Iowa State University

CPS-CDC & PowerCyber Testbed

Senior Design Final Document

Derek Augustyn

Adam Daniel

Justin Noronha

Yehoshua Meyer

Kanghee Lee

Brian Forsberg

Faculty Advisor:

Dr. Manimaran Govindarasu

Graduate Students:

Aditya Ashok

Pengyuan Wang

Table of Contents

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

ISERink - Deployable version of ISEAGE.

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.

ESXi - Is a type-1 hypervisor developed by VMware for deploying and serving virtual computers.

myDAQ - National Instruments (NI) Data Acquisition device used to interact with myGrid board.

myRIO - NI Re-programmable I/O device with wireless networking capabilities.

myGrid - Smart grid visualization tool used to simulate power generation, transmission, and distribution loads.

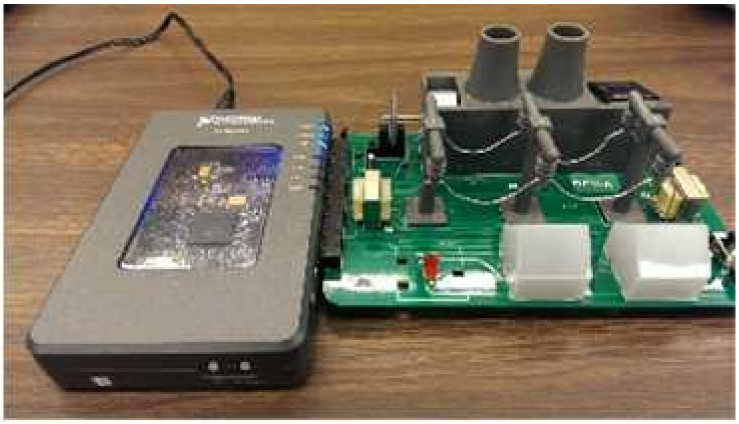


Figure 1: myRIO and myGrid

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, a connection to ICEAGE, an EXSi Server and Client housing ISERink, and various NI devices and equipment. 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. Our team goals are to lay the groundwork for a Cyber Physical System-Cyber Defense Competition (CPS-CDC) while providing proof of concept of the CPS-CDC layout, incorporate the physical devices within the lab into the existing Opal RT models, and integrate NI equipment and myGrid board to the lab and ISERink as a visualization tool for a CPS-CDC.

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 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 and never amounted to more than an idea. This year 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. The EE team has also been involved with this project the second semester working to integrate some new NI equipment into the competition as a visualization tool for competitors.

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 testbed. The functioning PowerCyber testbed was already implemented when we began our senior design project. We will expand the system by adding a few additional components in an effort to improve the PowerCyber testbed and add CPS-CDC functionality through the use of ISERink.

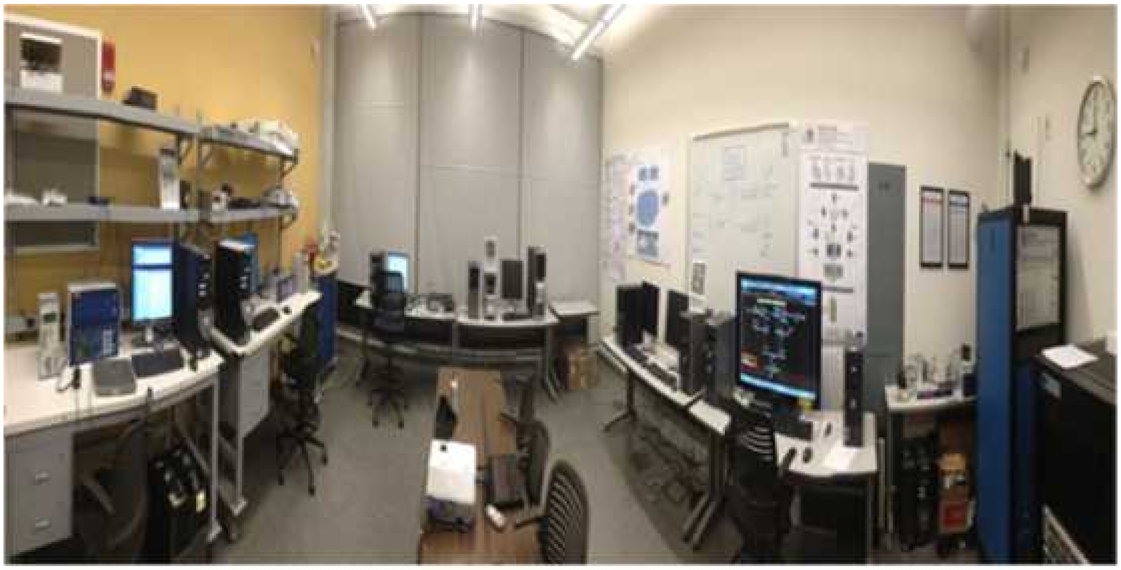


Figure 2: PowerCyber Lab

Intended Users and Uses

The primary users of the physical 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 does exist and could include 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. It will also serve as the hosting place for a CPS-CDC here at Iowa State that will incorporate both the physical lab and virtual machine hosted on an ISERink server within the lab.

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
- ISERink can be quickly and setup on a new server within the lab
- 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
- Hardware for ISERink. Initially we did not have hardware that was compatible for running ESXi which is what is used to run ISERink.

Expected End Product

By the end of fall 2014 semester at Iowa State we expect to integrate the physical devices into the 39 bus Opal RT model, and lay the groundwork for and provide proof of concept for CPS-CDC. 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 model tie ins and working with the new NI equipment for use within the CPS-CDC, while the CprE sub-team will be working to set up a CPS-CDC. In the end, the whole system will be integrated together as a whole and communicating with every part of the testbed. This will allow for full simulations of cyber-attacks and their impact on the physical models, as well as integration into a CPS-CDC that will utilize both physical devices within the lab and the virtual machine housed in the ISERink server.

Approach

Design Objectives

- Incorporate all physical devices into the simulated power system model, which will be used to analyze 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
- Integrate newly acquired NI equipment into lab and the CPS-CDC
  - This will allow for a nice visualization tool for the CPS-CDC competitors
- Design a standard implementation for scenarios
  - Scenarios should always include
    - Substations and relays
    - Communication Center
    - Attack objectives for Red Team
    - Design objectives for Blue Team
    - Test cases for Green Team
- Design a variety of CPS-CDC scenarios with increasing difficulty
  - This will allow other schools to quickly start their own CPS-CDC that fits their setup
  - This will allow modules to easily be added to the CPS-CDC
- Incorporate the PowerCyber components into ISERink.
  - This will allow the CPS-CDC to actually become a reality and easily deployable to other schools and organizations

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 as 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.
- Network connectivity of NI equipment
    - Integrate newly acquired equipment into the lab and ISERink through use of the already set up network. This will allow us to control the myGrid board and provide competitor visualizations as well as adding another physical device into the CPS-CDC.
- 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.

Non-Functional Requirements

- 39 Bus Model for OPAL-RT
    - Calculated reference angle on generator rotors
    - Clean and easy-to-read model
    - Easily maintainable by subsequent groups
- Simulator Relay Communication Systems
    - Devices configured for multiple profiles
- 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

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.
- ISERink - Collection of virtual machines that ISEAGE runs on top of.
- ISEMaker - Instructions for setting up one’s own instance of ISEAGE.

Physical Model Updates

- 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.

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
- NI myGrid, myRIO, & myDAQ
    - The myGrid board serves a perfect utilization tool for CPS-CDC that mimics an actual electrical grid with transformers, generation, transmission, and distribution
    - The myRIO is a re-programmable I/O device with wireless connectivity features that will serve as the communication device between the myGrid and the controlling LabVIEW program.
    - The myDAQ is a data acquisition device for which the myGrid board was designed to talk to, but was eliminated as it requires a physical connection to LabVIEW.

Cyber System Software and Equipment

- Computer Systems
    - Most of our interaction with the system has been completed with an PowerCyber host 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

Standards

- DNP3 (Distributed Network Protocol)
    - IEEE Std. 1815-2010
    - Set of communication protocols that is used between components in process automation systems.
- RDP (Remote Desktop Protocol)
    - ITU Telecommunication Standardization Sector T.T.128
    - To allow the Red (attackers) team to access any open ports on the blue network.
- VPN (Virtual Private Network)
    - A vulnerability is exposed in the blue teams system to allow a private network between the different subsystems in ISERink
- OPC UA (OLE for process control, Unified Architecture)
    - Successor to OLE for process control (OPC)
    - Improved upon the previous iteration with cross-platform support and Server oriented architecture.
    - Developed by the OPC Foundation
- IEC 61850 (GOOSE)
    - IEC Technical Committee 57
    - A reference architecture for electric power systems.

- ○ Used to communicate and trip physical relays in the lab.

Implementation

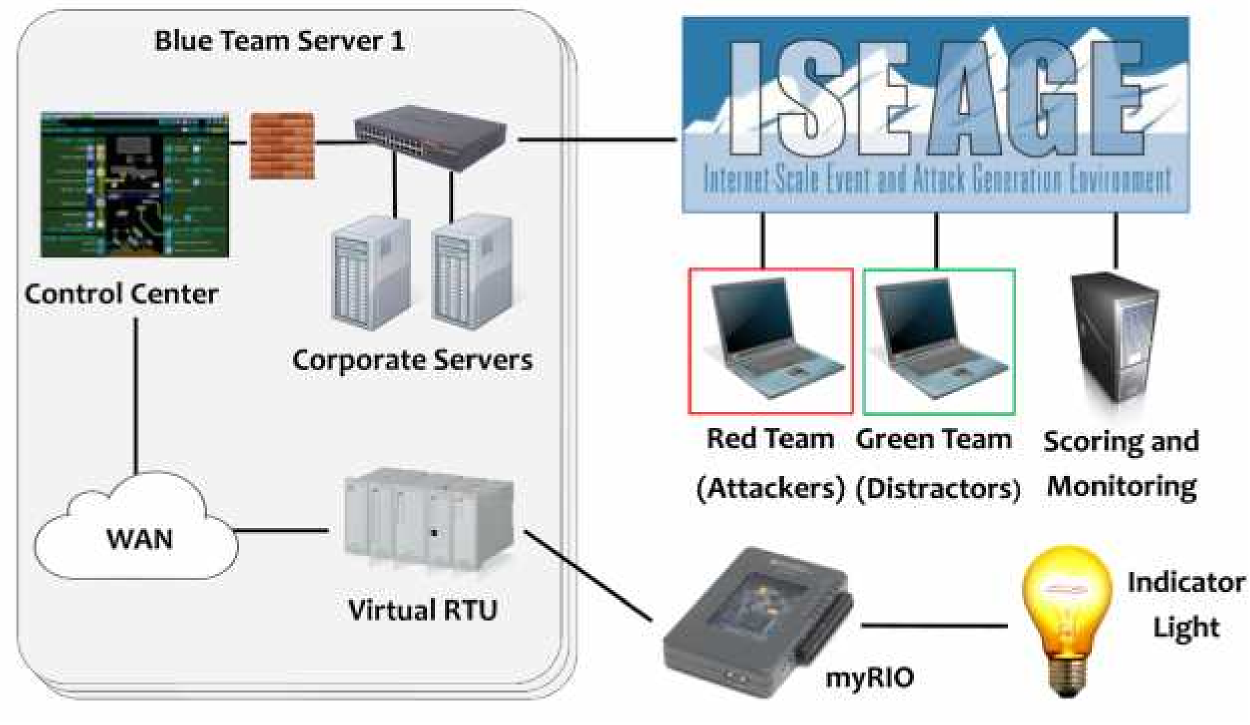


Figure 3: CPS-CDC Overview

In order to implement our project from a global level, we first needed to access the current CDC setup from ISEAGE. We spent the first few months of our project working on understanding the internal workings of the CDC systems through the ISEAGE environment. We worked with the lab to determine how and what we would do differently in our setup.

A current student working in the ISEAGE lab is currently working on virtualizing the entire lab into a platform called ISERink. We decided to use this virtualized environment for our purposes as it will be the most scalable and would allow us to completely replace the components for the blue team (the defending team). Everything else in the system was to stay almost the same, with the slight exception of some networking routes for the new network.

In order to implement our CPS-CDC event a university would basically follow the same setup instructions as the ISEAGE lab currently has available for the regular CDC event. In order to hook up the Cyber Physical System component, all that needs to be done is to replace the blue VM with a set of VMs running the SCADA control center.

The CDC ISERink environment runs on top of the VMware ESXi server. We had to install a server to a spare desktop in the lab and then upload the VMs provided to us by the ISEAGE lab. There was some tweaking that needed to be done to get computers in the PowerCyber lab to communicate properly. This is now a part of the VMs that are provided to build the ESXi server.

Testing

The procedure for testing our environment consists of several steps. The first step is to ensure all VMs on the network are connected to each other. If the VMs can each ping one another, then they are connected. The next step is to test that the SCADA applications on each of the PowerCyber VMs are communicating properly with the relay. If this is true, then the status icons in the Siemens substation operation software will all be green, and the relay is able to be tripped from the control center. After all of these connections are established, the final test is a proof of concept CPS-CDC attack scenario. VPN into the control center from a different VM that's connected through ISEAGE. If the relay can be tripped through the VPN, then the CPS-CDC infrastructure is working.

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.

Appendix I: Operations Manual

To Connect Login into vCenter

1. Launch vCenter
2. Enter IP Address / Name of ESXi server
3. Enter user name and password and select “Login”
4. vCenter will now launch into usable state

For more information on operating ESXi along with vCenter reference the GitHub repository for ISEMaker.
https://github.com/bvermeer/ISEAGE_Documentation

To Launch Virtualized SCADA Environment

1. Launch VMWare
2. Power on “substation”, “scada01”, and “scada02” virtual machines
3. In the VMWare settings, check to make sure each VM is bridged to the physical network
4. On “substation”, open SICAM Operation software

To Login to Control Center

1. Launch “Host Control” on the desktop of scada01
2. Select “Start Workstation”
3. At the login screen
    a. Press F9
    b. Type “scada”
    c. Press tab
    d. Type “siemens”
    e. Press F10

Appendix II: Iterations

Physical Devices - myRIO/myGrid

National Instruments (NI) - myGrid - myDAQ:

Our first iteration was to physically connect the myGrid to the myDAQ to the host computer (Figure 1) because this is how the myGrid was originally designed to be used.

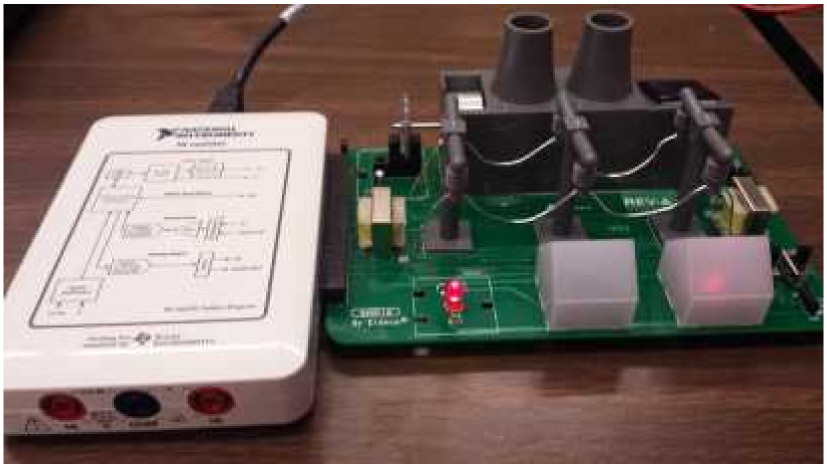


Figure 1: myDAQ - myGrid

The next iteration was to send the data from myGrid to the myDAQ to the myRIO since the RIO device has wireless functionality. However, we realized that this would not work properly because the pins could not be used by two devices at the same time.

To remedy this situation, we directly connected myGrid to myRIO (Figure 2) because the pins of the myDAQ and myRIO were interchangeable, and we were able to take advantage of the myRIO's wireless capabilities. However, this iteration didn't go as smoothly as we expected. Our major issue was that the myGrid was not able to receive enough voltage from the myRIO to light up the LED's.

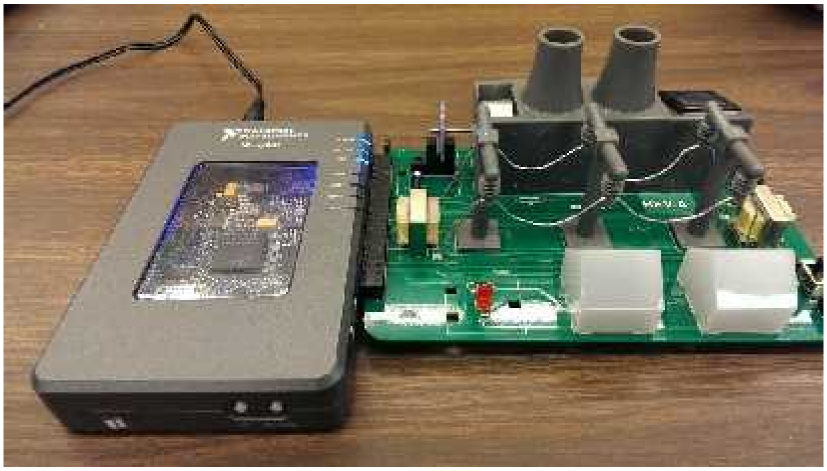
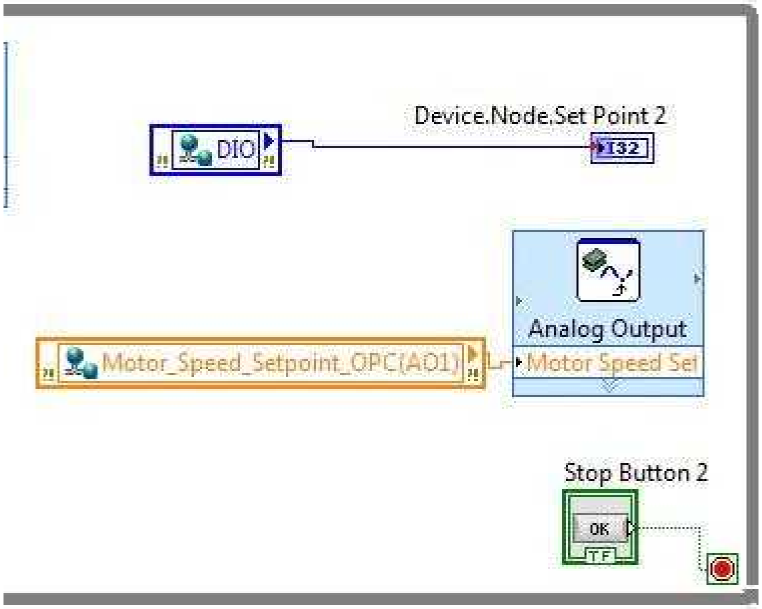


Figure 2: myRIO - myGrid

OPC Communications

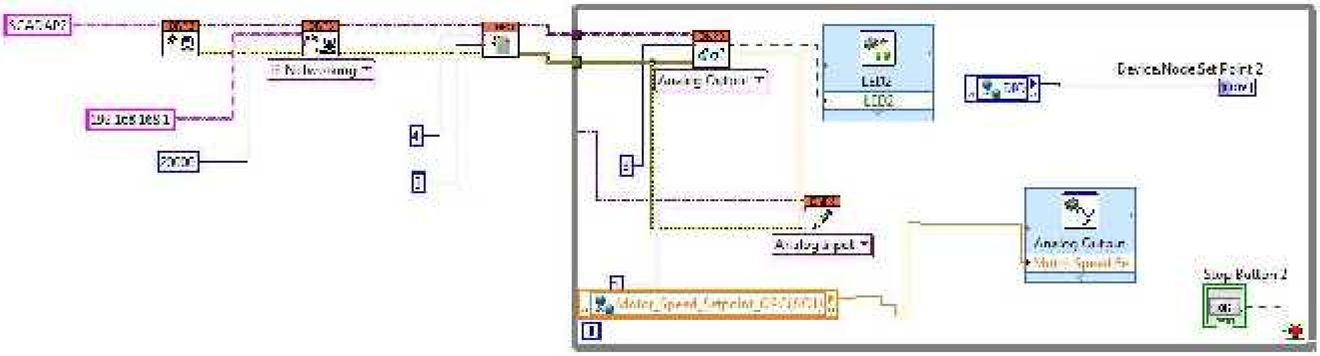
National Instruments (NI) - Shared Variables:

Our first iteration of the OPC network made use of the built in ‘Shared Variables’ feature of LabView. This system was extremely easy to setup and understand since the Shared Variables implemented the communications setup automatically. All you had to do was drag and drop the variable block into the block diagram and wire it to the component you needed. This simplicity inherently led to problems as you would need NI software installed in order to view the contents of the Shared Variable. Because we needed the communications to be easily deployable for other universities, this was unacceptable. So we scrapped that method and moved on to more complex industrial communications protocols.



DNP3 Protocol:

The second iteration we built utilized the DNP3 communications protocol that is used in industry worldwide. This would allow our network to be easily deployable since all you would need to access the variable is its IP address. Once we constructed the block diagram in LabView we had issues establishing a connection, and after a lot of research we found that the myRIO did not support DNP3 communications. So in order to retain the deployability of the system we moved to our third revision, OPC UA.



OPC Unified Architecture (UA):

The third and final version of our communications setup was assembled using OPC UA. This enabled us to have the communications function on the myRIO as well as being easily deployable. All you needed to access the data on the RIO was its IP address. Thus this method had the benefits of both the previous iterations combined, making it easily the best choice for our network configuration.