PROJECT PLAN

PowerCyber

Adam Daniel
Brian Forsberg
Derek Augustyn
Ian Pierce
Justin Noronha
Kanghee Lee
Yehoshua Meyer

Faculty Advisor: Dr. Manimaran Govindarasu

Dec1407

Cyber Security Smart Grid Testbed

Dec1407

Adam Daniel

Brian Forsberg

Derek Augustyn

Ian Pierce

Justin Noronha

Kanghee Lee

Yehoshua Meyer

Version	Date	Author	Change
0.1	2/23/14	All	Initial Document
1.0	4/11/14	All	Revised version
2.0	4/28/14	All	Final Revised version for Spring 14

Table of Contents

1 Current Situation

Supervisory Control and Data Acquisition (SCADA) is a type of industrial control system used to monitor and control industrial processes across the globe such as power generation, water treatment plants, oil and chemical refineries, and many other critical industrial systems. The current electrical power grid is a highly automated and complex network of various control systems, sensors, and communication networks all working together to monitor, protect, and control the grid. Due to the rapid development of the automated network and overall system, the threat of cyber based attacks are becoming more and more of a reality. These cyber attacks could create faults within the grid and potentially damage many of the smart grid elements that are essential to everyday life. Therefore, security of this smart grid, and the components housed within the grid, is one of the most important and most impatient development issues in the power industry today.

To conduct research on a physical system such as the smart grid, a PowerCyber Testbed has been developed in recent years by previous graduate and undergraduate senior design groups at Iowa State University. The testbed integrates industry standard control software with their respective communication protocols and field devices that work in combination with power system simulators to provide an accurate cyber-physical model of todays smart grid. The current testbed is composed of two physical system simulators, Real Time Digital Simulator (RTDS), and an Opal-RT simulator. It also houses various secondary devices including relays, Phasor Measurement Units (PMUs), two substations, a central command center, and a connection to ICEAGE. Continued improvement of the PowerCyber testbed will provide more accurate simulations and information about cyber vulnerability assessments, attack impact analysis, and studies of the overall cyber-physical system.

2 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.

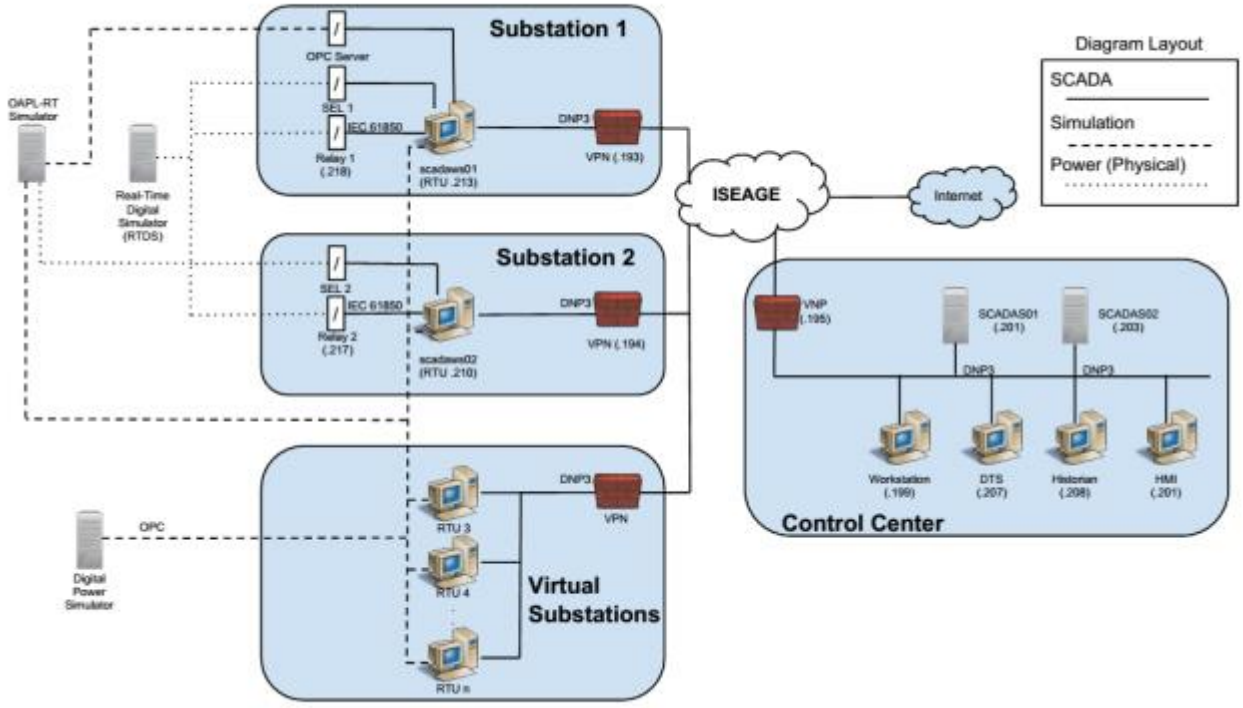
The SCADA system can be broken down into key components:

Control Center: An interface designed for human operators to view simulation data and control testbed processes.

Supervisory Station: Servers, software and stations responsible for providing communication between the Control Center and the RTU's.

Remote Terminal Unit (RTU): The RTU's in this testbed are both physical and emulated. The RTU is used to convert electrical signals from hardware sensors to digital data which is collected by the supervisory station and processed by the real-time digital simulator.

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


Substation 1
OPC Server
SEL 1
IEC 61850
Relay 1
(.218)
scadaws01
(RTU .213)
DNP3
VPN (.193)
Substation 2
SEL 2
IEC 61850
Relay 2
(.217)
scadaws02
(RTU .210)
DNP3
VPN (.194)
RTU 3
RTU 4
RTU n
DNP3
VPN
Virtual
Substations
OAPL-RT
Simulator
Real-Time
Digital
Simulator
(RTDS)
OPC
Digital
Power
Simulator
ISEAGE
Internet
VNP
(.195)
SCADAS01
(.201)
SCADAS02
(.203)
DNP3
DNP3
Workstation
(.199)
DTS
(.207)
Historian
(.208)
HMI
(.201)
Control Center
Diagram Layout
SCADA
Simulation
Power (Physical)

3 Operating Environment

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

3.1 HARDWARE

3.1.1 Siemens SCALANCE S612 Security Module

3.1.1.1 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.

3.1.2 Siemens SIPROTEC 4 7SJ61 Relay (Sensor)

3.1.2.1 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).

3.2 SOFTWARE

3.2.1 Siemens Spectrum Power TG SCADA/EMS (HMI)

3.2.1.1 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.

3.2.2 Siemens SICAM PAS v6.00 (RTU)

3.2.2.1 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.

3.2.3 Siemens DIGIS (Software for SIPROTECT Protection Relays)

3.2.3.1 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.

3.2.4 VmWare ESXi Hybervisory Operating System

3.2.4.1 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.

3.2.5 Backtrack 5

3.2.5.1 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.

4 Requirements

4.1 FUNCTIONAL REQUIREMENTS

- **Electrical Engineering Sub-Team**
    - Increase the capacity of the current Power Grid Model
        - Verify the system is functional and accurate.
        - Modify the current 39-Bus Model to communicate with the physical devices.
    - Implement a Power Protection System for the previous 39-Bus Model
    - Design a Two-Way Communications Network between Simulator, Relays, and Control Center
        - Send/Receive Commands using IEC/GOOSE Communication Protocol between Relay and Simulator
        - Transmit Simulated Analog Values to Command Center via OPC Communication Protocol
- **Computer/Software Engineering Sub-Team**
    - Discover System Vulnerabilities
        - Design and Verify countermeasures for new vulnerabilities.
    - Develop patches to previously discovered system vulnerabilities

4.2 NON-FUNCTIONAL REQUIREMENTS

- **General**
    - Improve the SEL PMU
        - Check interfacing with SCADA system.
        - Thoroughly test for vulnerabilities.
    - Expand the Capabilities of the current Cyber-Physical Environment
        - Explore more attack vectors and coordinated attack types.
        - Create an active, rather than reactive, threat detection and defense system.
    - Document past work and all future work to improve project handover time.
- **Electrical Engineering Sub-Team**
    - Simplify the 39-Bus Model and Power Protection Systems
        - Clean the model to make it “easier to read”
    - Install RT-Lab on Multiple Machines

        - Maximize workflow and efficiency.
        - Enables work to be done even while the lab is in use.
- **Computer/Software Engineering Sub-Team**
    - Ensure System Robustness
        - Withstand attacks from various types of malicious programs.
        - Physical Firmware will be secured.
    - Develop testbed framework
        - Easy to use library of known vulnerabilities
        - Develop GUI to implement individual vulnerabilities

5 Risk/Mitigation

Risk	Mitigation
One of our major risk is that we need to add a power protection system to the 39-Bus model and we have little knowledge of these protection systems.	We will be experiencing numerous errors. However, we have a graduate student who is familiar with protection systems who will support us in this area.
Since we are modifying the current 39-Bus system model to be functional and communicate with the physical devices, there is a chance of creating numerous errors within the system and the model may no longer be functional.	We have planned ahead to keep our original model so that we can always go back to the previous version when the system is hard to restore to its original state.
The primary risk is the lack of understanding of this complex system. There is little to no documentation regarding previous attack methods and mitigation.	A graduate student experienced with this system will be available in early March to walk us through the inner workings of the system. We plan on creating our own documentation as we go for future groups.
The secondary risk is potentially breaking the system to the point where it is no longer useable. This situation would warrant some level of system restore.	We will ensure a default configuration of each subsystem is stored separately. In the event of an emergency, a subsystem can be restored to its original configuration.

6 Work Plan

ID	Task Name	Start	Finish	Duration
1	Form Team	1/13/2014	1/21/2014	7d
2	Researched PowerCyber	1/20/2014	2/7/2014	15d
3	Vulnerability analysis (CprE)	1/20/2014	5/9/2014	80d
4	Learn the system	1/27/2014	2/19/2014	18d
5	Familiarize with RT-Lab and models (EE)	1/27/2014	3/5/2014	28d
6	Project Plan	2/10/2014	2/24/2014	11d
7	Develop mitigation techniques (CprE)	2/17/2014	5/9/2014	60d
8	Implement missing interfaces	2/17/2014	3/14/2014	20d
9	Cyber Physical CDC planning (CprE)	2/24/2014	5/1/2014	49d
10	Modify and clean model	3/6/2014	3/25/2014	14d
11	CPS-CDC Scenario Development	4/7/2014	5/7/2014	23d
12	Build cyber-physical system scenario (EE)	4/21/2014	6/11/2014	38d
13	Siemens Goose communication	4/21/2014	4/29/2014	7d
14	SEL Goose communication	4/28/2014	5/15/2014	14d

7 CPS-CDC

Background / Current Situation

Cyber security of the power grid - encompassing attack prevention, detection, mitigation, and resilience - is among the most important R&D priorities today. The ongoing threat to our national cyber-physical infrastructures, including Supervisory Control and Data Acquisition (SCADA) systems, demonstrates the need for professionals trained in the science, as well as the art, of cyber defense, computer and network security, and cyber-physical system protection. By leveraging Iowa State's PowerCyber testbed and the ISEAGE platform, we can provide a high-fidelity, real-time, scalable cyber-physical infrastructure to enable realistic attack-defense as a unique, first-in-the-nation CPS-CDC promoting inquiry-based learning.

Iowa State's ISEAGE has long hosted Cyber Defense Competitions. Cyber Defense Competitions are a chance to learn and teach about practical Information Assurance in a fast-paced and real-world environment. Teams of competitors are given a limited amount of time to build and secure a network that provides required services. These networks are then attacked by a team of experienced intrusion specialists whose only goal is to compromise these networks, and even bring them down. Teams are scored based upon the security of their networks, quality of their documentation, usability of their systems (as scored by competition guests on the Green Team), and their participation in other fun events during the course of the competition. (From ISU INFAS Student Group). As PowerCyber has grown over the years the interest along with the importance of SCADA systems have grown and in an effort to spread knowledge and interest in SCADA systems the CPS-CDC idea was born.

Requirements

Goals for CPS-CDC

1. Enhance knowledge of students studying cyber security to protect smart grid.
2. Develop a framework to integrate cyber-physical components into the CDC model.
3. Develop scenarios, real-time anomalies, visualizations, score board & learning modules
4. Creation and Dissemination of inquiry-based CPS-CDC modules to other universities.

Features of CPS-CDC

1. Cyber-Physical System integration
2. High-fidelity, real-time, HIL power system simulators included in CDC
3. Realistic Attack-Defense exercise: discovery of new vulnerabilities, security best practices.
4. Interdisciplinary research, education, training, outreach, and workforce development.

8 Costs

The only foreseeable cost will be those associated with setting up a backup system for the lab. However, because of external funding for this part of the senior design the overall cost for this senior design can be considered near zero.

9 Definitions

SCADA - Supervisory Control and Data Acquisition

Smart Grid - Electrical grid that uses information and communication technology to gather and act on information

Testbed - A platform for simulation of large developmental projects that cannot be experimented on in their real world/implemented versions

ISEAGE - Internet-Scale event and Attack Generation Environment

PMU - Phasor Measurement Unit

RTDS - Real Time Digital Simulator

10 Citations

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

http://www.wecc.biz/Pages/Default.aspx

http://info.deterlab.net/

http://www.nerc.com/Pages/default.aspx

http://www.ferc.gov/

Some information has been gathered from previous senior design groups Dec13-11, May12-21, May11-11, and May10-13