Iowa State University

Cyber Security Smart Grid Testbed

Senior Design Project Plan

Derek Reiser

Cole Hoven

Jared Pixley

Rick Sutton

Faculty Advisor: Professor Manimaran Govindarasu

Table of Contents

Problem/Need 3

System Overview 3

Operating Environment 4

Functional Requirements 9

Non-Functional Requirements 9

Risks/Mitigation 10

Resource Requirements 10

Work Plan 11

Definitions 12

Citations 13

Problem/Need

Supervisory Control and Data Acquisition (SCADA) is a typer of industrial control system used to monitor and control industrial processes in the world such as power generation, water treatment, oil and gas pipelines and many other critical systems. The electric power grid is a highly automated and complex network comprised of a variety of control systems, sensors, communication networks and many other forms of information all with the purpose of monitoring, protecting and controlling the power grid. Due to the continuos development of this automated network and many other critical systems, the threat of cyber-based attacks are becoming more and more of a reality. These attacks could stop and damage many important systems that most of us take for granted. Therefore, security of the power grid and other critical automated networks (through the SCADA system) is one of the most impatient developmental issues we have today.

To conduct this research, a PowerCyber testbed has been developed in recent years by other graduate and undergraduate students resulting in a properly functioning testbed network. This testbed allows us to simulate power systems and the communication protocols they use and attempt cyber attacks on the system. The current testbed in composed of Real-Time Digital Simulator, industry-grade power system control center software, substation automation systems, communication protocols, security devices, relays, and a fuzzer device (for vulnerability analysis). Our team will be responsible for integrating additional components to the system and perform addition security attack analysis with a larger power system network.

System Overview

The PowerCyber testbed provides a realistic electric grid control infrastructure based on a combination of physical, simulated, and emulated components. The testbed integrates industry standard control software, communication protocols, and field devices combined with power system simulators to provide an accurate representation of a cyber-physical grid. We are continuing to improve the testbed to provide numerous cyber-security and power system research capabilities. Continued improvement of the PowerCyber testbed will provide better demonstration and information regarding cyber vulnerability assessment, attack impact analysis, and cyber-physical system studies.

The SCADA system can be broken down into a few key components:

Control Center: Usually consist of a Human-Machine Interface (HMI). This let a human operator view processed data and control that same process.

Supervisory Station: This element consists of the servers, software and stations responsible for providing communication between the Control Center and RTU's.

Remote Terminal Unit (RTU): Typically connected to physical equipment. The RTU is used to convert electrical signals from hardware sensors to digital data which is collected by the supervisory station.

Sensor: A device that measures an analog or status value in some element of a process. A sensor collect the raw process data used to make decisions about a process.

Below, one can see the high level diagram to illustrate the SCADA network that has been provided from previous years.

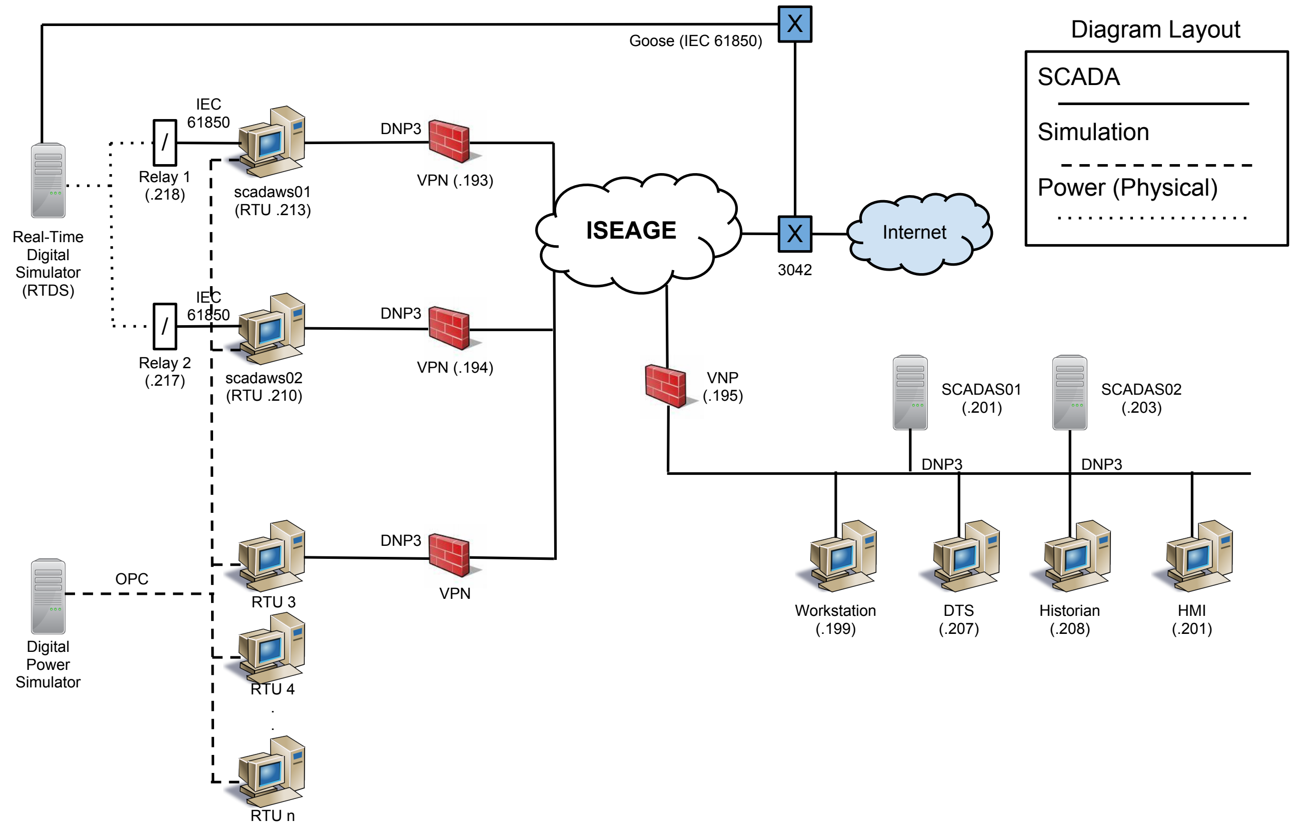


Figure 1: Current Testbed

Operating Environment

Our SCADA network testbed consist of a few key pieces of hardware and software:

Hardware:

1) Siemens SCALANCE S612 Security Module
2) Siemens SIPROTEC 4 7SJ61 Relay (Sensor)

Software:

3) Siemens Spectrum Power TG SCADA/EMS (HMI)
4) Siemens SICAM PAS v6.00 (RTU)
5) Siemens DIGIS (Software for SIPROTECT Protection Relays)
6) VmWare ESXi Hypervisory Operating System
7) Backtrack 5

1) Siemens SCALANCE S612 Security Module

SCADA systems operate across large distances and are required transmit process information across Wide Area Networks (WANs). It is therefore important to employ some sort of protection method to ensure the integrity and confidentiality of this data. The SCALANCE S612 Security Module is used to provide point-to-point data integrity and confidentiality within SCADA system networks by controlling data traffic to and from SCALANCE S612 cells. These devices will be used within our SCADA system test bed to protect information being transmitted between our SCADA control center and substation RTUs across Wide and Local Area Networks.

This device, developed by Siemens, is designed to provide data protection to and from the SCALANCE cell by being connected upstream from the devices to be protected. The SCALANCE device solves the problem of security rule and configuration checks that hinder the transmission and use of information in real-time by encrypting and sending data transmissions in real-time. The SCALANCE S612 can protect up to 32 devices and supports a maximum of 64 VPN tunnels simultaneously.

2) Siemens SIPROTEC 4 7SJ61 Relay (Sensor)

The SIPROTEC 4 7SJ61 Relay can be used to provide simple control of circuit- breaker and automation functions and will be used in our SCADA system test bed to act as a sensor that performs our system's process data collection. The relays that will be used within our SCADA system will be operated and managed by Siemens DIGSI 4 software, allowing the operator implement customized automation functions via the relays' integrated programmable logic (CFC).

3) Siemens Spectrum Power TG SCADA/EMS (HMI)

The Spectrum Power TG software is the supervisory control and data acquisition (SCADA) system within our tested. It is also the Human-Machine Interface (HMI) by which a human operator can view data from and make decisions about a process.

According to Siemens this software is the most reliable, scalable, flexible, highly available SCADA system on the market and can be used to control various large scale infrastructures such as those of electric, gas, and water utilities and railways. This system is scalable from a single Substation/RTU to the world's largest control centers with hierarchical systems capable of linking in infinite number of systems.

4) Siemens SICAM PAS v6.00 (RTU)

SICAM PAS (Power Automation System) is a piece of software used in conjunction with Spectrum Power TG software as a part of a SCADA system. The SICAM PAS software runs in and acts as a Remote Terminal Unit that is responsible for interpreting sensory data about a process and communicating this data to a control center running the Spectrum Power TG software.

Siemens describes SICAM PAS as a computer-based information management system used to structure the diverse substation information and ensure that it is used efficiently. This software can be implemented in a distribution configuration, allowing the system to operate simultaneous on multiple systems. At the same time SICAM PAS acts as a gateway, requiring only one connection to higher-level control centers. SICAM PAS can be use existing hardware components and communication standards as well as their connections.

5) Siemens DIGIS (Software for SIPROTECT Protection Relays)

The Siemens DIGSI 4 software is used for configuration, operation and organization of Siemens SIPROTEC protection relays. This software will be used in this capacity to support the SIPROTEC Relays used in our SCADA system test bed to retrieve simulated “process information”.

DIGSI 4 is considered Siemens easy-to-use and user-friendly solution for commission and operation of Siemens protection devices. This system integrates password protection to restrict access for different jobs only authorized staff. The DIGSI software allows for easy of use of PLCs with a graphical editor without any programming skills. Additionally, DIGSI remote allows access to process data and event logs from a remote station when the location of a relay station may be far away.

6) VmWare ESXi Hypervisory Operating System

In order to provide virtualized substations for the test bed, we will be using VmWare ESXi Hypervisor Operating System to host all the virtual machines. This OS is used by many companies for their virtual platform. It allows easy control over Virtual Machines by using a VSphere client to connect to the VmWare Server. VmWare ESX also has the ability for virtual machine templates. Meaning that we can setup a RTU the way we want and then we can deploy many RTU’s from that one RTU.

7) Backtrack 5

Backtrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. The penetration distribution has been customized down to every package, kernel configuration, script and patch solely for the purpose of the penetration tester.

We have been given additions devises and software that we are going to add to the testbed:

Hardware:

1) OPAL-RT Technologies OP5600 HIL Box
2) Schweitzer Engineering Laboratories SEL-3378 (Synchrophasor vector processor)
3) Schweitzer Engineering Laboratories SEL-421 (Protection Automation Control)

Software:

4) RT-LAB
5) Quickset

1) OPAL-RT Technologies OP5600 HIL Box

The OPAL-RT real time digital simulator is a simulator that can run in real time to better simulate a power system. Multiple busses can be virtually simulated while running the test to minimize physical equipment needed.

OPAL-RT Technologies says that the OP500 adds advanced monitoring capabilities and scalable I/O and processor power. It is also modular and flexible to meet specific I/O requirements.

2) Schweitzer Engineering Laboratories SEL-3378 (Synchrophasor vector processor)

The SEL-3378 acts as a logic engine between all of the SEL PMU's. It take the incoming data and based on what the readings are it will send out predefined actions.

The Synchrophasor Vector Processor (SVP), the first real-time synchrophasor programmable logic controller, collects the synchrophasor messages from relays and phasor measurement units (PMUs). The SVP time-aligns incoming messages, processes them with an internal logic engine, and sends control commands to external devices to perform user-defined actions. Additionally, the SVP can send calculated or derived data to devices such as other SVPs, phasor data concentrators (PDCs), and monitoring systems.

3) **Schweitzer Engineering Laboratories SEL-421 (Protection Automation Control)**

Like the Siemens SIPROTEC 4 this is a relay can be used to provide simple control of circuit-breaker and automation functions. One of the big differences between this relay and the Siemens is the High-Accuracy Time Stamping. This allows all the SEL devices to communicate on the same clock within 10 nano seconds of each other. This makes all timed actions much more accurate.

4) **RT-LAb**

RT-LAB is the software used to set up and run the OPAL-RT simulator. Models for the simulator are created in Simulink and RT-LAB runs the models on the simulator. RT-LAB is scalable and allows us to add computing power where and when it is needed.

5) **Quickset**

Quickset is a template based software which allows us to connect the different SEL devices to the RTU's. This also allows us to ensure that the devices are all set up the same on devices when needed or allows us to make small changed in the communication between devices.

Once we add in these new devices our high level diagram should look like the diagram below.

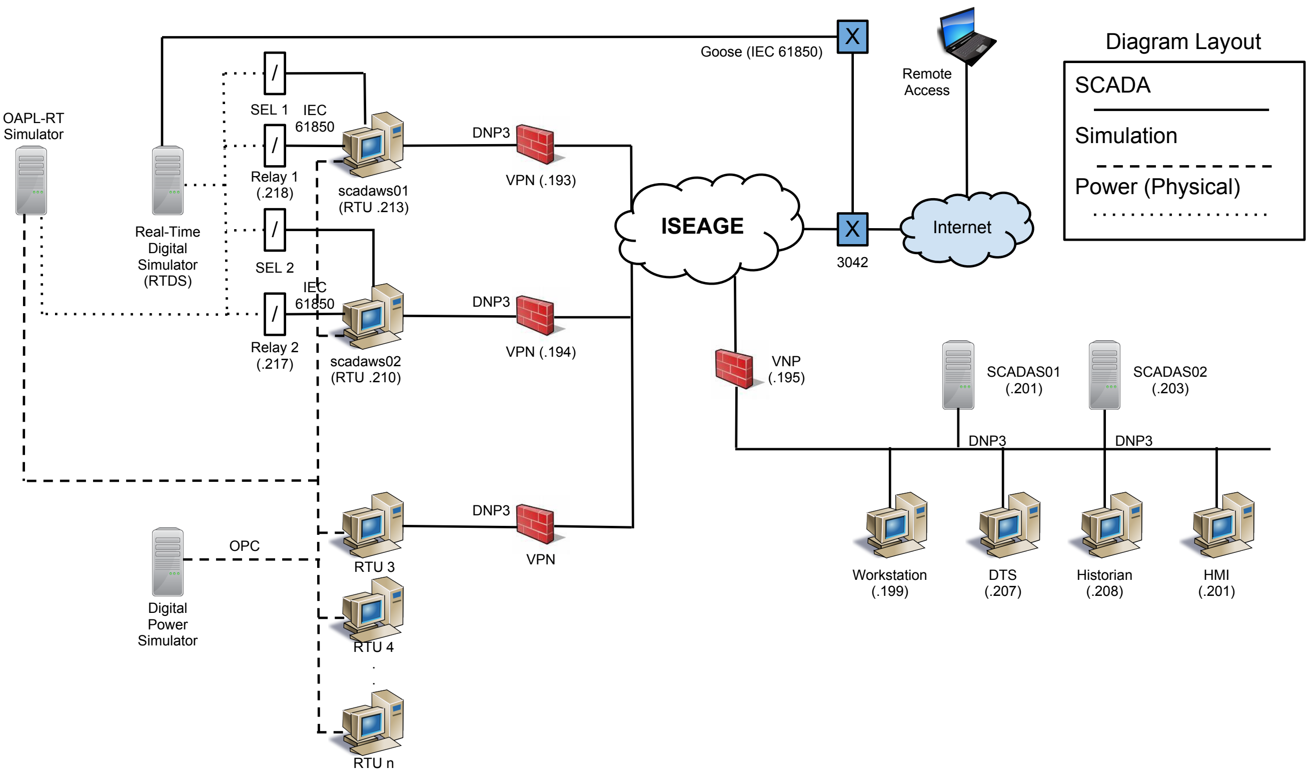


Figure 2: Future Testbed

Functional Requirements

1) Integrate the OPAL-RT simulator into the current testbed.
   - i) Create a 9 bus system for the OPAL-RT simulator in RT-LAB and Simulink
   - ii) Make physical connections with components in the current testbed
   - iii) Set up proper data transfer between the simulator and testbed
   - iv) Run functional tests to assure successful integration

2) Integrate the SEL PMU's into the testbed.
   - i) Connect PMU's with current testbed
   - ii)Set up proper data transfer between the simulator and testbed
   - iii)Run functional test to assure successful integration

3) Integrate a 30 bus system into the testbed.
   - i) Create a 30 bus model for the OPAL-RT Simulator in RT-LAB and Simulink
   - ii) Implement 30 bus model with simulator and the rest of the testbed

4) Set up remote access capabilities.
   - i) Create a remote login server
   - ii) Automate the testbed software
   - iii) Run "the demo" remotely

Nonfunctional Requirements

1) Simplify the current 30 bus model.
   - i) Clean up the current 30 bus model in Power Factory
   - ii) Properly implement the 30 bus model in the control software and testbed

2) Implement analog reading from PMU's.
   - i) Determine whether test ports in the PMU's can be used to receive data during testing
   - ii) Connect simulator to PMU's and set up data transfers accordingly

3) Have an easy to use GUI for the remote access server.

4) Return the results from a simulation in a specified way.
   - i) Give the user specific data pertaining to their simulation

5) Offer multiple types of simulations.
   - i) Offer multiple types of systems
   - ii) Offer multiple types of attacks

Risks/Mitigation

Risk	Mitigation
One of the major risks that we currently have is doing something to the system that would make no longer functional. We are very new to this type of system and we are going to be adding a lot of new hardware which in some cases could make the old hardware no longer work.	We already have been and plan on spending a lot of time in the lab with to learn the systems. If for some reason we would connect something that would not work we always have the previous years projects to fall back to and hook everything up the way that they had it.
We are not sure if we are going to be able to use the test ports on the SEL PMU to read analog values from the OPAL-RT simulator.	This is going to be trial and error. Even if this would not work we can still read signals from the device though impact analysis will not be as accurate.
We don't know if the SEL PMU is going to be able to connect to the RTU or if it will have to connect directly to the command center.	This again is going to be trial and error. If we are not able to connect the PMU to the RTU we will be forced to connect it to the command center.
We are not sure if the back end of the remote access will be able to start up the all of the different SCADA software.	We are going to have to test the software early to find any limitations and issues that we might run into.

Table 1: Risk/Mitigation

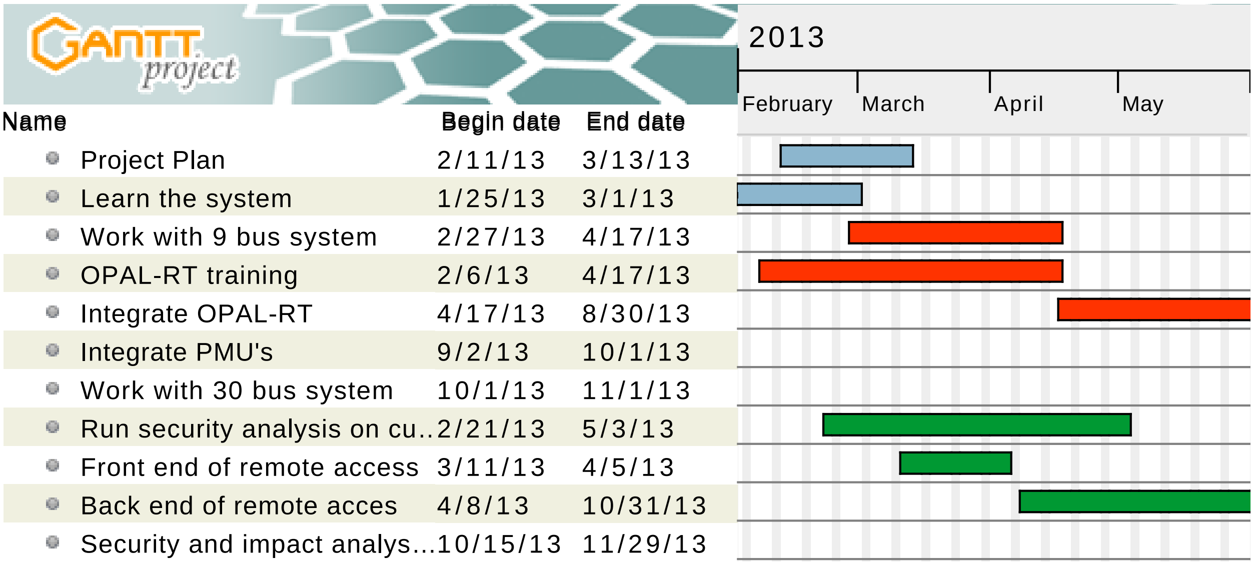
Resource Requirements

Item	Real World Cost	Our Cost
Personal Hours (550hrs)	$11,000 ($20 an hour)	$0
OPAL-RT Simulator		$0
SEL Vector Processor	$9000	$0
SEL Protection Control	$7000 (x2)	$0
RT Lab		$0
Quick Set	$1500 (x2)	$0
Total	$37,000	$0

Table 2: Budget Estimate

Work Plan

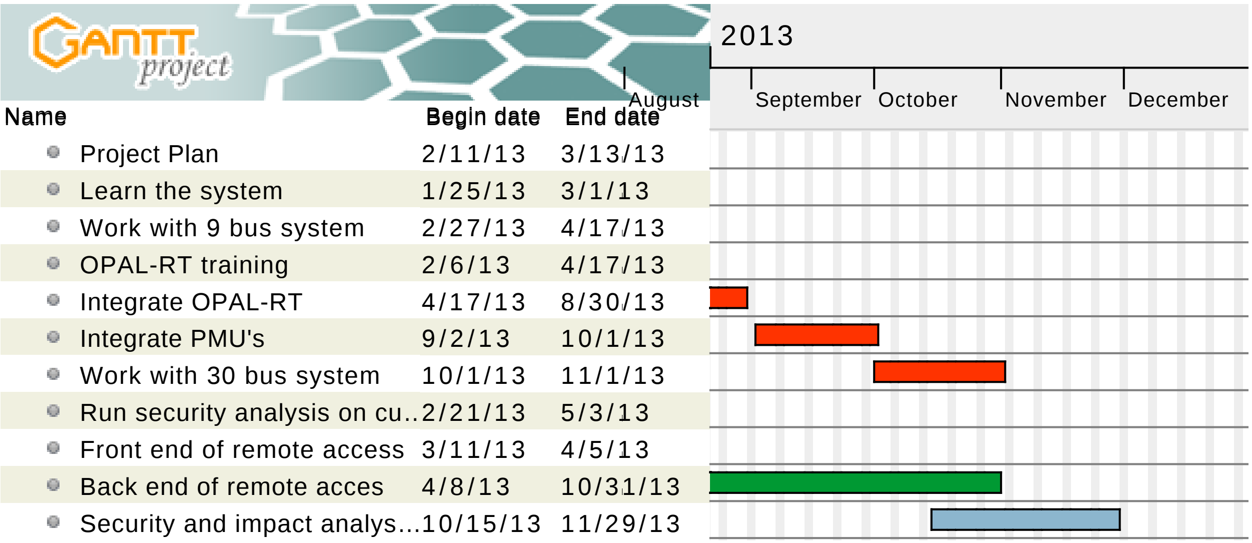
Semester 1:



Name	Begin date	End date
Project Plan	2/11/13	3/13/13
Learn the system	1/25/13	3/1/13
Work with 9 bus system	2/27/13	4/17/13
OPAL-RT training	2/6/13	4/17/13
Integrate OPAL-RT	4/17/13	8/30/13
Integrate PMU's	9/2/13	10/1/13
Work with 30 bus system	10/1/13	11/1/13
Run security analysis on cu..	2/21/13	5/3/13
Front end of remote access	3/11/13	4/5/13
Back end of remote acces	4/8/13	10/31/13
Security and impact analys...	10/15/13	11/29/13

Figure 3: Spring 2013 Work Plan

Semester 2:



Name	Begin date	End date
Project Plan	2/11/13	3/13/13
Learn the system	1/25/13	3/1/13
Work with 9 bus system	2/27/13	4/17/13
OPAL-RT training	2/6/13	4/17/13
Integrate OPAL-RT	4/17/13	8/30/13
Integrate PMU's	9/2/13	10/1/13
Work with 30 bus system	10/1/13	11/1/13
Run security analysis on cu..	2/21/13	5/3/13
Front end of remote access	3/11/13	4/5/13
Back end of remote acces	4/8/13	10/31/13
Security and impact analys...	10/15/13	11/29/13

Figure 4: Fall 2013 Work Plan

Things that are in Blue are going to be done by both the E E students and the CPR E students. Things in Red are mainly going to be done by the E E students and things in Green are going to be don by the CPR E students.

Definitions

EMS: Energy Management System

ISEAGE: Internet-Scale Event and Attack Generation Environment

PAS: Power Automation System

PDC: Phasor Data Connect

PMU: Phasor Measurement Unit

RTDS: Real Time Digital Simulator

RTU: Remote Terminal Unit

SCADA: Supervisory Control and Data Acquisition

SEL: Schweitzer Engineering Laboratories

Smart Grid: An electrical grid that uses information and communication technology to gather and act on information

Testbed: A platform for experimentation of large development projects

Citation

http://www.inl.gov/scada/factsheets/d/nstb.pdf

http://www.automation.siemens.com/mcms/industrial-communication/en/ie/industrialsecurity/scalance-s/Pages/scalance-s.aspx

http://www.backtrack-linux.org/

https://www.selinc.com/

http://www.opal-rt.com/

http://www.dhs.gov/

Some information gathered from previous senior design team May1013, May1111, May1221