Iowa State University

Cyber Security Smart Grid Testbed

Senior Design, Design Document

Dec 13 - 11

Derek Reiser

Cole Hoven

Jared Pixley

Rick Sutton

Faculty Advisor: Professor Manimaran Govindarasu

Table of Contents

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

Executive Summary

Supervisory Control and Data Acquisition (SCADA) is a type 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 continuous 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)..

The previous senior design teams have created and continuously improved upon a SCADA testbed. This includes a control center, relays, RTU's communications devices, a web server and a DTS. The goals of this year's design team is to further enhance the test bed by incorporating more relays from a different vendor, a new simulator and to also incorporate a remote access feature which will allow people to run simulations of the test bed from anywhere.

Problem

Our goal is to improve the current SCADA testbed. The previous design teams have done testing on the system that is currently in place. Once we have added in the new devices we will run the test that they have provided seeing the difference in the results from the old test be to the enhanced testbed and also run new cyber security attacks to see how the different types of relays will respond.

Operating Environment

The operating environment for the test bed is a lab in Coover Hall. The SCADA system has been an ongoing project and we are the fourth senior design team to work with and improve the functionalities of the system. A functioning testbed (Figure #) was already implemented when we began our project. We intend on expanding the system by adding a few additional components to create a more improved SCADA system (Figure #)

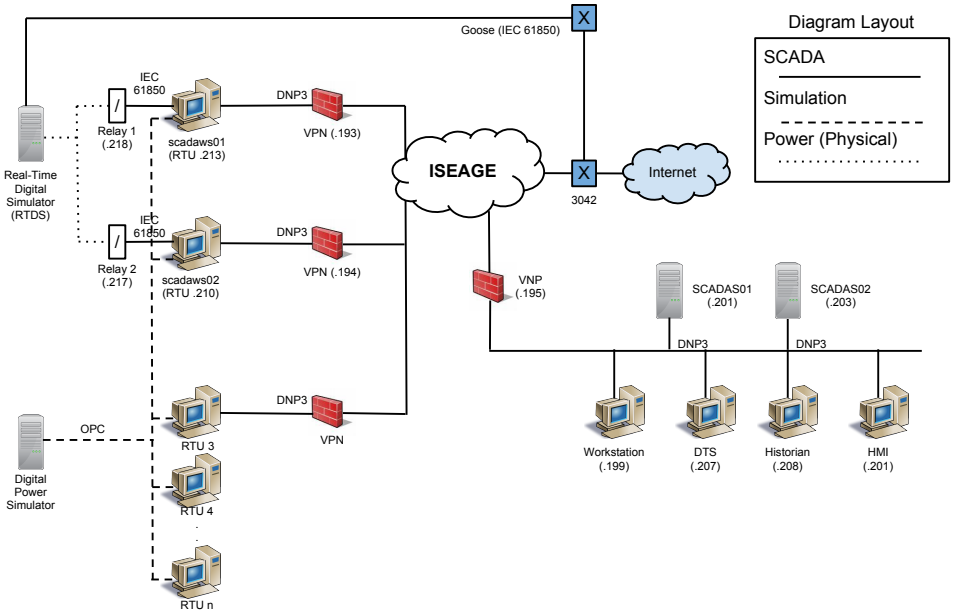

Figure 1: Current Testbed

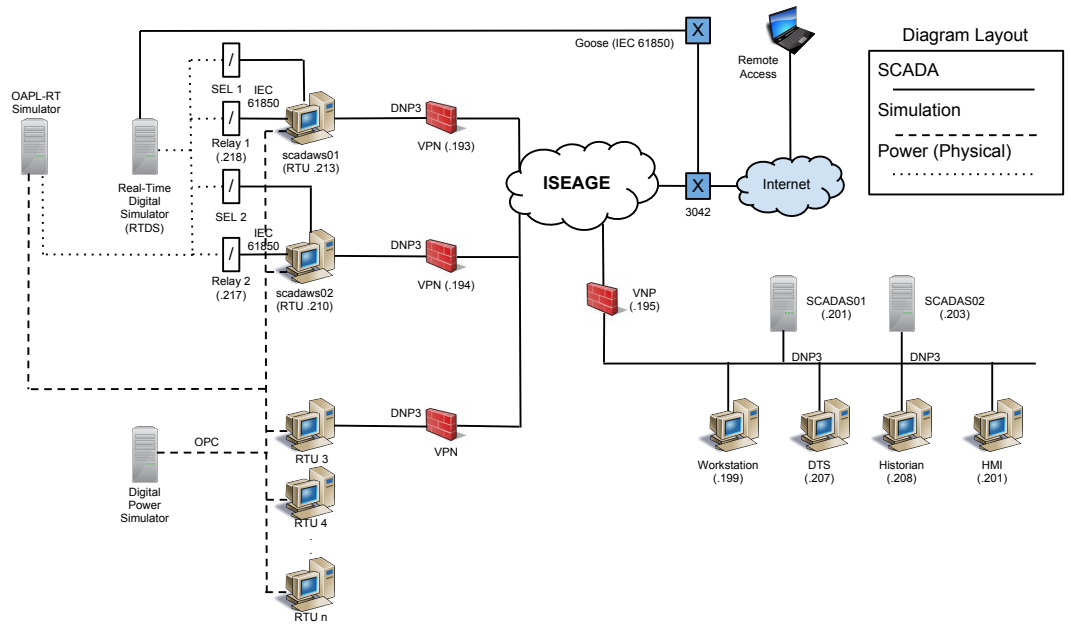

Figure 2: FutureFigure 1:

Intended Users and Uses

The primary users of this system will be graduate and undergraduate students in computer engineering or electrical engineering who are researching the cyber security of SCADA systems. Other users of this system might be researchers or companies interested in learning more about the test bed and its functionality.

The primary uses of this system will be the creating and testing of cyber-attacks and researching the effects that a cyber-attack could have on a SCADA system, especially in regards to power flow. Another use of this system might be showing people the basics of how a SCADA system works.

Assumptions and limitations

Assumptions List:

- All test equipment will function properly.
- Simulated devises function identical to physical devises
    - Such as the physical RTU's and the simulated RTU's.
- The test bed is similar to a real-world SCADA system.
    - 15 substations in the test bed will be enough to simulate a real-world system.
- Systems protocols provide the test bed system to accurately portray real-world protocols.
- The test bed will be demonstrated to those interested in SCADA systems and cyber-security.
- Industrial companies/providers are interested in vulnerabilities found through the test bed analysis.
- The test bed will be used and continuously improved upon in years to come for continuation of cyber-security attacks on a SCADA system.

Limitations List:

- We have two semesters to complete the project.
- Only 120V will be used by the relays.
    - Real-world systems exceed more than 230kV.
- Only 2 physical relays will be used due to physical, financial and time limitations.
    - Other relays will be simulated.

Expected End Product

At the end of this senior design project period, we expect to add multiple components to the current test bed. We shall integrate an Opal-RT simulator and two SEL PMU's which will enable us to more accurately analyze an attack on the SCADA system. Once the devices are properly integrated into the system, we will run multiple cyber-security analysis tests using standard nine and thirty bus systems we have created. Along with these previously stated end products, we shall set up a remote access capability to run multiple types of simulations and attacks using previously formatted demo cases.

Approach

Design Objectives

- Continue to improve the current SCADA testbed that can be used to simulate cyber attacks
    - This testbed will allow us to mimic real-world power systems and demonstrate the effects of a cyber-attack on a SCADA system.
- Add new components to the SCADA testbed
    - This will allow further attack analysis and more realistic testing scenarios.

Functional Requirements

Power System Integration

- Create a 9 bus model in Simulink for the OPAL-RT simulator
    - Creating a 9 bus model in Simulink will allow the simulator to run with the current testbed. The model will be created by adding components from the ARTEMIS and Powersim libraries in Simulink. The components will be arranged to replicate a 9 bus power system. Special blocks will need to be used to allow for the transmission and receiving of measurements to and from physical components.
- Connect the OPAL-RT simulator to the physical components in the testbed
    - Adding the OPAL-RT simulator to the testbed will consist of connecting the physical components via cables. The physical connections will allow for the transfer of data values for the measurements that are important to the testbed. Once connected successfully, the simulator will be able to be used as the central point for running real time simulations on the testbed.

- Add the PMU's to the current testbed
    - Adding the PMU'S will allow for the measurement of more data during tests. The PMU's will run alongside the current relays at the RTU stations. Connection of the test ports to the OPAL-RT simulator will give us actual voltage and current levels while running a test
- Create a 30 bus model for the OPAL-RT simulator
    - Creating a 30 bus model will allow us to run more complex tests on a larger power system. The model will be created by adding components from the ARTEMIS and Powersim libraries in Simulink. The components will be arranged to replicate a 9 bus power system. Special blocks will need to be used to allow for the transmission and receiving of measurements to and from physical components. The larger system will allow for more meaningful results as it is closer to the complex power grid systems of industry.

Cyber Integration

- Set up Remote access capabilities
    - Creating a remote access server will allow users to be able to create and run simulations without having to be in the lab, offering a variety of pre determined scenarios and attacks for the user.
- Understand the functionality of the MU Security Analyzer
    - The MU Security Analyzer is automated network security tester. This device has a selection of pre-set attacks and the ability to create custom attacks as well. Using this device for fuzz testing can allow us to discover unknown vulnerabilities in the system. Our hope it to be able to incorporate this device into the automated system as offering different types of fuzz testing and denial of service attacks.

Non Functional Requirements

Power System Constraints

- 9 bus and 30 bus models should be easy to understand
    - We want to make sure that the models created in Simulink for the OPAL-RT simulator are well organized and easy to understand. By leaving adequate spacing between components in the models and using a similar layout between the two models, users will be able to understand the models and adjust values if desired for testing.
- Connect the OPAL-RT simulator to the PMU test ports
    - This will allow for the transmission of actual voltage to the PMU's. By using actual values, more measurements can be made during operation of the testbed.

Cyber Constraints

- Have an easy to use GUI for the remote access server
    - Having an easy to use and understand GUI for the remote access server will allow users to create custom simulations without having to understand any of the other software or internal working of the network to be able to run their simulation.
- Return the results of the simulations in a specified way
    - Giving the users the results of the simulation in a way that highlights the areas that are affected will save them time and energy of reading through raw data.
- Offer multiple types of simulations
    - Offering multiple types of simulation will allow the user to run different types of attacks seeing the difference between attack types and the same attacks on different devices.

Technical Considerations

- OPAL-RT Simulator
    - Advantages
        - Already Purchased for the testbed
        - Allows for real time simulation of modeled systems
        - Can connect and work with components currently in testbed
        - Models are created in Simulink which 2 of the group members are familiar with
        - Vendor is willing to provide support as well as training on the simulator
    - Disadvantages
        - Model designs are limited due to the number of cores in the simulator
- IEC PMU's
    - Advantages
        - Already Purchased for the testbed
        - Can connect and work with components currently in testbed as well as the OPAL-RT simulator
        - Allow for the measurement of more values during testing
        - They are industry grade equipment
    - Disadvantages
        - Test ports may not be able to be used for voltage levels during testing
        - Not familiar with setup of devices

Since the OPAL-RT simulator and IEC PMU's were previously purchased for the testbed, we were not involved in the decision process. The OPAL-RT simulator was purchased due to its real time simulation capabilities as well as the fact that it will work with the current testbed. The IEC PMU's were purchased because they will work with the current testbed and are industry grade components.

Integration Testing

- 9 Bus and 30 Bus models
    - The 9 bus and 30 bus models can first be run within Simulink to check for errors. Hooking up a computer to the OPAL-RT simulator in the lab will allow us to run the models on the simulator. Once the model is running correctly, and the simulator is connected to the testbed, the models will be run on the testbed to work out issues and assure proper operation.
- OPAL-RT Simulator Integration
    - All OPAL-RT simulator testing will take place in the lab. Measurements to and from the other testbed components will need to be monitored to ensure they are being transmitted correctly. Monitoring of the model will be needed to be sure it is running correctly. At a minimum the OPAL-RT simulator will need to be able to run the same tests possible on the current testbed.
- IEC PMU Integration
    - Once the PMU's are connected to the simulator and system and are set up correctly they can be tested. By running simulations, values can be transferred to and from the PMU's to ensure proper operation.

Detailed Design

Power System Software and Equipment

- Opal-RT – Real Time Simulator (Figure 3)
    - Allows us to run and solve our simulink models through the RT-Lab software, providing a real time analysis and functionality
    - Allows for physical connection to current testbed and components gaining us access to real time data transfer and analysis with the connected comments throughout the system

Figure 3: OPAL-RT

- RT-Lab/Simulink software
    - Power system models (Figure 4) are created in Simulink using various Opal-RT block sets provided through RT-Lab software.
    - The created models are imported into RT-Lab which then runs the models on the Opal-RT simulator in a real time environment.

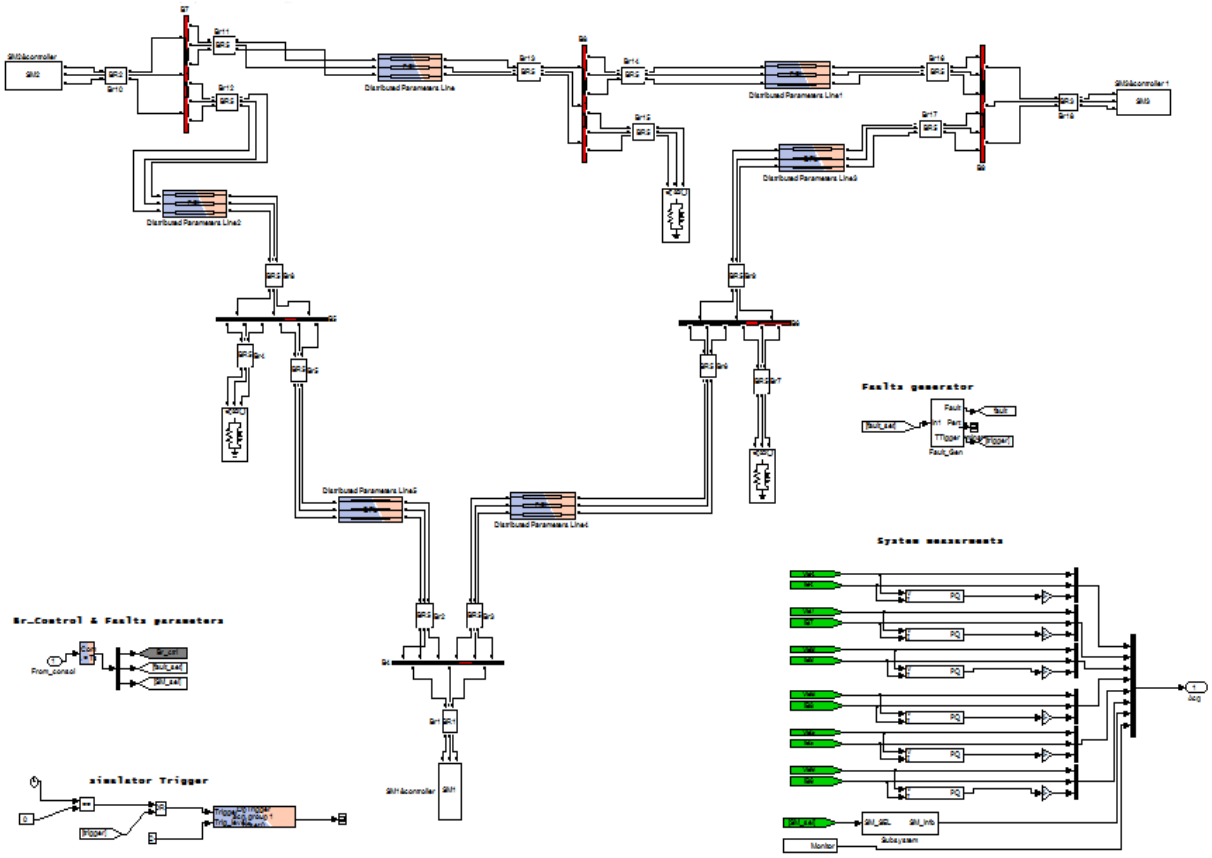

Figure 4: Simulink Model

- SEL Devices
    - SEL-421 (Protection Automation Control) (Figure 5) provides simple control of circuit-breakers and automation functions.
    - SEL-3378 (Syncrophasor Vector Processor) (Figure 6) acts as a logic engine between all of the SEL PMU's taking incoming data and sending predefined actions.

Figure 5: SEL-421

Figure 6: SEL-3378

Cyber System Software and Equipment

- Ubuntu Server
    - For our server we are using Ubuntu 12.04. This gives us a full range of utilities to access and control the different devices on the network.
- MU Security Analyzer
    - The MU Security Analyzer (MU-4000) (Figure 7) gives us the ability to run automated denial of service and fuzz testing attacks on any device on the network.

Figure 7: MU-4000

Closing Summery

The goal of the SCADA testbed is to mimic real world SCADA systems and to analyze and document vulnerabilities that the industrialized SCADA system may have. These industrial control systems are 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 continuous 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.