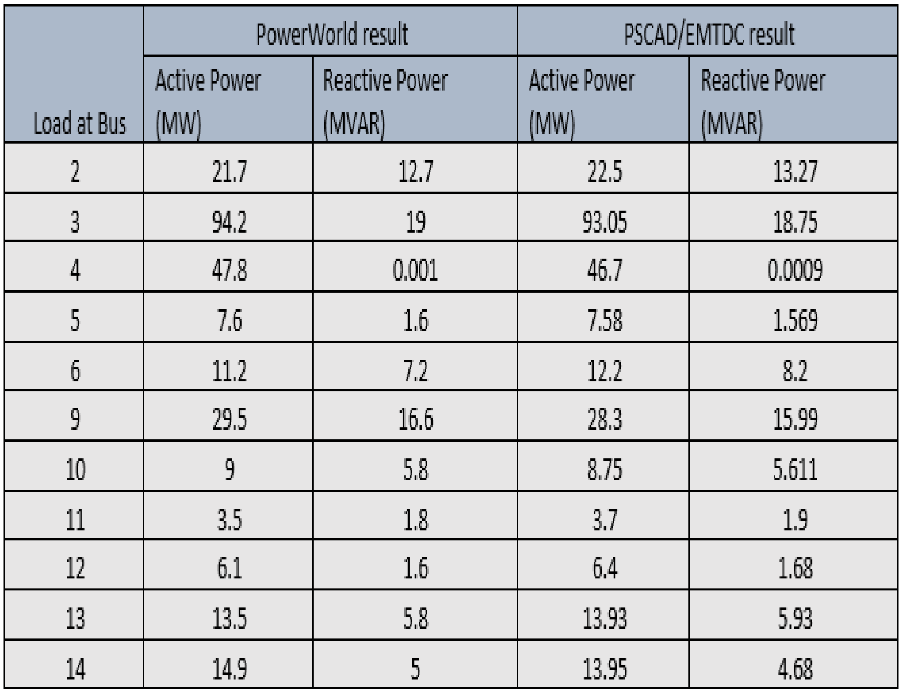
Generators	PowerWorld result		PSCAD/EMTDC result	
	Active Power (MW)	Reactive Power (MVAR)	Active Power (MW)	Reactive Power (MVAR)
G1	82.1	11.3	75.7	16.34
G21	20	6.1	22.1	5.7
G22	20	6.1	22.1	5.7
G31	20	0.1	20.5	2.7
G32	20	0.1	20.5	2.7
G33	10	0.1	14.1	2
G61	30	0.1	30.3	6.5
G62	30	0.1	30.3	6.5
G8	30	16.5	29.9	18.1

Table 3.2: Transmission Line Power Flow for the Modified IEEE 14-Bus System at Steady-State



Transmission line	PowerWorld result		PSCAD/EMTDC result	
	Active Power (MW)	Reactive Power (MVAR)	Active Power (MW)	Reactive Power (MVAR)
T2_3	32.45	9.21	30.25	8.91
T3_4	12.26	-6.98	12.34	-3.4
T2_4	24.76	0.04	24.58	5.688
T4_5	38.52	5.56	36.14	6.5
T2_5	15.64	1.08	16.2	6
T1_5	27.01	4.73	25.9	6.138
T1_2	55.08	6.59	51.36	10.2
T7_8	30	-14.47	25	-11.8
T9_10	1.78	7.53	2.1	1.993
T7_9	27.99	8.51	23.65	10.3
T10_11	10.8	1.68	11.33	3.1
T6_11	14.56	0.7	15.3	6.5
T6_12	8.64	1.99	9.1	2.5
T6_13	21.42	5.82	22.1	8.2
T9_14	5.04	5.79	4.43	2.139
T12_13	2.46	0.22	2.6	0.94
T13_14	10.08	-0.33	10.3	2.8

Table 3.3: Power Drawn by Loads for the Modified IEEE 14-Bus System at Steady-State



Load at Bus	PowerWorld result		PSCAD/EMTDC result	
	Active Power (MW)	Reactive Power (MVAR)	Active Power (MW)	Reactive Power (MVAR)
2	21.7	12.7	22.5	13.27
3	94.2	19	93.05	18.75
4	47.8	0.001	46.7	0.0009
5	7.6	1.6	7.58	1.569
6	11.2	7.2	12.2	8.2
9	29.5	16.6	28.3	15.99
10	9	5.8	8.75	5.611
11	3.5	1.8	3.7	1.9
12	6.1	1.6	6.4	1.68
13	13.5	5.8	13.93	5.93
14	14.9	5	13.95	4.68

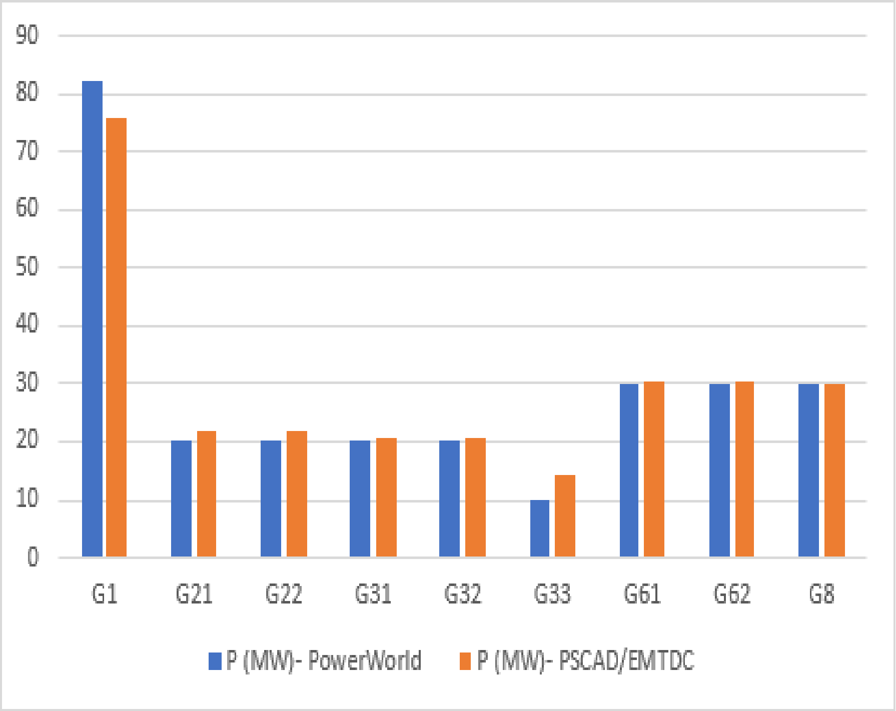


Figure 3.3: Comparison of Generator Active Power Between PowerWorld and PSCAD/EMTDC for the Modified IEEE 14-Bus System

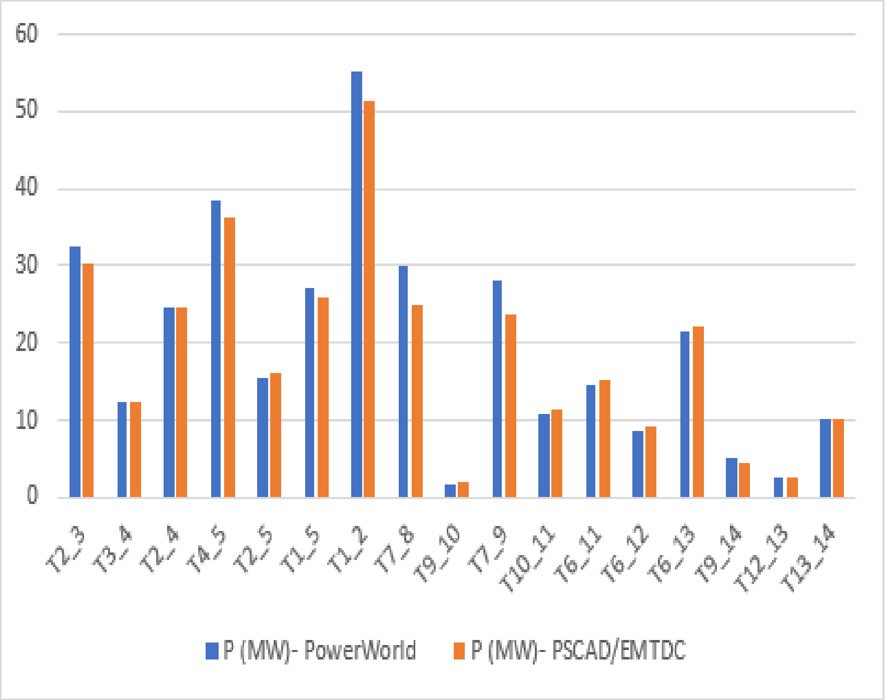


Figure 3.4: Comparison of Transmission Line Active Power Flows Between PowerWorld and PSCAD/EMTDC for the Modified IEEE 14-Bus System

3.3 Transient Study to Determine Relay and Hardware Metering Locations

Transient studies are performed to evaluate system response to various fault events. The contingencies are analyzed to determine the buses that most impact system performance to use as basis for choosing locations for installing protective relays and automation controllers in the real-time digital simulation model of the 14-bus system. All of the generators are modeling using detailed machine modes including governers and exciters in PSCAD/EMTDC includes detailed generator model (machine model).

3.3.1 Example Cases

Case 1

This case simulates a scenario of where one of the generators at Bus 6 is disconnected due to a false command issued through a cyber-attack. The generator disconnected is shown in a partial system one-line diagram in Figure 3.5.

When Generator 1 at Bus 6 is suddenly disconnected from the system due to a cyber-attack, the voltage magnitude and angles at Bus 6 and other buses will be affected. The governer droop controllers for the remaining generators will change their power setpoints in response to the small change in frequency. Similarly the exciters at the generators vary their reactive power output in response to the event to regulate their terminal voltage magnitudes.

Sequence of Events:

- At t = 1.0 seconds, Generator 1 at Bus 6 suddenly disconnects from the system.
- The voltage magnitudes and angles at Bus 6 will be affected (as shown in Figures 3.6 and 3.7). Both the angle and voltage decrease slightly due to the loss in generator.
- The output power for Generator 1 at Bus 6 is shown in Figure 3.8 and the output from Generator 2 at Bus 6 is shown in Figure 3.9.

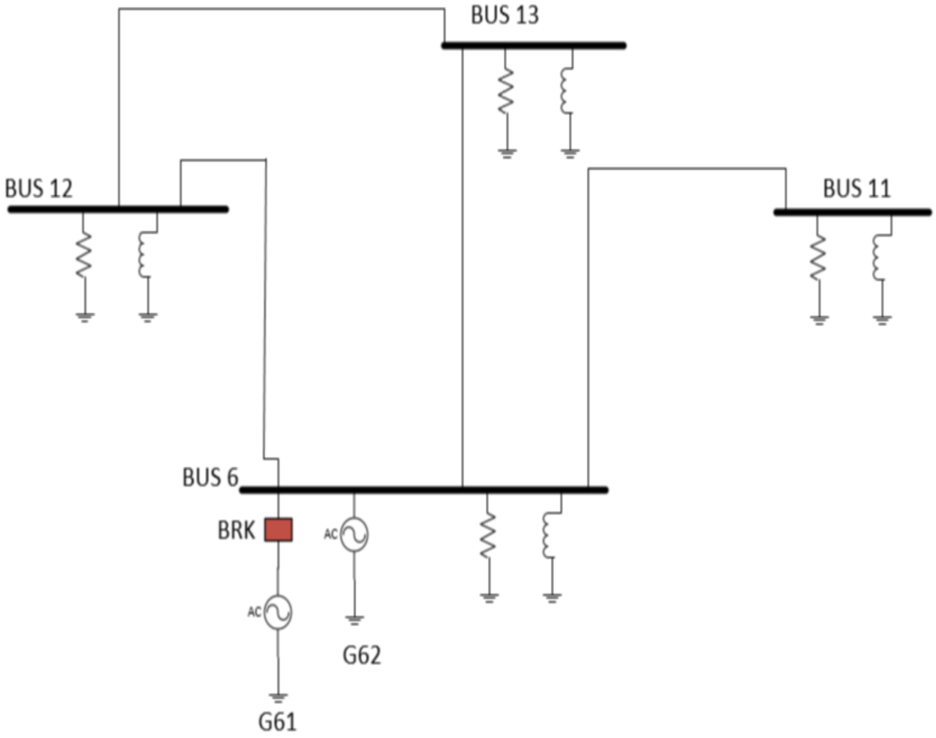


Figure 3.5: Generator 1 at bus 6 is Disconnected by Opening the Breaker

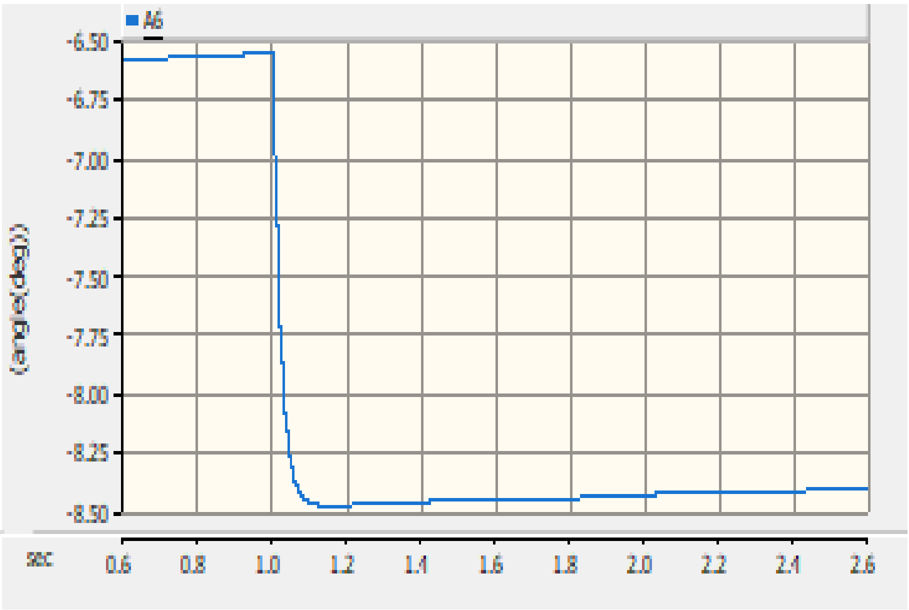


Figure 3.6: Change in Bus 6 Voltage Phase Angle in Response to Dropping Generator 1, X-axis: Time (seconds) and Y-axis: Angle in degrees

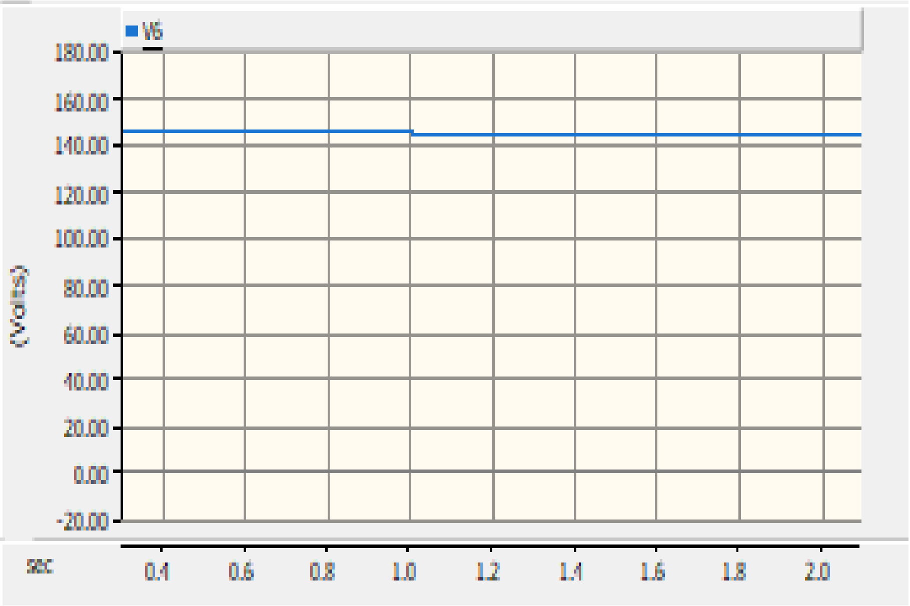


Figure 3.7: Change in Bus 6 Voltage Magnitude in Response to Dropping Generator 1, X-axis: Time (seconds) and Y-axis: Voltage Magnitude (volts)

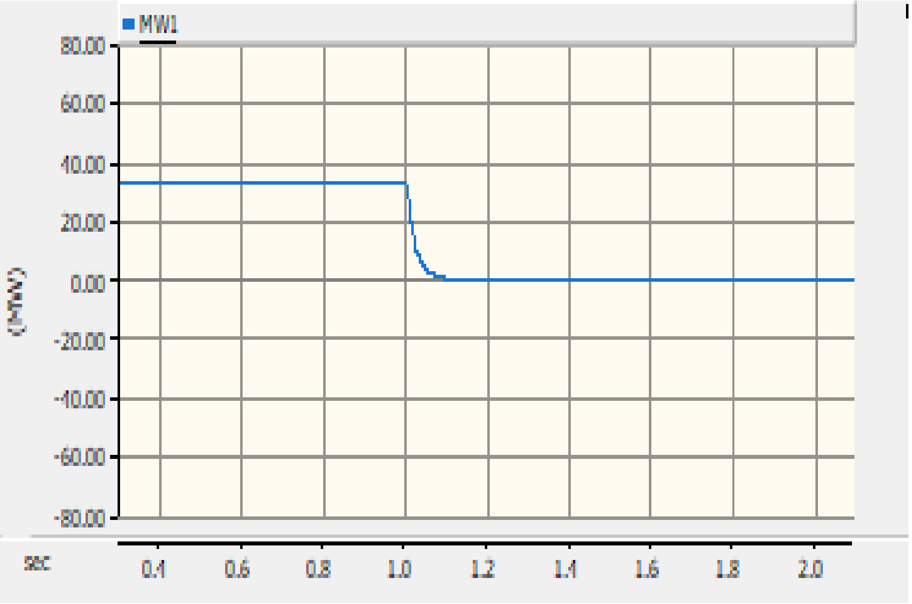


Figure 3.8: Change in Generator 1 Output Power at Bus 6, X-axis: Time (seconds) and Y-axis: Output Power (MW)

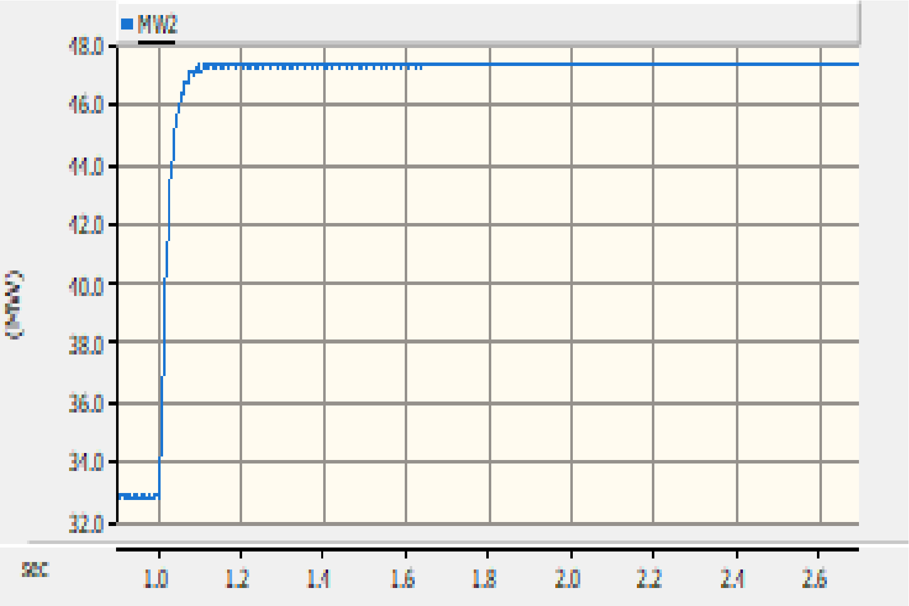


Figure 3.9: Change in Generator 2 Output Power at Bus 6 in Response to Drop of Generator 1, X-axis: Time (seconds) and Y-axis: Output Power (MW)

Case 2

In this scenario a three-phase fault is applied 50% of the way from Bus 1 to Bus 2.

Sequence of Events:

- At t = 0.5 seconds a three-phase fault is applied at 50% of line 1-2.
- At t = 2.0 seconds the circuit breaker at Bus 1 (BKR1) opens and the circuit breaker at Bus 2 (BKR2) fails to open.

The voltage magnitude and angle at Bus 1 show the collapse of the voltage due to the fault, but the magnitude recover after the fault clears. The bus voltage phase angle recovers to a different angle. As one would expect, since the breaker at the Bus 2 end of the line fails to clear, the voltage magnitude and angle do not recover.

Figures 3.11 and 3.12 show the response of the voltage angle and magnitude at Bus 1 respectively. Note the oscillation in the phase angle during the fault and after the breaker clears. Figures 3.13 and 3.14 show the response of the voltage angle and magnitude at Bus 2 respectively. Note the oscillation in the phase angle during the fault and the change when the breaker at Bus 1 clears. Figures 3.15 through 3.18 show the response of the power injected by the generators at Bus 1 and generator 1 at Bus 2, respectively.

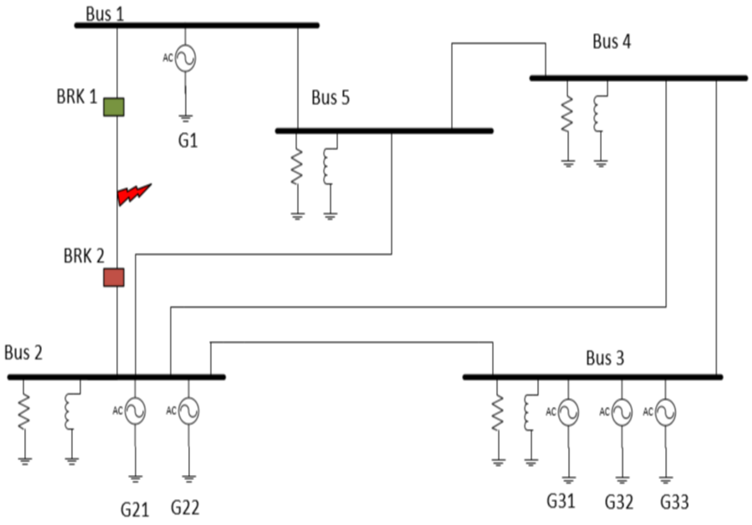


Figure 3.10: A Three Phase Fault is Applied at the Midpoint of the Line Between Bus 1 and Bus 2. BRK 1 Trips and BRK 2 Fails to Trip.

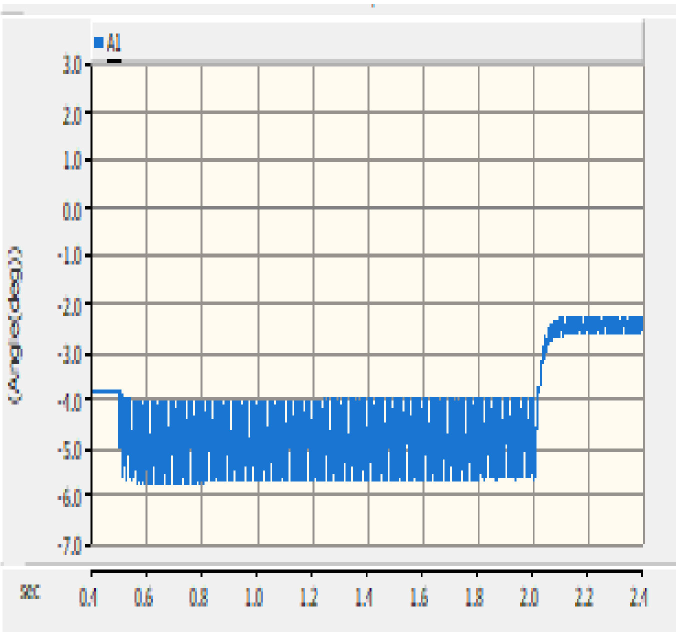


Figure 3.11: Change in Bus 1 Voltage Phase Angle in Response to 3-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Angle in degrees

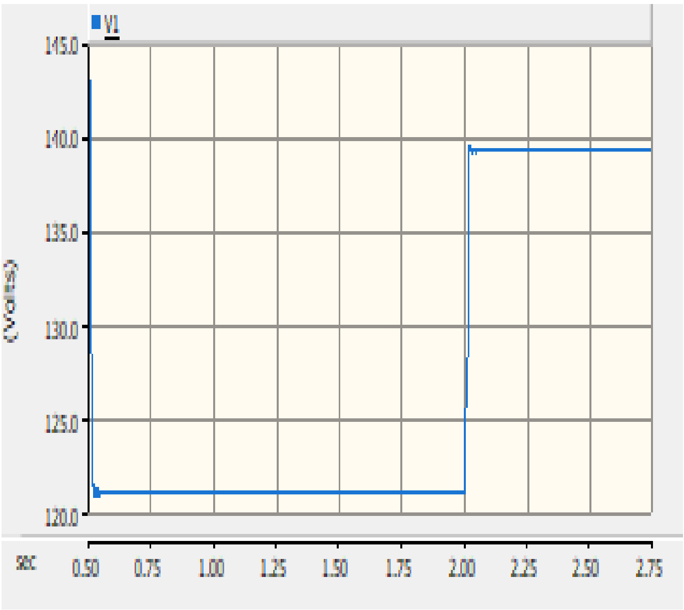


Figure 3.12: Change in Bus 1 Voltage Magnitude in Response to 3-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Voltage Magnitude (volts)

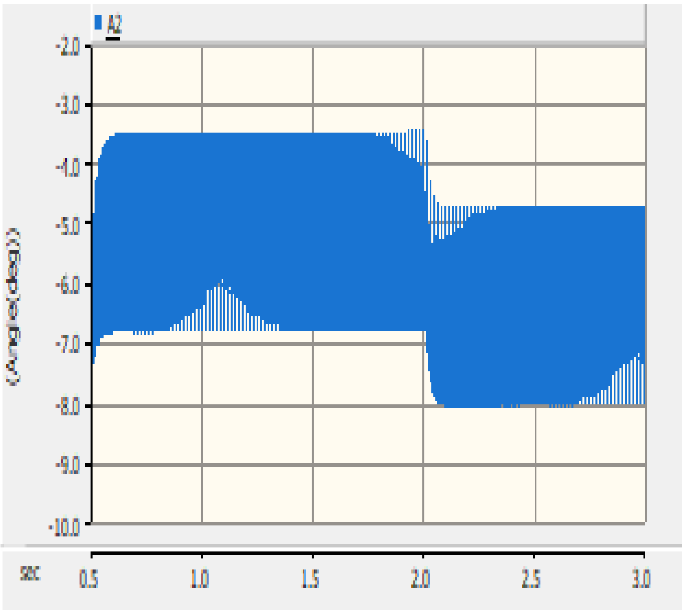


Figure 3.13: Change in Voltage Phase Angle at Bus 2 When Breaker Fails to Clear Following a Three-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Angle in degrees

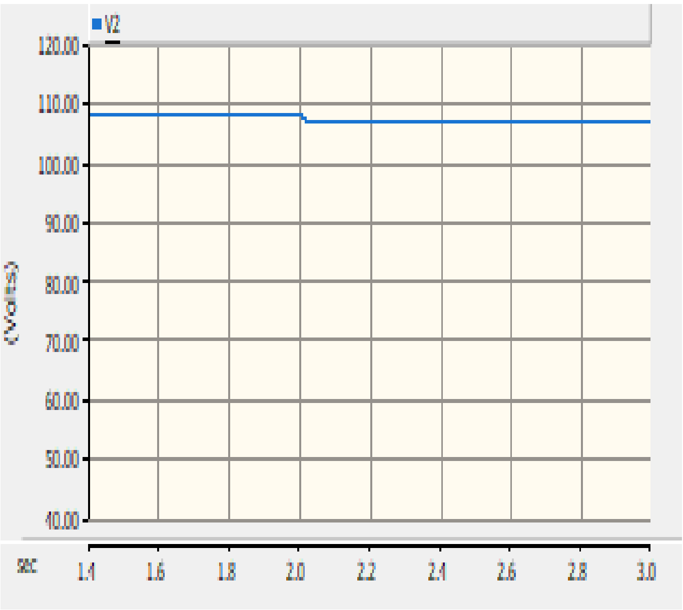


Figure 3.14: Change in Voltage Magnitude at Bus 2 Due to Three-Phase Fault on Line 1-2 Where the Breaker at Bus 2 does not Open, X-axis: Time (seconds) and Y-axis: Voltage Magnitude (volts)

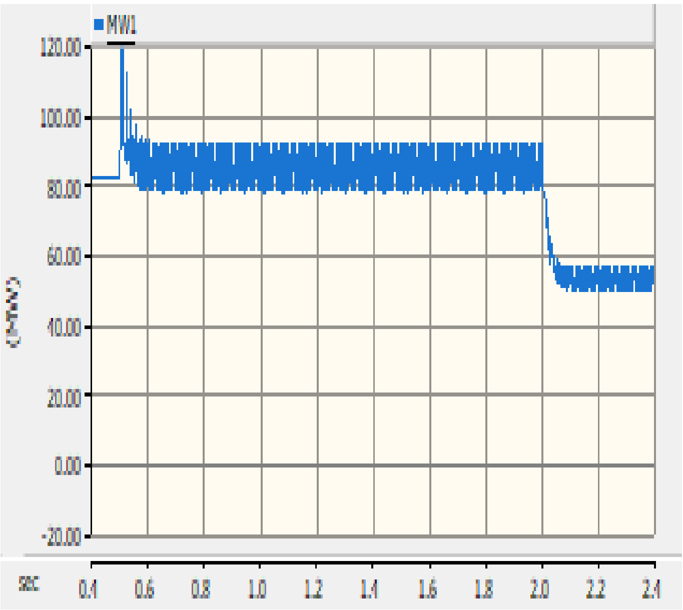


Figure 3.15: Change in Generator 1 Output Power at Bus 1 Due to 3-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Output Power (MW)

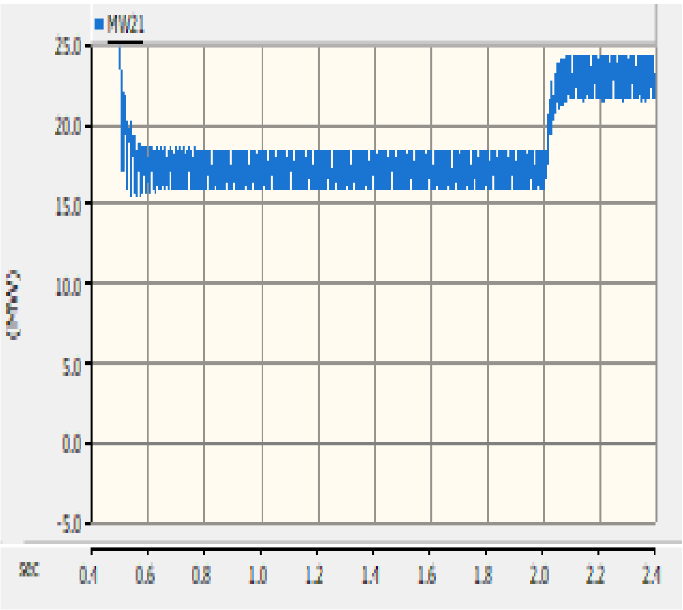


Figure 3.16: Change in Generator 1 Output Power at Bus 2 Due to 3-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Output Power (MW)

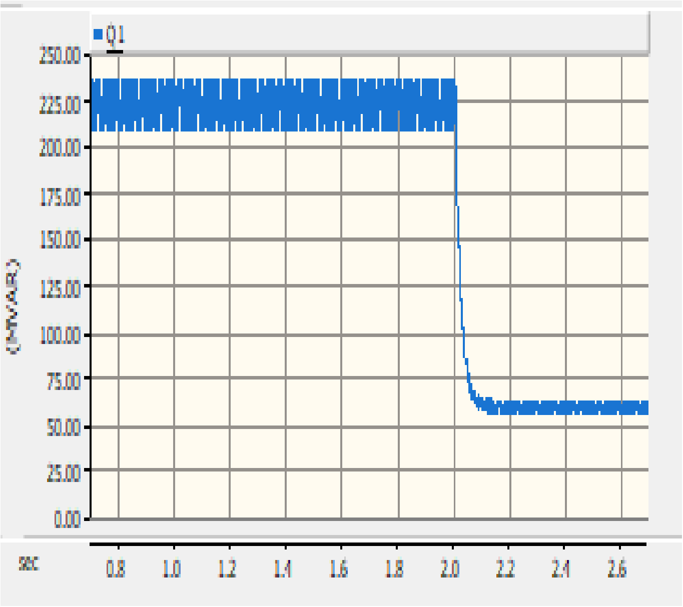


Figure 3.17: Change in Generator 1 Output Power at Bus 1 Due to 3-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Output Power (MVAR)

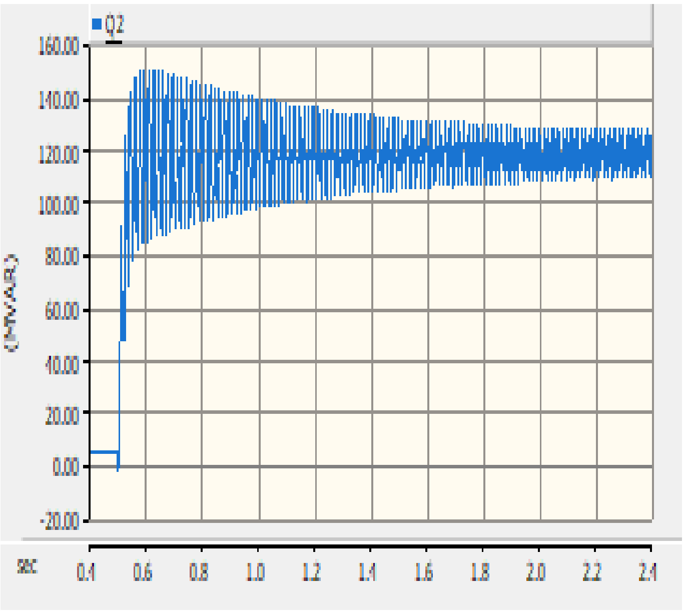


Figure 3.18: Change in Generator 1 Output Power at Bus 2 Due to 3-Phase Fault on Line 1-2, X-axis: Time (seconds) and Y-axis: Output Power (MVAR)

Case 3

This case starts out the same as Case 2, with a three phase fault at 50% of the line from Bus 1 to Bus 2. Again, the Bus 1 end breaker clears and the Bus 2 end fails to open. One second after BRK2 fails to trip the breaker failure relay clears the remaining breakers on the bus.

Events:

- At t = 0.5 seconds a three-phase fault is applied at 50% of line 1-2.
- At t = 1.0 seconds the circuit breaker at Bus 1 (BRK1) opens and the circuit breaker at Bus 2 (BRK 2) fails to open.
- At t = 2.0 seconds the breaker failure relay trips all of the other breakers on lines and components connected to Bus 2.

Figure 3.20 and Figure 3.21 show the response of the voltage and magnitude at Bus 1 due to the fault and subsequent clearing of the BRK1 and the breakers at Bus 2.

The components at Bus 2 are all impacted by the breaker failure (BRK 2) and the breaker failure relay tripping all of the remaining breakers at the bus. In this case we lose that bus.

Figures 3.22 and 3.23 show the response of the voltage angle and magnitude at Bus 2. The voltage magnitude at Bus 2 goes to zero when the breaker failure relay clears the bus. Figures 3.24 and 3.27 show the power output from generators 1 and 2. The power output (MW) of generator 2 goes to zero when the breakers clear the bus. The power output (MW) at generator 1 also decreases after the breakers clear.

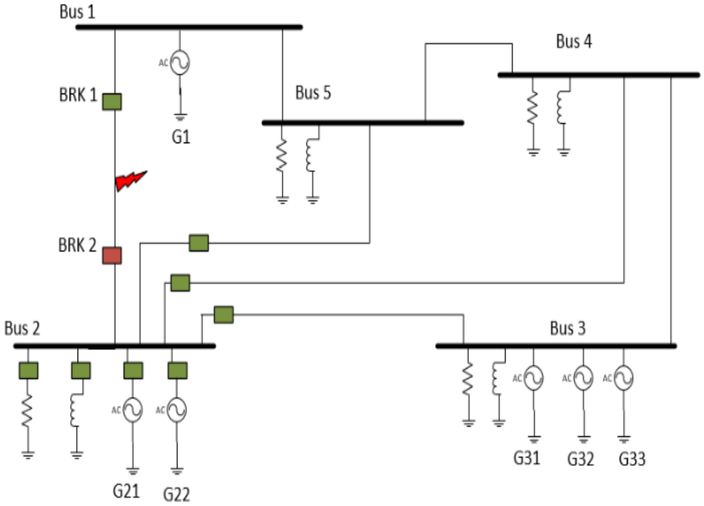


Figure 3.19: A Three Phase Fault is Applied at the Midpoint of the Line Between Bus 1 and Bus 2. BRK 1 Trips and BRK 2 Fails to Trip. Remaining Breakers at Bus 2 Will Open

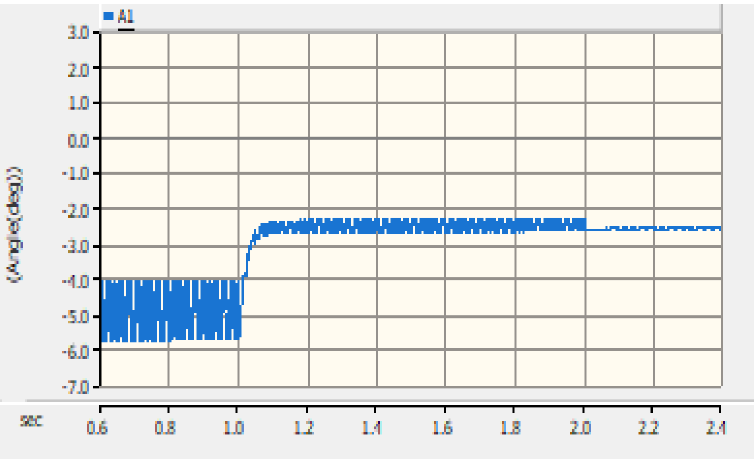


Figure 3.20: Change in Voltage Phase Angle at Bus 1 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Angle in degrees

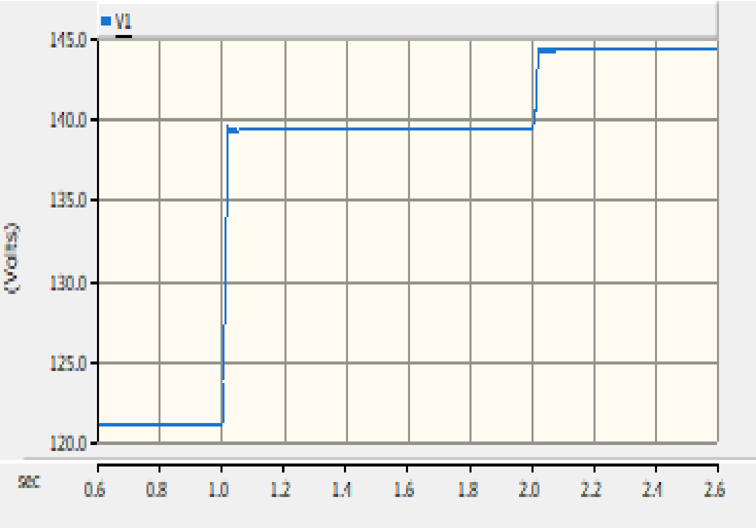


Figure 3.21: Change in Voltage Magnitude at Bus 1 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Voltage Magnitude (volts)

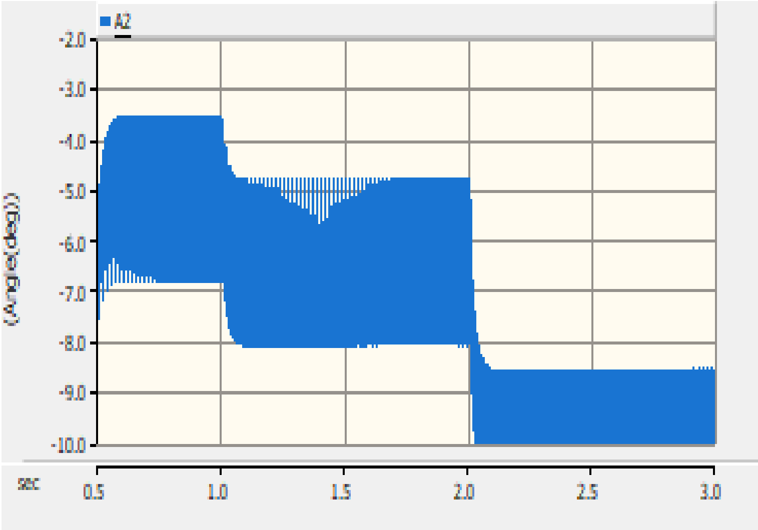


Figure 3.22: Change in Voltage Phase Angle at Bus 2 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Voltage Magnitude (volts)

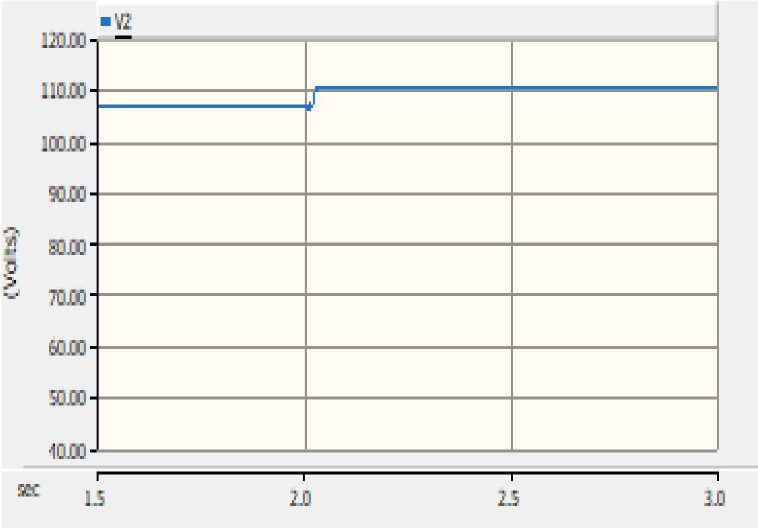


Figure 3.23: Change in Voltage Magnitude at Bus 2 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Voltage Magnitude (volts)

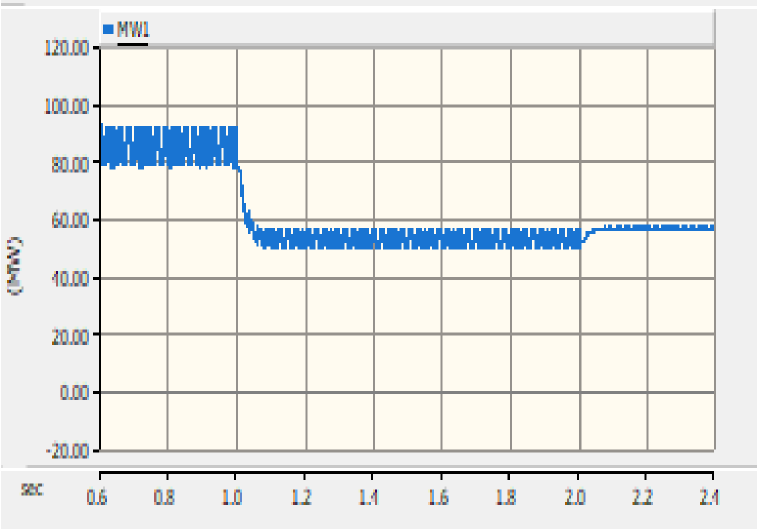


Figure 3.24: Change in Power Generation at Bus 1 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Output Power (MW)

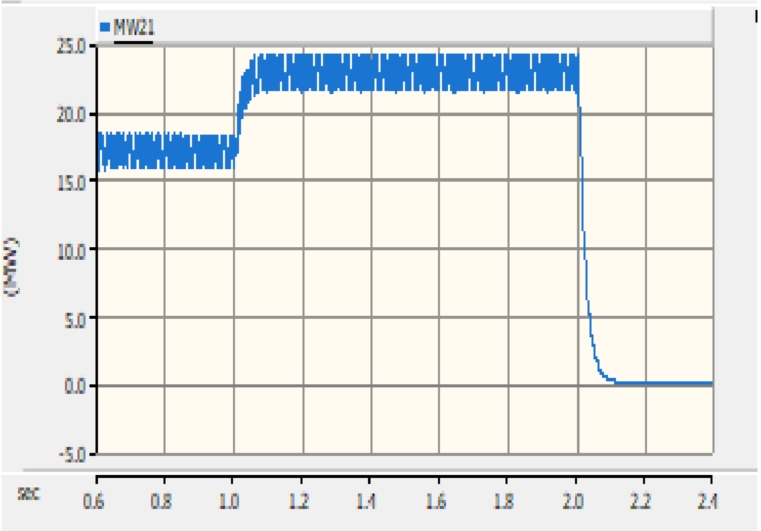


Figure 3.25: Change in Power Output for Generator 1 at Bus 2 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Output Power(MW)

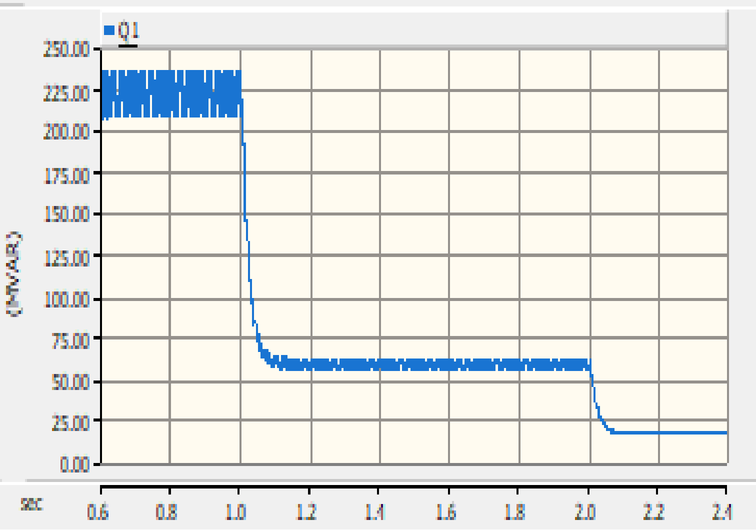


Figure 3.26: Change in Power Generation at Bus 1 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Output Power (MVAR)

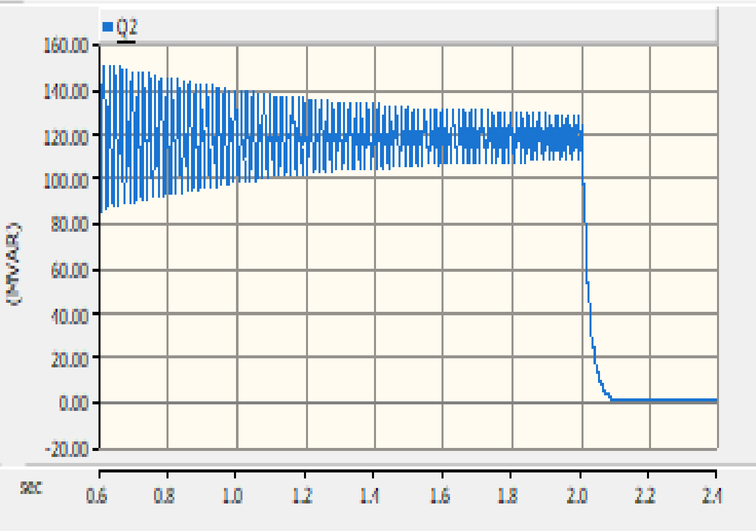


Figure 3.27: Change in Power Output for Generator 1 at Bus 2 Due to Three-Phase Fault on Line 1-2 Where Backup Protection Clears Bus 2, X-axis: Time (seconds) and Y-axis: Output Power (MVAR)

CHAPTER 4

Case Study

4.1 Imitating SCADA Polling in PSCAD/EMTDC

The sample and hold model concept are used to implement solicited integrity polling behavior. Figures 4.1 and 4.2 show built-in blocks from PSCAD/EMTDC that are utilized. The sampler block from the PSCAD Continuous System Model Functions (CSMF) library is used to represent holding a measurement value between polling requests. The impulse generator shown in Figure 4.2 was used to trigger the sampling at fixed intervals.

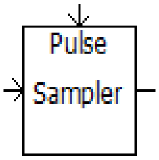


Figure 4.1: Sampler

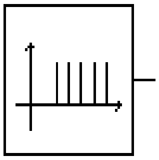


Figure 4.2: Impulse Generator

The Sampler samples a continuous input signal at discrete intervals, and then holds the output at the sampled level until the next sample is taken. The sampling is triggered at a specified sampling rate (by an input pulse train) [30].

In order to generate an impulse train at particular frequency, a built-in impulse generator is used [30].

For instance, consider root mean square (RMS) voltage Erms at Bus 1 in the modified IEEE 14-bus system (see Figure 3.2). Figure 4.3 shows the setup for modelling the polling behavior. SH produces the pulse to activate the sample at particular instances in time by providing pulses at a set sampling frequency. Erms is set as input and Eout is the sampled

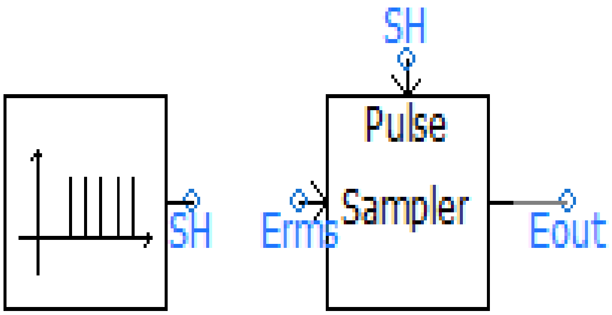


Figure 4.3: Sample and Hold Model

RMS voltage. In the impulse generator the frequency has been set to 5Hz to the sample time period, T=1/5Hz=0.2 seconds. There Eout will be updated ever 0.2 seconds.

The Figure 4.4 depicts the variation of RMS voltage, Erms (V-original), and the output voltage, Eout (V-polling), sampled every 0.2 second using the sample and hold model.

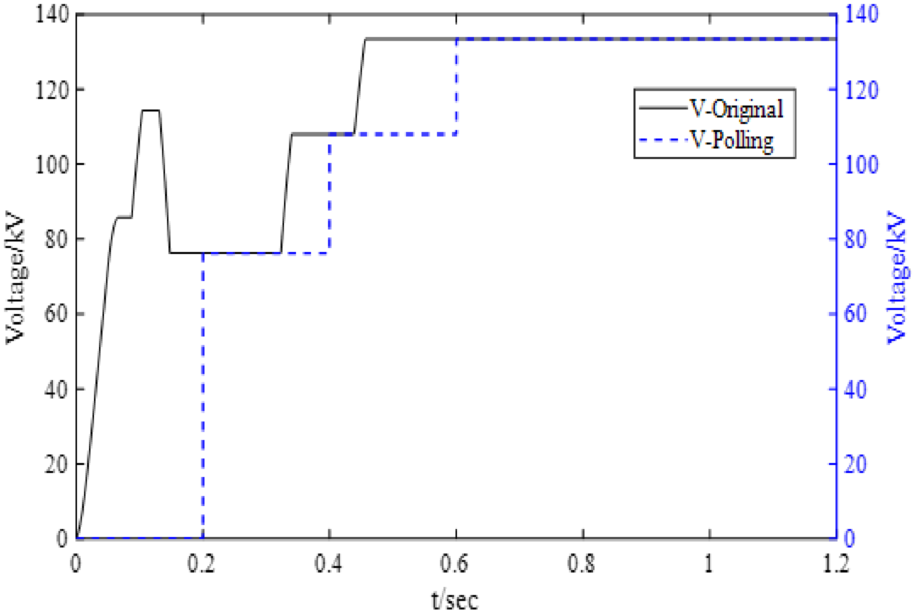


Figure 4.4: Example Showing Polling Input, Erms, and Output, Eout, in PSCAD/EMTDC

4.2 Cyber-Attack on Measurements

4.2.1 Case description

4.2.1.1 Transmission Line Opened

The branch 1-5 (from Bus 1 to Bus 5) is opened due to false command send to the breakers by an attacker. The attacker wishes to follow up on this attack by sending the operator false SCADA data indicating that the line is still in service. This is done by playing back a recording of data from before the attack.

4.2.1.2 False Injection Data

The false SCADA data is sent to the control center on the regular polling interval.

Figures 4.5 through 4.7 compare the actual power injections from the generators at Buses 2, 3 and 6 due to the line trip with the false values sent to the control center. The simulation is executed in PSCAD/EMTDC.

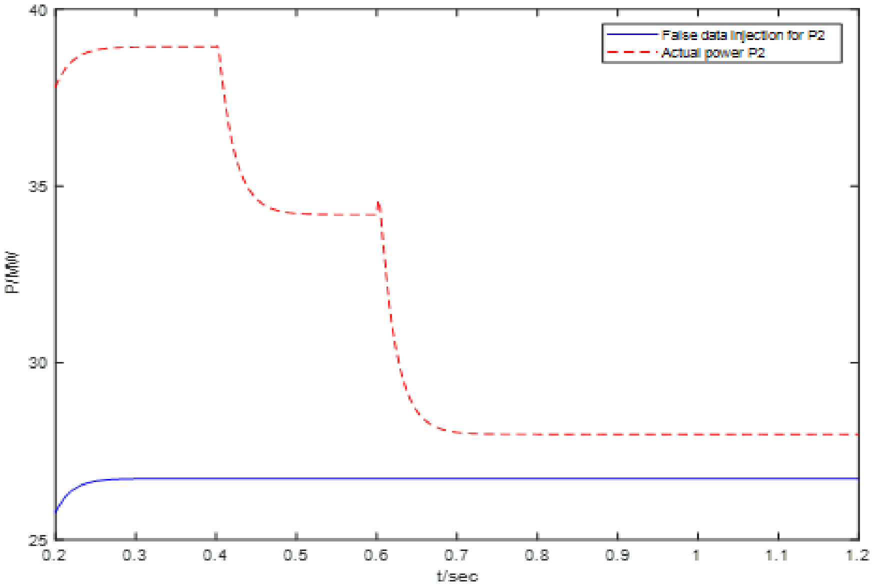


Figure 4.5: Actual Power Output for Generator 1 at Bus 2 in Response to Line Trip (Red Trace) Compared to False Data Sent to Control Center (Blue Trace)

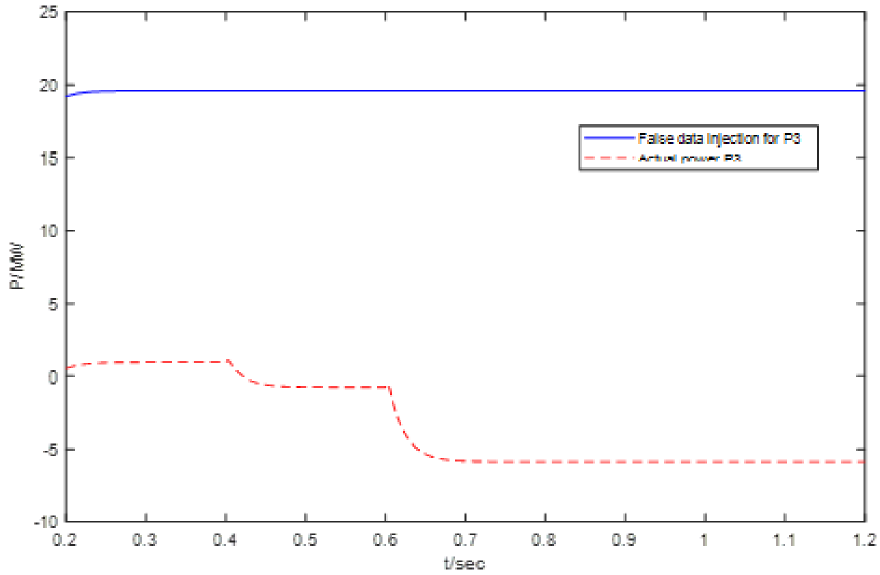


Figure 4.6: Actual Power Output for Generator 1 at Bus 3 in Response to Line Trip (Red Trace) Compared to False Data Sent to Control Center (Blue Trace)

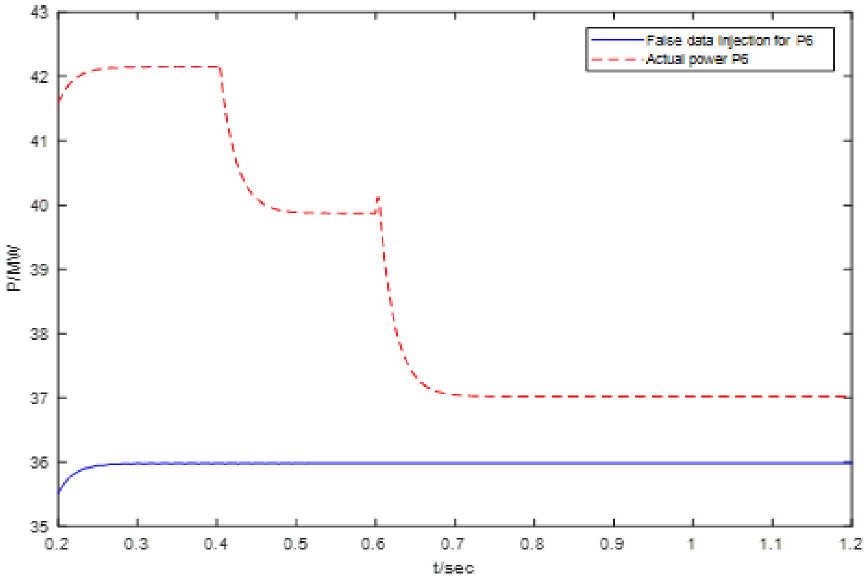


Figure 4.7: Actual Power Output for Generator 1 at Bus 6 in Response to Line Trip (Red Trace) Compared to False Data Sent to Control Center (Blue Trace)

Figures 4.8 through 4.10 show the SCADA polling data for generator power injections. The figures show the actual SCADA data prior to the false data injection. The simulation is executed in PSCAD/EMTDC. Figure 4.8 compares the actual and sampled (polling behavior) power injection from generator 1 prior to the false data injection at Bus 2 polled every 0.2 seconds.

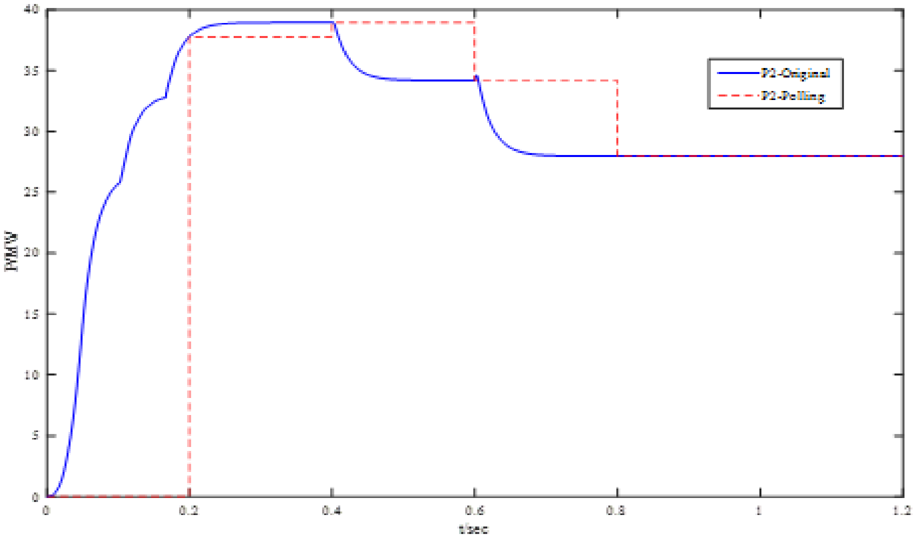


Figure 4.8: Active Power (MW) of Generator 1 at Bus 2

Figure 4.9 compares the actual and sampled (polling behavior) real power injection from generator 1 prior to the false data injection at Bus 3 polled every 0.25 seconds.

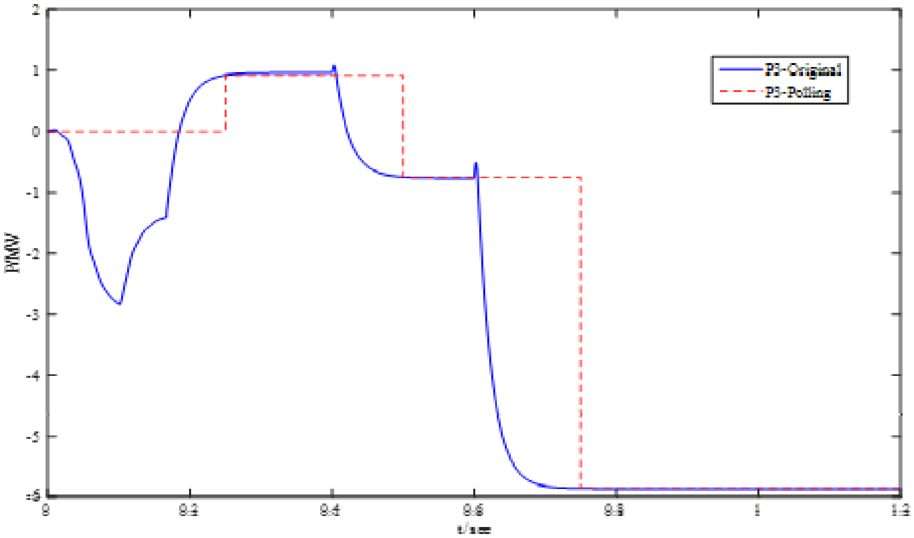


Figure 4.9: Active Power (MW) of Generator 1 at Bus 3

Figure 4.10 shows a comparison of actual and sampled (polling behavior) power injection from generator 1 prior to the false data injection at Bus 6 polled every 0.33 seconds.

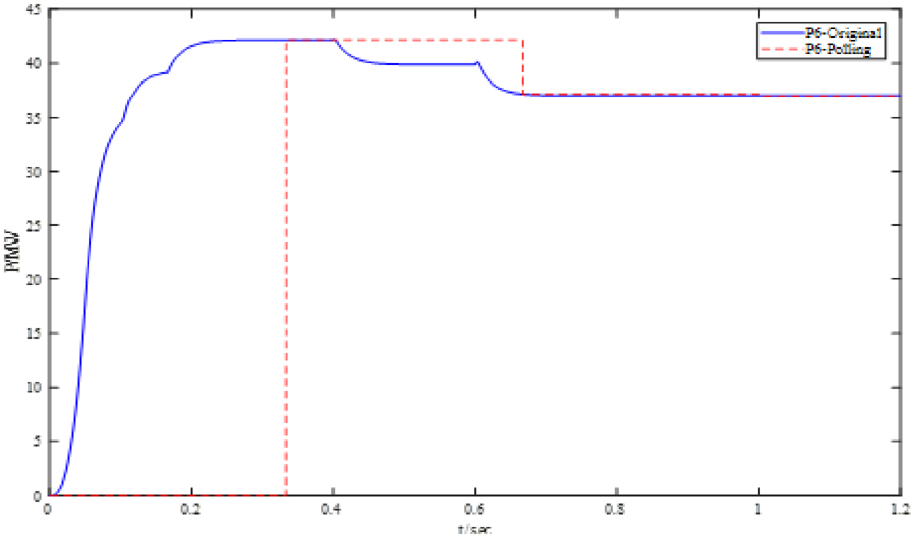


Figure 4.10: Active Power (MW) of Generator 1 at Bus 6

These figures demonstrate how the SCADA polling model in PSCAD/EMTDC can be used to simulate a false data injection attack. The actual generator power is updated every simulation time step, but the data sent to the control center is updated at Bus 2 every 0.2 seconds, at Bus 3 every 0.25 seconds and at Bus 6 every 0.33 seconds

CHAPTER 5

Implementing DNP Communication on RTDS Test Bed

An existing RTDS model of IEEE 14-bus system was modified by a project teammate as part of the project. The modified test system is to be connected to a physical SCADA test bed and use a standard commercial protocol to communicate with a control center.

Distributed Network Protocol 3 (DNP3): It is a communication protocol used between components in industrial process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between data acquisition and control equipment. DNP3 plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (a.k.a. Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs. Similarly, ICCP, the Inter-Control Center Communications Protocol (a part of IEC 60870-6), is used for communication between master stations in different companies but it is not used in this project since there is only one control center. Other standards in use industrial control systems include the Modbus protocol and generic object oriented substation events (GOOSE) messages, a part of the newer IEC 61850 family of protocols [31].

In this project, a lab scale SCADA network using DNP3 was set up to communicate between each substation in the 14-bus system and a SCADA master implemented on a computer running General Electric iFIX. Each substation has one or more intelligent electronic devices fed measurements from the real time digital simulator (RTDS). Each substation has a real time automation controller (RTAC) as the interface to the SCADA network.

5.1 Cyber-Physical Testbed for Power system

Figure 5.1 shows the cyber-physical testbed built around the IEEE 14-bus test system, which is divided into 12 substations for SCADA development. This testbed is intended to be used for power systems resilience studies, including considering both physical events and cyber-attacks.

Cyber-Physical system (CPS) testbeds can fill a role for studying behaviors and vulnerabilities of SCADA networks since real life systems are not available for studies. The use of CPS test beds is especially of value for performing cyber security studies.

The CPS testbed is a platform for teaching and research and will be valuable for exploring scenarios related with cyber security of the power grid. Users can interface with the power system operations and control devices during simulations of disturbances and attacks in the testbed.

Figure 5.1 shows the physical part of the CPS test bed implementation of the IEEE 14-bus system. Substations 1-9 each have a relay receiving raw measurements from the RTDS and sending processed measurements to a RTAC.

The SEL 487B relay in substation 1 receives low level analog measurements from the RTDS GTAO card. The SEL 487B relay communicates with the RTAC using a serial data link. The RTAC communicates with the SCADA master over DNP3 communicated over a TCP/IP network. The figure shows a simplified view of the DNP3 network.

Substations 2-9 will each have a relay that receives IEC 61850 GOOSE messages multicast from the RTDS GTNET card over a second TCP/IP based network. Each relay subsequently communicates with the substation RTAC over a serial data link, and then the RTAC is interfaced to the DNP3 network.

Substations 10-12 are combined into a single relay-RTAC combination due to hardware limitations.

The Cisco managed switch is segmented with the upper ports of the switch configured to support the DNP3 network and the lower ports of switch configured to support the IEC 61850 GOOSE network.

This initial design describe here has subsequently been replaced by a more complex network structure to better study cyber-attack effects.

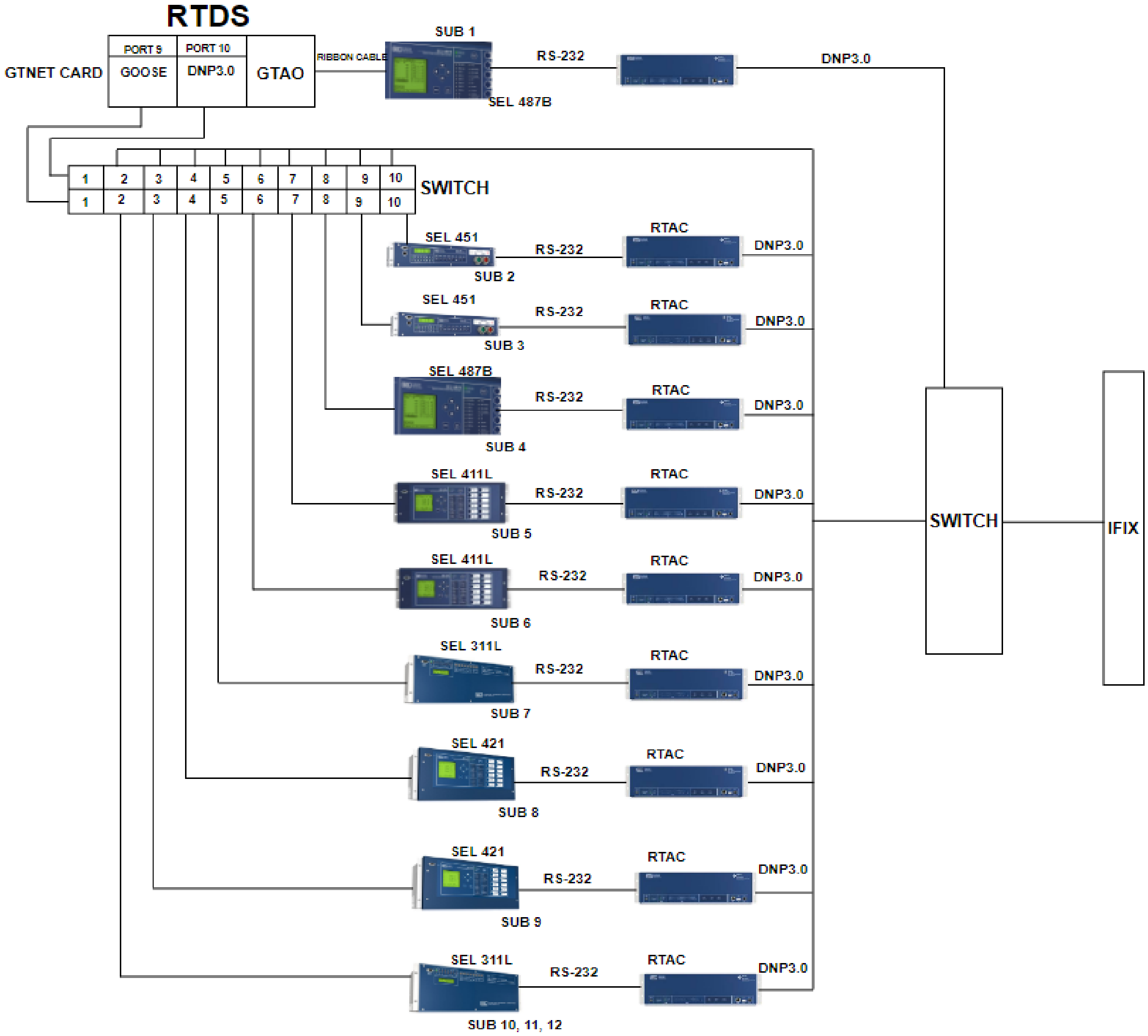


Figure 5.1: Cyber-Physical Testbed for the IEEE 14-Bus System

CHAPTER 6

Summary and Future Work

The thesis implements a polling model in PSCAD/EMTDC that replicates SCADA data on a simulated IEEE 14-bus system. The impacts of cyber-attacks targeting generator and lines are illustrated on the system. The approach implemented here can be used for preliminary studies prior to use of a real-time simulator based test bed for SCADA and control systems. The approach in this thesis explores lower cost options that are able provide a reasonable approximation of the behavior of detailed test beds for use in senior and graduate level courses especially for distance education students.

There are many potential avenues for future work building on this thesis.

- Build a realistic operator interface where the interface shows the SCADA data on a human machine interface, and the operator can take action based on the data, for example, change a generator set point. The command would be transmitted to the component through a SCADA command simulating the timing delay in response.

- Build on the SCADA polling model to develop an energy management system (EMS) for teaching applications. The collected SCADA data can be down sampled and transferred to another simulation program running a state estimator. The state estimation results would go to a power flow/contingency analysis tool and the results presented to an operator interface.

- This thesis implemented a few very simple cyber- attack scenarios. There is a significant amount of work needed to develop a user interface for these attacks for use in a classroom setting, including combining them with the human machine interface and the simulated EMS.

Bibliography

[1] Saranga Menike, Pradeepa Yahampath, and Athula Rajapakshe. "Implementation of Communication Network Components for Transient Simulations in PSCAD/EMTDC". In: *International Conference on Power Systems Transients (IPST2013)*. 2013.

[2] Jie Yan. "A new emergency control method and a preventive mechanism against cascaded events to avoid large-scale blackouts". In: *Doctoral Dissertation, Iowa State University, 2018*. 2018.

[3] J. Yan et al. "A PMU-based risk assessment framework for power control systems". In: *2013 IEEE Power Energy Society General Meeting*. July 2013, pp. 1–5. DOI: 10.1109/PESMG.2013.6672731.

[4] Cleveland. "IEC TC57 Security Standards for the Power System's Information Infrastructure - Beyond Simple Encryption". In: *2005/2006 IEEE/PES Transmission and Distribution Conference and Exhibition*. 2006, pp. 1079–1087.

[5] *A System View of the Modern Grid*. https://www.hsdl.org/?view&did=16088. [Online; accessed 10-October-2019].

[6] S. Sridhar, A. Hahn, and M. Govindarasu. "Cyber-Physical System Security for the Electric Power Grid". In: *Proceedings of the IEEE* 100.1 (2012), pp. 210–224.

[7] "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems". In: *US Government Accounting Office, GAO-04-354, March 2014*. 2004.

[8] X. Cai et al. "Review of Cyber-attacks and Defense Research on Cyber Physical Power System". In: *2019 IEEE Sustainable Power and Energy Conference (iSPEC)*. 2019, pp. 487–492.

[9] D.I. Dogaru and I. Dumitrache. "Cyber attack of a Power Grid Analysis using a Deep Neural Networks Approach". In: *Control Engineering and Applied Informatics* 21 (Jan. 2019), pp. 42–50.

[10] Ning Cai, Jidong Wang, and Xinghuo Yu. "SCADA System Security: Complexity, History and New Developments". In: *2008 6th IEEE International Conference on Industrial Informatics*. 2008, pp. 569–574.

[11] D. J. Marihart. "Communications Technology Guidelines for EMS/SCADA Systems". In: *IEEE Transactions on Power Delivery* 16.2 (2001), pp. 181–188.

[12] J. Newbury and W. Miller. "Potential Metering Communication Services Using the Public Internet". In: *IEEE Transactions on Power Delivery* 14.2 (1999), pp. 1202–1207.

[13] S. Mak and D. Radford. "Communication system requirements for Implementation of a Large Scale Demand Side Management and Distribution Automation". In: *IEEE Transactions on Power Delivery* 11.2 (1996), pp. 683–689.

[14] M. Wei and Z. Chen. "Distribution system protection with communication technologies". In: *IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society*. 2010, pp. 3328–3333.

[15] B. Chen et al. "Impact of Cyber attacks on Transient Stability of Smart Grids with Voltage Support Devices". In: *2013 IEEE Power Energy Society General Meeting*. 2013, pp. 1–5.

[16] P. McLaren et al. "Incorporating PSCAD/EMTDC into a Real Time Playback Test Set". In: *In Proc. Int. Conf. Power Systems Transients* (1997).

[17] Mesut Baran, Raghuram Sreenath, and Nikhil Mahajan. "Extending EMTDC/PSCAD for Simulating Agent-Based Distributed Applications". In: *IEEE Power Engineering Review* 22 (Dec. 2002), pp. 52–54. DOI: 10.1109/MPER.2002.1098049.

[18] B. Chen et al. "Network Delay caused by Cyber attacks on SVC and its Impact on Transient Stability of Smart Grids". In: *2014 IEEE PES General Meeting — Conference Exposition*. 2014, pp. 1–5.

[19] D. Willenberg, P. Erlinghagen, and A. Schnettler. “Analysis of the Impact of Cyber Attacks in Active Distribution Grids Onto the Transient System Stability”. In: *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. 2018, pp. 1–6.

[20] A. Farraj, E. Hammad, and D. Kundur. “On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control”. In: *IEEE Transactions on Industrial Informatics* 13.6 (2017), pp. 3322–3333.

[21] Y. Chakhchoukh et al. “Statistical Outlier Detection for Diagnosis of Cyber attacks in Power State Estimation”. In: *2016 IEEE Power and Energy Society General Meeting (PESGM)*. 2016, pp. 1–5.

[22] J. Zhao, L. Mili, and A. Abdelhadi. “Robust dynamic State Estimator to Outliers and Cyber attacks”. In: *2017 IEEE Power Energy Society General Meeting*. 2017, pp. 1–5.

[23] Y. Chakhchoukh, H. Lei, and B. K. Johnson. “Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation”. In: *IEEE Transactions on Power Systems* 35.2 (2020), pp. 1188–1197.

[24] Irina Kolosok and L. Gurina. “Determination of the Vulnerability Index to Cyberattacks and State-Estimation Problems According to SCADA Data and Timed Vector Measurements”. In: *Russian Electrical Engineering* 88 (Jan. 2017), pp. 23–29. DOI: `10.3103/S1068371217010096`.

[25] A. A. Jahromi et al. “Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes”. In: *IEEE Transactions on Power Systems* 35.1 (2020), pp. 440–450.

[26] Deepa Kundur et al. “Towards Modelling the Impact of Cyber attacKs on a Smart Grid”. In: *IJSN* 6 (Apr. 2011), pp. 2–13. DOI: `10.1504/IJSN.2011.039629`.

[27] *National Institute of Standards and Technology.* `http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913905]`. [Online; accessed 10-October-2019].

[28] *scada-and-polling-1*. https://www.taitradioacademy.com/topic/scada-and-polling-1/. [Online; accessed 10-October-2019].

[29] *IEEE 14-Bus System*. http://www.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm. [Online; accessed 10-October-2019].

[30] $PSCAD_On - Line_Help_System$. https://www.pscad.com/webhelp/PSCAD/The_Application_Environment/PSCAD_On-Line_Help_System.htm. [Online; accessed 10-October-2019].

[31] *DNP3*. https://en.wikipedia.org/wiki/DNP3. [Online; accessed 10-October-2019].

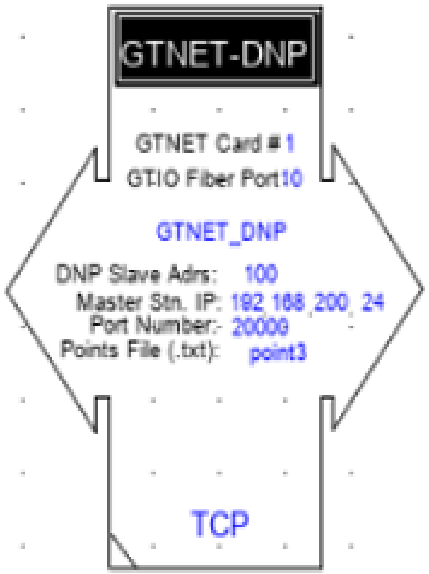
APPENDIX A

Procedure for Implementing DNP Between RTDS and RTAC

Procedure for interconnecting the RTDS and RTAC:

This procedure is writtento help student or researchers. Before implementing this procedure, make sure RTDS rack has a GTNET card with DNP protocol licensed on it.

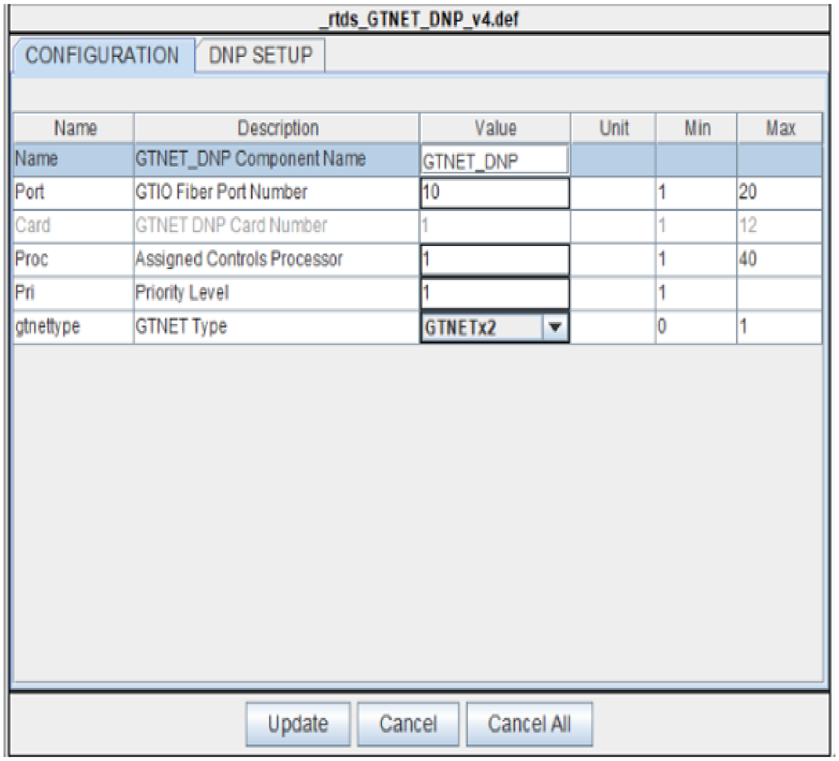
- RTAC and GTNET card should be in same network.
- Import a DNP block in RSCAD model.



GTNET Card # 1
GTIO Fiber Port 10
DNP Slave Adrs: 100
Master Stn. IP: 192 168 200 24
Port Number:- 20000
Points File (.txt): point3

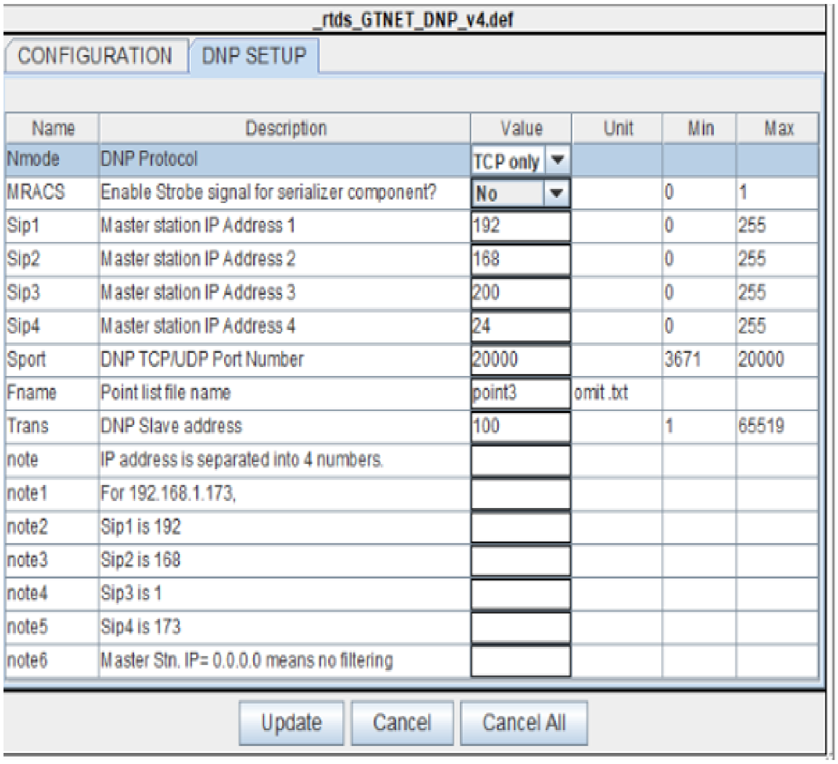
Figure A.1: DNP Block in RSCAD

- Consider RTAC as a client and mention proper IP address, fiber port number, DNP slave address in GTNET-DNP model.
- Map the points in .txt format and save this in same destination where you saved the RTDS model of system. For example, figure below shows the format for mapping analog inputs.



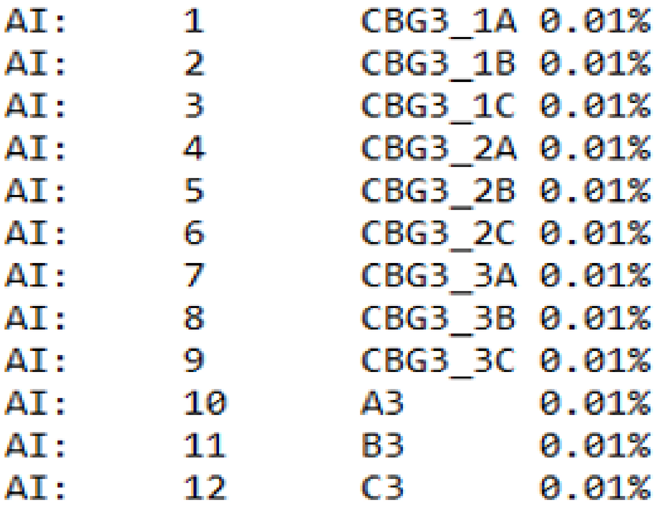
Name	Description	Value	Unit	Min	Max
Name	GTNET_DNP Component Name	GTNET_DNP			
Port	GTIO Fiber Port Number	10		1	20
Card	GTNET DNP Card Number	1		1	12
Proc	Assigned Controls Processor	1		1	40
Pri	Priority Level	1		1	
gtnettype	GTNET Type	GTNETx2		0	1

Figure A.2: DNP Configuration Tab



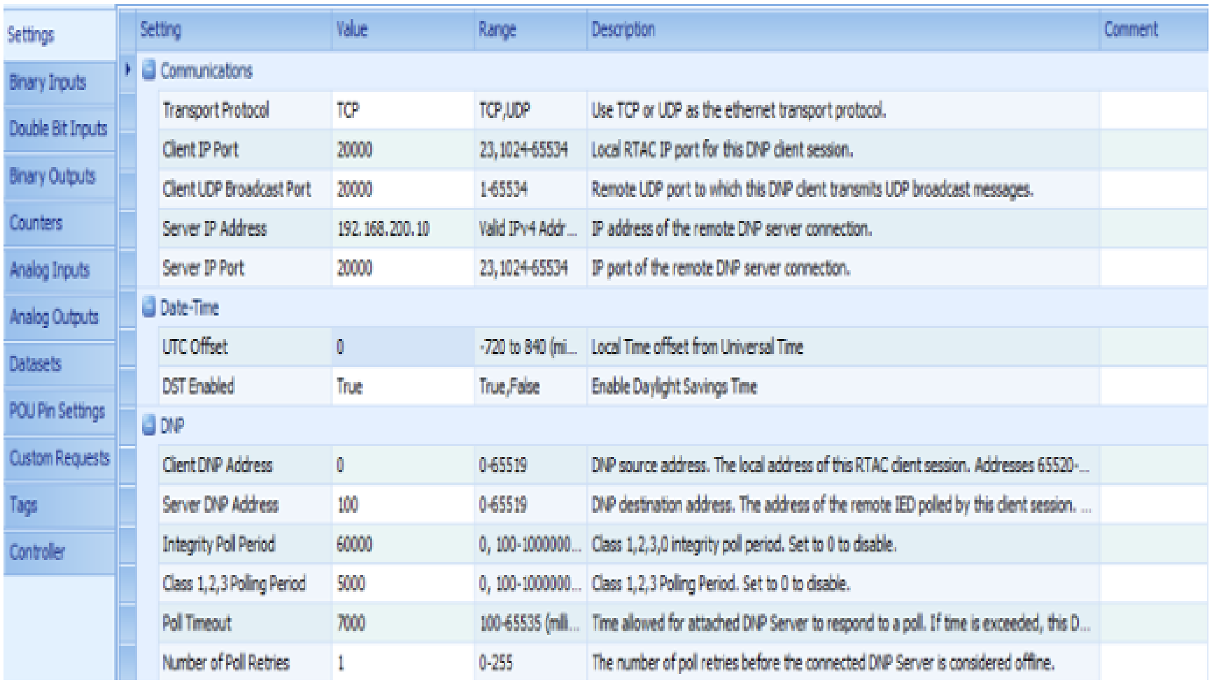
Name	Description	Value	Unit	Min	Max
Nmode	DNP Protocol	TCP only			
MRACS	Enable Strobe signal for serializer component?	No		0	1
Sip1	Master station IP Address 1	192		0	255
Sip2	Master station IP Address 2	168		0	255
Sip3	Master station IP Address 3	200		0	255
Sip4	Master station IP Address 4	24		0	255
Sport	DNP TCP/UDP Port Number	20000		3671	20000
Fname	Point list file name	point3	omit .txt		
Trans	DNP Slave address	100		1	65519
note	IP address is separated into 4 numbers.				
note1	For 192.168.1.173,				
note2	Sip1 is 192				
note3	Sip2 is 168				
note4	Sip3 is 1				
note5	Sip4 is 173				
note6	Master Stn. IP= 0.0.0.0 means no filtering				

Figure A.3: DNP Setup Tab



```
AI:     1       CBG3_1A 0.01%
AI:     2       CBG3_1B 0.01%
AI:     3       CBG3_1C 0.01%
AI:     4       CBG3_2A 0.01%
AI:     5       CBG3_2B 0.01%
AI:     6       CBG3_2C 0.01%
AI:     7       CBG3_3A 0.01%
AI:     8       CBG3_3B 0.01%
AI:     9       CBG3_3C 0.01%
AI:     10      A3      0.01%
AI:     11      B3      0.01%
AI:     12      C3      0.01%
```

Figure A.4: Mapping points from RTDS model in .txt format

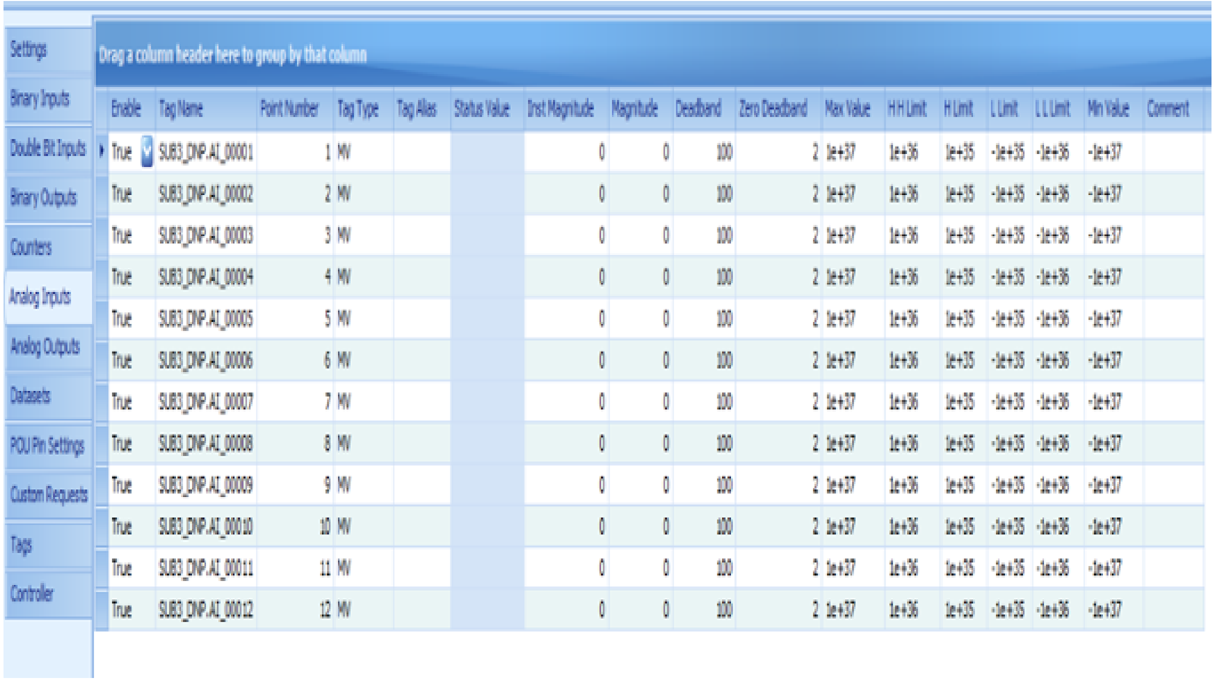


Setting	Value	Range	Description	Comment
Communications				
Transport Protocol	TCP	TCP,UDP	Use TCP or UDP as the ethernet transport protocol.	
Client IP Port	20000	23,1024-65534	Local RTAC IP port for this DNP client session.	
Client UDP Broadcast Port	20000	1-65534	Remote UDP port to which this DNP client transmits UDP broadcast messages.	
Server IP Address	192.168.200.10	Valid IPv4 Addr...	IP address of the remote DNP server connection.	
Server IP Port	20000	23,1024-65534	IP port of the remote DNP server connection.	
Date-Time				
UTC Offset	0	-720 to 840 (mi...	Local Time offset from Universal Time	
DST Enabled	True	True,False	Enable Daylight Savings Time	
DNP				
Client DNP Address	0	0-65519	DNP source address. The local address of this RTAC client session. Addresses 65520-...	
Server DNP Address	100	0-65519	DNP destination address. The address of the remote IED polled by this client session. ...	
Integrity Poll Period	60000	0, 100-1000000...	Class 1,2,3,0 integrity poll period. Set to 0 to disable.	
Class 1,2,3 Polling Period	5000	0, 100-1000000...	Class 1,2,3 Polling Period. Set to 0 to disable.	
Poll Timeout	7000	100-65535 (mili...	Time allowed for attached DNP Server to respond to a poll. If time is exceeded, this D...	
Number of Poll Retries	1	0-255	The number of poll retries before the connected DNP Server is considered offline.	

Figure A.5: DNP Settings for RTDS (GTNET-DNP) to Communicate With RTAC

- Open AcSELerator RTAC software. Consider GTNET-DNP as a server and configure its setting with proper IP address and other shown in Figure A.5.

- Mark the number of points that to be tagged, and all the analog points that are mapped in .txt format will appear automatically in analog inputs, shown in Figure A.6.



Enable	Tag Name	Point Number	Tag Type	Tag Alias	Status Value	Inst Magnitude	Magnitude	Deadband	Zero Deadband	Max Value	H H Limit	H Limit	L Limit	L L Limit	Min Value	Comment
True ☑	SUB3_DNP.AI_00001	1	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00002	2	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00003	3	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00004	4	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00005	5	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00006	6	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00007	7	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00008	8	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00009	9	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00010	10	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00011	11	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	
True	SUB3_DNP.AI_00012	12	MV			0	0	100	2	1e+37	1e+36	1e+35	-1e+35	-1e+36	-1e+37	

Figure A.6: Mapping RTDS Model Tags

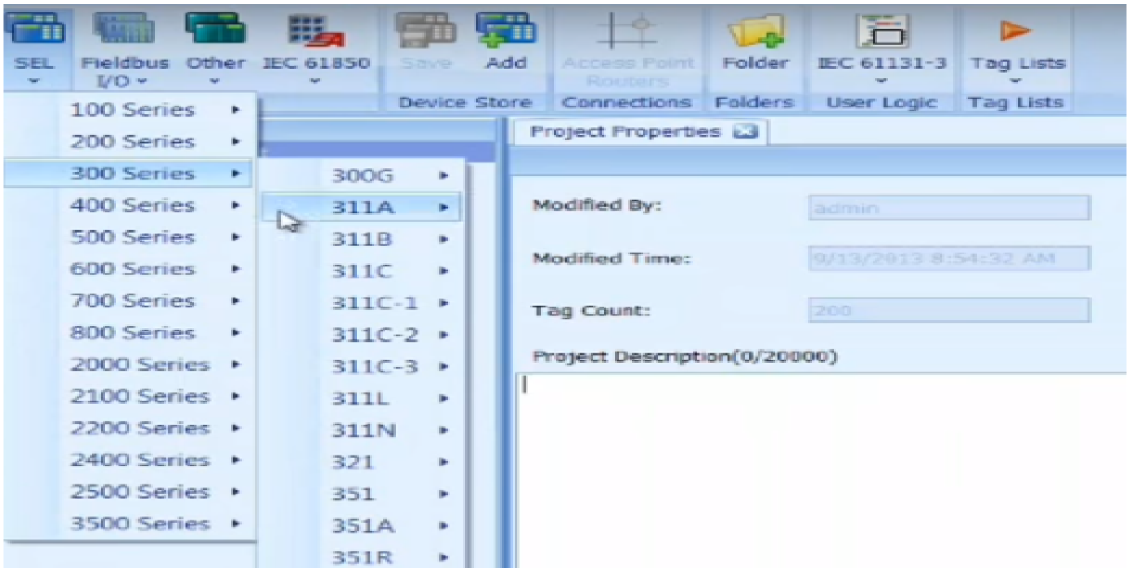
- Then go to controller and go online. We can see all data in Tags (instMag).

APPENDIX B

Procedure for Implementing DNP Between RTAC and Relay

- RTAC and Relay card should be in same network.

- Open AcSELerator RTAC software and select corresponding relay to be used.



Modified By: admin

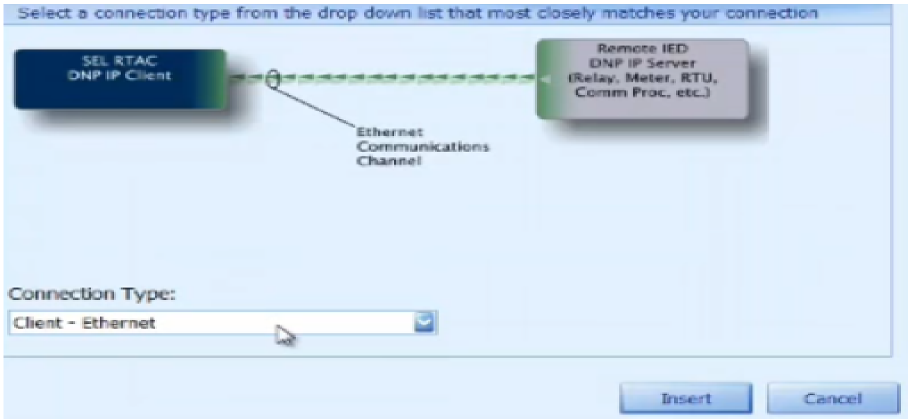
Modified Time: 9/13/2013 8:54:32 AM

Tag Count: 200

Project Description(0/20000)

Figure B.1: Selection of Relay

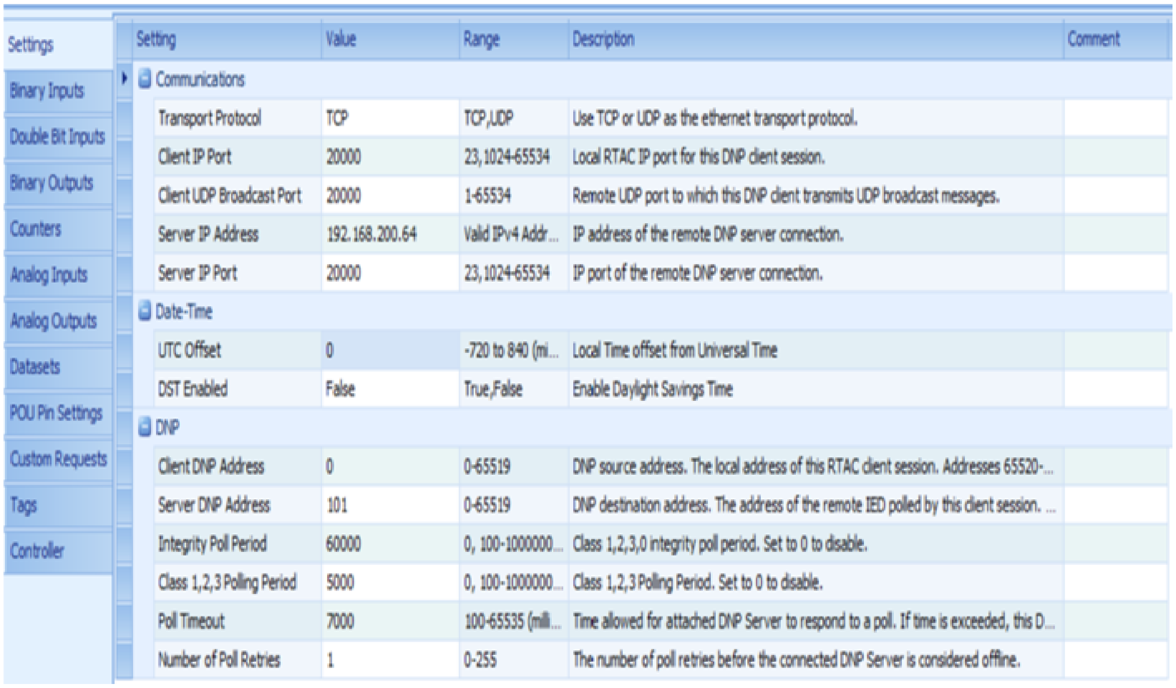
- Select the connection type used between RTAC and the Relay.



Select a connection type from the drop down list that most closely matches your connection

Connection Type: Client - Ethernet

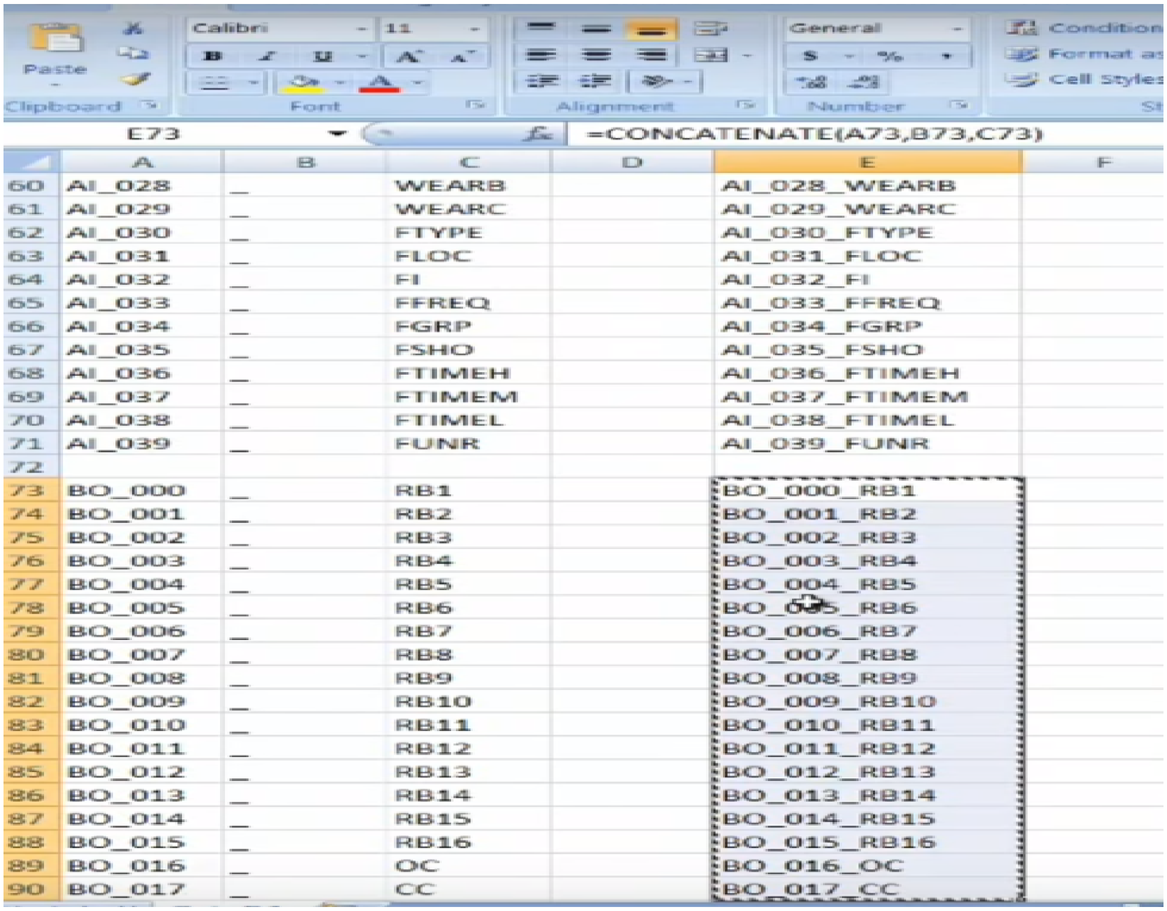
Figure B.2: Connection Type from Relay to RTAC



Setting	Value	Range	Description	Comment
Communications				
Transport Protocol	TCP	TCP,UDP	Use TCP or UDP as the ethernet transport protocol.	
Client IP Port	20000	23,1024-65534	Local RTAC IP port for this DNP client session.	
Client UDP Broadcast Port	20000	1-65534	Remote UDP port to which this DNP client transmits UDP broadcast messages.	
Server IP Address	192.168.200.64	Valid IPv4 Addr...	IP address of the remote DNP server connection.	
Server IP Port	20000	23,1024-65534	IP port of the remote DNP server connection.	
Date-Time				
UTC Offset	0	-720 to 840 (mi...	Local Time offset from Universal Time	
DST Enabled	False	True,False	Enable Daylight Savings Time	
DNP				
Client DNP Address	0	0-65519	DNP source address. The local address of this RTAC client session. Addresses 65520-...	
Server DNP Address	101	0-65519	DNP destination address. The address of the remote IED polled by this client session. ...	
Integrity Poll Period	60000	0, 100-1000000...	Class 1,2,3,0 integrity poll period. Set to 0 to disable.	
Class 1,2,3 Polling Period	5000	0, 100-1000000...	Class 1,2,3 Polling Period. Set to 0 to disable.	
Poll Timeout	7000	100-65535 (mili...	Time allowed for attached DNP Server to respond to a poll. If time is exceeded, this D...	
Number of Poll Retries	1	0-255	The number of poll retries before the connected DNP Server is considered offline.	

Figure B.3: DNP Settings for Relay to Communicate With RTAC

- Enter proper Server IP address, Server and Client DNP address.
- Extract all analog and binary input/output points from AcSELerator quickset software to Microsoft Excel spreadsheet shown in Figure B.4.
- Copy and paste these mapped points into respective tags (analog and binary input/output tag) and then go to controller and go online.



E73 =CONCATENATE(A73,B73,C73)

	A	B	C	D	E	F
60	AI_028	_	WEARB		AI_028_WEARB	
61	AI_029	_	WEARC		AI_029_WEARC	
62	AI_030	_	FTYPE		AI_030_FTYPE	
63	AI_031	_	FLOC		AI_031_FLOC	
64	AI_032	_	FI		AI_032_FI	
65	AI_033	_	FFREQ		AI_033_FFREQ	
66	AI_034	_	FGRP		AI_034_FGRP	
67	AI_035	_	FSHO		AI_035_FSHO	
68	AI_036	_	FTIMEH		AI_036_FTIMEH	
69	AI_037	_	FTIMEM		AI_037_FTIMEM	
70	AI_038	_	FTIMEL		AI_038_FTIMEL	
71	AI_039	_	FUNR		AI_039_FUNR	
72						
73	BO_000	_	RB1		BO_000_RB1	
74	BO_001	_	RB2		BO_001_RB2	
75	BO_002	_	RB3		BO_002_RB3	
76	BO_003	_	RB4		BO_003_RB4	
77	BO_004	_	RB5		BO_004_RB5	
78	BO_005	_	RB6		BO_005_RB6	
79	BO_006	_	RB7		BO_006_RB7	
80	BO_007	_	RB8		BO_007_RB8	
81	BO_008	_	RB9		BO_008_RB9	
82	BO_009	_	RB10		BO_009_RB10	
83	BO_010	_	RB11		BO_010_RB11	
84	BO_011	_	RB12		BO_011_RB12	
85	BO_012	_	RB13		BO_012_RB13	
86	BO_013	_	RB14		BO_013_RB14	
87	BO_014	_	RB15		BO_014_RB15	
88	BO_015	_	RB16		BO_015_RB16	
89	BO_016	_	OC		BO_016_OC	
90	BO_017	_	CC		BO_017_CC	

Figure B.4: Relay Data Extracted from AcSELerator Quickset