DESIGN DOCUMENT

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	3/10/14	All	Initial Document
1.0	4/28/14	All	Final Spring 14 version

Table of Contents

1 Executive Summary

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 urgent 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 today's 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. The goals of our senior design team is to integrate the physical devices into the existing Opal RT models, build a protection scheme for the physical models, plan a Cyber Physical System Cyber Defense Competition (CPS-CDC), and create a library of attacks, vulnerabilities, and patches.

2 Problem

Previous senior design teams have spent more time integrating components to the RTDS systems, but were not able to connect them to the newer Opal RT systems. They also did not spend much time creating any protection systems for the physical models. The EE sub team will work to remedy this situation and make the testbed more accurate to a modern SCADA Smart Grid system.

Previous groups were able to run simple cyber attacks and find a handful of vulnerabilities, however they were unable to find any patches for these vulnerabilities. They also did a poor job of compiling and documenting their work. Our group will work to find the same vulnerabilities previous groups found, find any additional ones, and create a library of all attacks run, vulnerabilities found, and patches created.

Previous groups were also pitched ideas for a Cyber Physical System Cyber Defense Competition (CPS-CDC), but because they lacked the necessary resources and man power this idea was put on the back burner. This semester since we have a team of seven seniors, three Electrical, three Computer, and one Software engineer, this idea has been brought to the top of the CprE team goal list. The team will work through setting up project plans, and design documents to help set up this CPS-CDC next fall.

3 Operating Environment

The PowerCyber testbed operating environment is located in Coover Hall. We are the fifth senior design team to work on and improve the SCADA system. The functioning PowerCyber testbed was already implemented when we began our senior design project. We intend to expand the system by adding a few additional components in an effort to improve the PowerCyber testbed.

4 Intended Uses and Users

The primary users of the PowerCyber testbed will be the graduate and the undergraduate students in computer engineering or electrical engineering who are researching cyber security of SCADA systems. This also includes those students who are enrolled in Seminar in Computer Engineering, CprE 592. The possibility of other users exist and could include other researchers or companies that are interested in the cyber security of SCADA systems or learning more about the PowerCyber testbed and its functionality.

The primary use of the PowerCyber testbed is the creation and testing of cyber-attacks, mitigation of those cyber-attacks, and researching the effects that cyber-attacks have on a SCADA system, focusing mainly on power flow. The PowerCyber testbed also serves as a learning module for SCADA systems.

5 Assumptions and Limitations

Assumptions

- All systems are working properly - SCADA control system, switches, RTS model, etc.
- Virtualized devices will function exactly like physical devices
- Integration of SCADA environment with ISEAGE CDC is feasible
- Systems protocols provide the testbed system to accurately portray real-world protocols
- Testbed will be used and continuously improved upon in years to come for continuation of cyber-security attacks on a SCADA system
- All PMUs and relays are capable of communicating with the Opal-RT physical models

Limitations

- We have two semesters for this project
- Only two physical relays and two PMU units are available
- Documentation from previous groups is minimal and hard to find

6 Expected End Product

By the end of the fall 2014 semester here at Iowa State we expect to integrate the physical devices into the 39 bus Opal RT model, implement a wide area protection system on the model, and possibly create a new larger 54 bus model. We shall run various attack scenarios on the new physical model and analyze the outcomes to make the protection system work more efficiently. Since our senior design group is divided into two sub-teams, electrical engineering (EE) and computer engineering (CprE), the EE sub-team will mainly focus on the physical models and protection, while the CprE sub-team will develop cyber-attacks, find vulnerabilities, and fix the vulnerabilities, if possible. They will also be working very hard on setting up a Cyber-Physical System Cyber Defense Competition (CPS-CDC). In the end, the whole system will be integrated together as a whole, possibly patched, and communicating with every part of the testbed. This will allow for full simulations of cyber-attacks and their impact on the physical models.

7 Approach

Design Objectives

- Expand the current SCADA testbed to incorporate a larger power system model and apply a protection system on it
    - This will allow us to have a more realistic and accurate testbed to compare to real-world power systems
- Incorporate all physical devices into the cyber-physical system scenario which will be used to simulate cyber attacks
    - This will allow us to demonstrate the effects of a cyber-attack on a SCADA system and allow us to implement the physical units within a protection scheme
- Create attack scenarios and discover new vulnerabilities
    - This will allow further attack analysis and more realistic testing scenarios
- Implementing patches and intrusion detection systems
    - This will allow us to run all hacks from a central framework that can share resources and allow multiple attacks at once on different parts of the network

8 Functional Requirements

- 39 Bus Model for OPAL-RT
    - Understand all functions of the model, how it works, and how to manipulate the model. This enables us a group to make changes to the model quickly and provide any sort of demonstrations of the PowerCyber testbed as a whole.
- Simulator Relay Communication Systems
    - Integrate the physical devices into the existing Opal-RT 39 bus model so we can create a tangible protection scheme using the existing devices. This will enable the testbed to be modeled as a more realistic simulation of the smart grid.
- Power Protection Control Systems
    - Autonomous attack mitigation will utilize the physical devices to isolate certain areas of the testbed depending on current conditions in the physical testbed and within the simulation model. This will mitigate damages caused by an attack and discourage further attacks.
- CPS-CDC
    - Includes Learning Modules
        - Provide documentation and guides for participants in the CPS-CDC who are not familiar with power grid security. This will include SCADA software topics for EE students and power grid topics for CprE/SE students.
    - Exploitable CPS
        - For this competition to work, there must exist viable attack vectors for red team to exploit. We will manually punch holes in the substation software before it is distributed to the teams if the inherent security flaws are not enough.

9 Non-Functional Requirements

- 39 Bus Model for OPAL-RT
    - Well documented and maintainable by subsequent groups
    - Clean and easy-to-read model
    - Calculated reference angle on generator rotors
- Simulator Relay Communication Systems
    - Devices configured for multiple profiles
- Power Protection Control Systems
    - Use of multiple types of protection
- CPS-CDC
    - Portable
        - Other Universities must be able to host their own CPS-CDC events without specialized power systems hardware (OPAL-RT, relays, PMU's).
    - Scalable
        - Design must consider resource constraints for when the CPS-CDC expands. A virtualized environment is much cheaper to scale up than one which requires a relay and PMU for each substation.
    - Maintainable
        - All security holes in the CPS must be well documented and replicable. This documentation be used as a reference by those working on the CPS-CDC and also subsequent teams who research smart grid security.

10 Technical Considerations

ISEAGE - a cluster of nodes which are capable of simulating an arbitrary, reconfigurable, static routing topology that is abstracted away from the physical hardware

- Contains a suite of tools to research internet-scale cyber security events in a controlled environment
- *ISEFLOW* - The core of ISEAGE
    - Routes packets between the flows to ensure proper delivery
- *ISEBOX* - A portable version of ISEAGE
    - the virtual implementation of an ICLE
    - Consists of a high-powered server running the VMWare ESXi operating system

ICLE - the backbone of ISEAGE, simulating the routing infrastructure of arbitrary networks.

11 Integration Testing

- 39 Bus Model
    - The current model needs to be updated with a new excel input file that will enable us to expand the capabilities and realism of the simulation. Once we are able to configure the model's Inputs and Outputs we will be able to start work on implementing a two-way data stream between the simulator and the other components of the SCADA environment.

- Simulator-Relay Communication System
    - This system will open a direct pathway between the Opal-RT Simulator and the various Siemens and SEL Relays that we have in the SCADA environment. Specifically so that the simulation will be kept 'In-the-Loop' and will be able to actually send out commands itself to mitigate any problems that may occur in the Power Grid. Thus increasing the realism and utility of the simulator, while enabling the design and integration of Protection Control Systems.

- Power Protection Control Systems
    - Using the two-way communications we can now implement control systems that will be able to mitigate the impact of attacks autonomously. We already have access to measurements on almost every part of the Grid so we can take that information, such as the voltage, current, and phase on any line or generator and use it to detect issues. Once an issue has been detected we will then have systems in place that will be able to take the necessary action in order to reduce damage to the system. Since instability in one component of the Grid can spread to other parts if nothing is done then it can lead to widespread instability and even a blackout. Thus using Protection Control Systems we can isolate problem sectors from the rest of the Grid as quickly as possible and prevent unnecessary damage.

12 Detailed Design

Power System Software and Equipment

- Opal-RT – Real Time Simulator
    - Allows us to run and simulate our Simulink models through the RT-Lab software.
    - Provides us with a real time analysis of the physical models
    - Allows for a physical connection to the current test-bed and components that give us access to the real-time data transfer and analysis with the connected components of the system
- 39 Bus Model
    - In order to improve on the current test-bed, we are using a 39 bus model
    - Simulator Relay Communication System
        - Integrating the physical device into the existing 39 bus model will allow us to create a tangible protection scheme.
- RT-Lab/Simulink software
    - Power system models are created in Simulink using various Opal-RT block sets provided through RT-Lab software and a Microsoft Excel spreadsheet to populate the model
    - The created models are imported into RT-Lab which then runs the models on the Opal-RT simulator in a real-time environment

Cyber System Software and Equipment

- Computer Systems
    - Most of our interaction with the system has been completed with an Alienware laptop that has all the necessary software provided by the lab and configured by previous teams
    - A VPN is being setup to allow remote access to the lab so that the vulnerabilities can be tested from outside of the lab as well
- Virtual Machines
    - We are setting up virtualized environments that should allow for anyone in the lab to get to work quickly using vmware clients

- CPS-CDS
    - We are also using the virtual machines as individual learning modules for the scenarios that will be proposed for the teams joining the CPS-CDC

13 Closing Summary

The PowerCyber Lab is a SCADA testbed that is capable of mimicking a real-world SCADA system. It allows us to find, analyze, and document vulnerabilities of the physical devices in the testbed and within the simulated model. We are also able to attempt to patch these vulnerabilities and fix them in any way possible as well as notifying manufacturers of these vulnerabilities. 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. There needs to be a system in place to protect these systems from cyber-threats as these systems are used to monitor and control the industrial processes in the world, including but not limited to, power generation, water treatment, oil and natural gas, security systems, and lake/river dams around the country. Due to the continuous development of this automated network the cyber-threat is becoming more and more real each day. Setting up a system that can emulate and test a real-world scenario is crucial today more than it ever has been.

14 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

CPS-CDC - Cyber Physical System, Cyber Defense Competition

Opal-RT - Software, hardware, and target node used for real time simulations

VMWARE - Software that allows for virtualization of operating systems.

GOOSE - Generic Object Oriented Substation Events that utilizes the IEC 61850 and OPC 61850 protocols