# Dec14 - 07

PowerCyber Testbed

# Our Team

Derek Augustyn - Project Dictator
Adam Daniel - Webmaster
Shuky Meyer - CprE Team Lead
Justin Noronha - EE Team Lead
KangHee Lee - Key Idea Holder
Brian Forsberg - Key Idea Holder

Dr. Manimaran Govindarasu - Advisor/Client

# Problem Statement

- Today's electrical smart grid is a highly automated and complex network
  - Comprised of various sensors and communication abilities to monitor, protect, and control the grid
- Cyber security is becoming a major concern due to the rapid development of this network and the IEDs within
- Realistic testing for cyber-physical scenarios cannot be done in the field
- To remedy this, we combine the PowerCyber testbed and the ISEAGE platform to create a first of its kind Cyber Physical System Cyber Defense Competition (CPS-CDC)

# Why CPS-CDC?

- Gather interest and concern for utility systems among students
- Enhance knowledge of students studying cyber security to protect smart grid
- Develop mitigation strategies for SCADA systems
- Crowdsource possible attack vectors gained by participating students


Source: https://cdc.iseage.org/

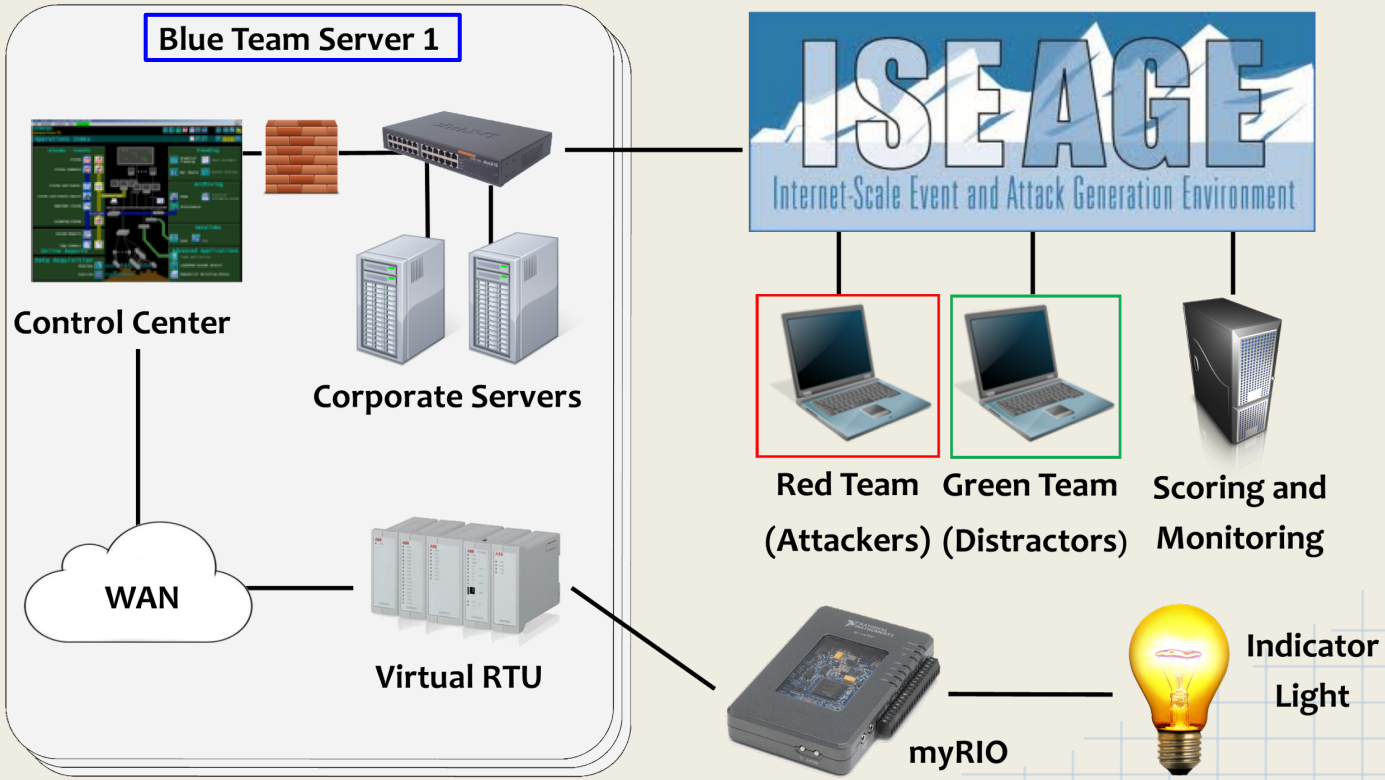
# Functional Requirements

- Gain and learn to use National Instruments myDAQ, myRIO, and myGrid
- Utilize myRIO to control myGrid board
- Develop attack scenarios for the competition
- Setup virtualization environments for CPS-CDC simulations
- Integrate National Instruments equipment into PowerCyber Lab, ICERink, and CPS-CDC

# Non-Functional Requirements

- Document all work to improve project handover time
- CPS-CDC should be scalable and portable
- Develop learning materials to quickly immerse students in SCADA systems
- Reverse-Engineer old myGrid backend to function normally

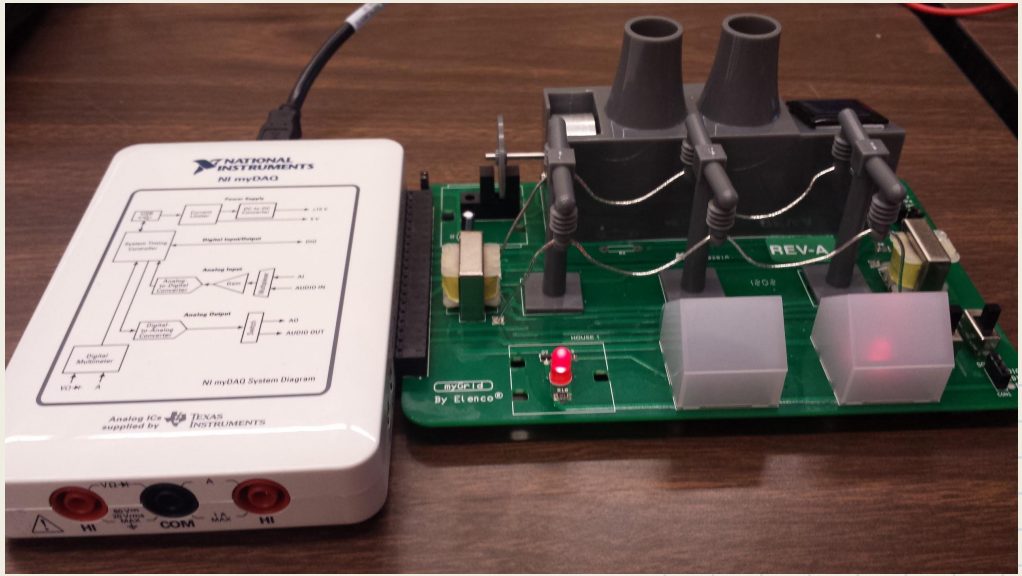
# Competition Layout

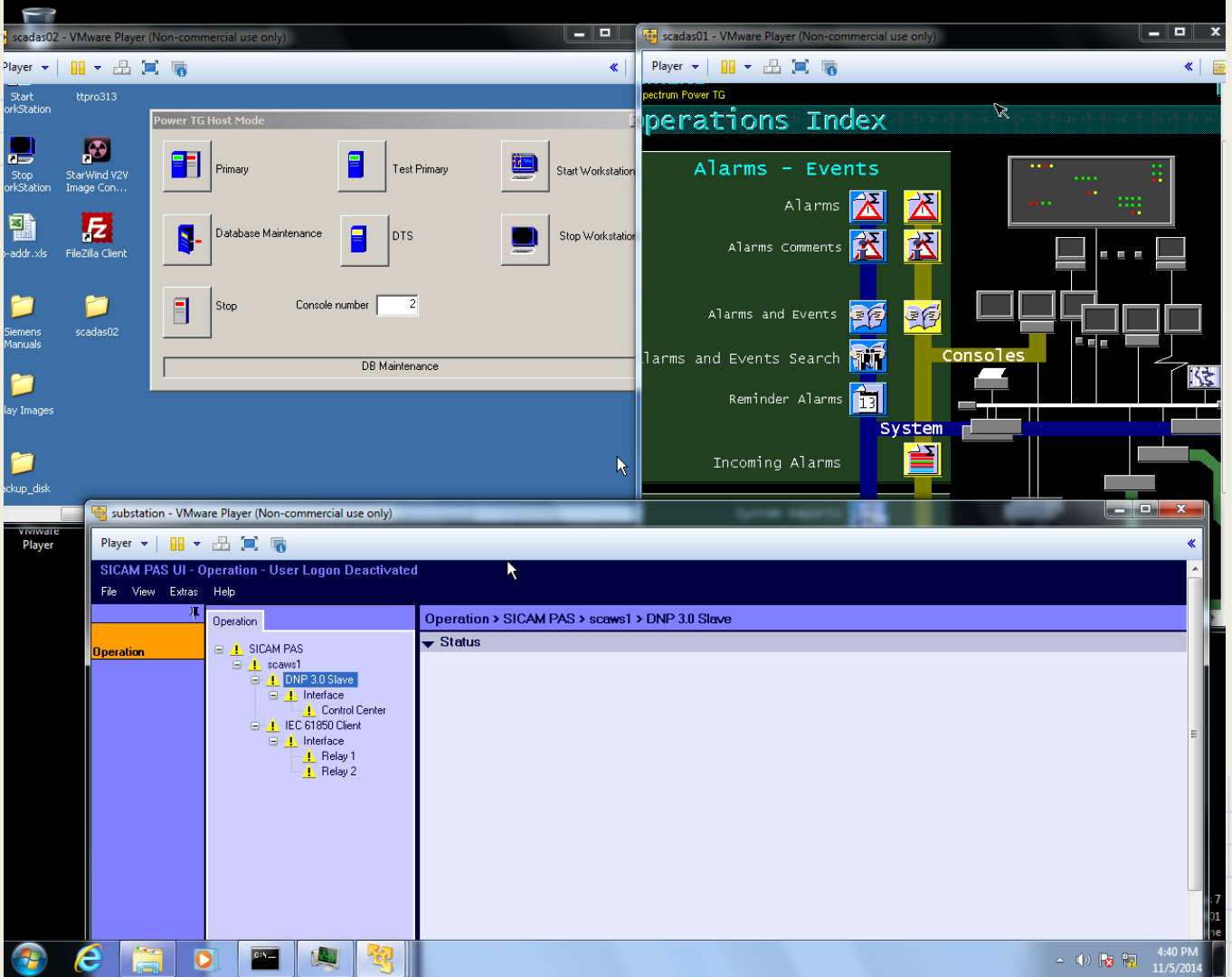


# Equipment

- myRIO


- myDAQ and myGrid




scadas02 - VMware Player (Non-commercial use only)
Power TG Host Mode
Primary
Test Primary
Start Workstation
Database Maintenance
DTS
Stop Workstation
Stop
Console number
2
DB Maintenance
scadas01 - VMware Player (Non-commercial use only)
Operations Index
Alarms - Events
Alarms
Alarms Comments
Alarms and Events
Alarms and Events Search
Reminder Alarms
Incoming Alarms
Consoles
System
substation - VMware Player (Non-commercial use only)
SICAM PAS UI - Operation - User Logon Deactivated
File View Extras Help
Operation
SICAM PAS
scaws1
DNP 3.0 Slave
Interface
Control Center
IEC 61850 Client
Interface
Relay 1
Relay 2
Operation > SICAM PAS > scaws1 > DNP 3.0 Slave
Status
4:40 PM
11/5/2014

Dec14-07

# Design-Virtualization

- For the CPS-CDC to be portable and scalable, we need to virtualize our current SCADA testbed.
  - CDC teams need to be able to control a variable number of VMs, depending on the scenario
  - These VMs must be able to bridge to the physical network
  - VMs also must be able to communicate with physical relays
- We need to have an environment similar to CDC
  - We will utilize ISEAGE and add a Cyber Physical component to it
    - Internet-Scale Event and Attack Generation Environment
  - Needs to connect to the PowerCyber network

# Iterations

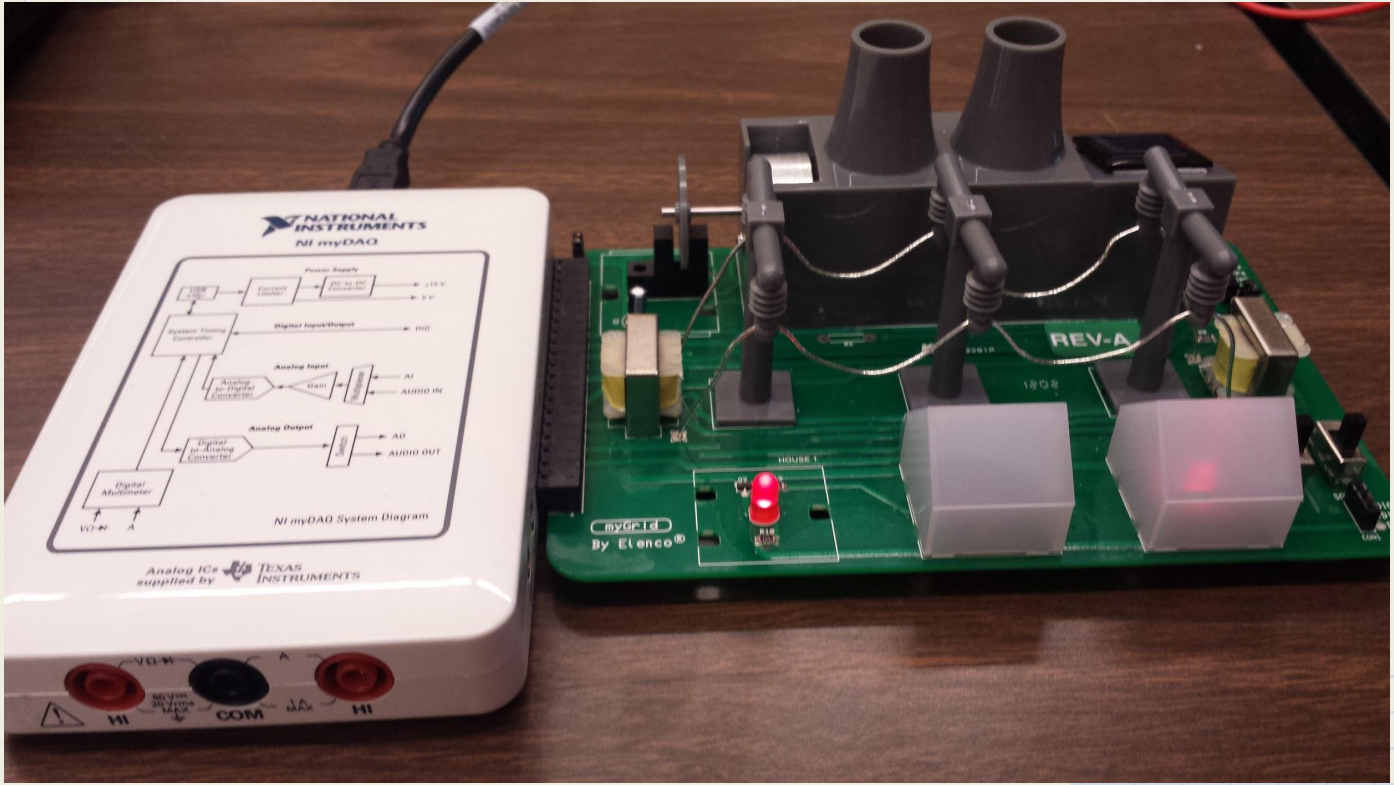
- VMware ESXi
  - hostd issues in our configuration of ESXi
    - Used a pre-built ISERink instead

- Virtualized SCADA Environment
  - Control Center originally installed by Siemens employee and we cannot reinstall by ourselves.
    - Virtualized the instance installed by Siemens in the lab
  - Multiple subnets in lab and preconfigured with ISERink affected communication between RED team and virtualized environment
    - Hard-coded IP configuration
    - Reconfigured ISERink subnets to allow communication

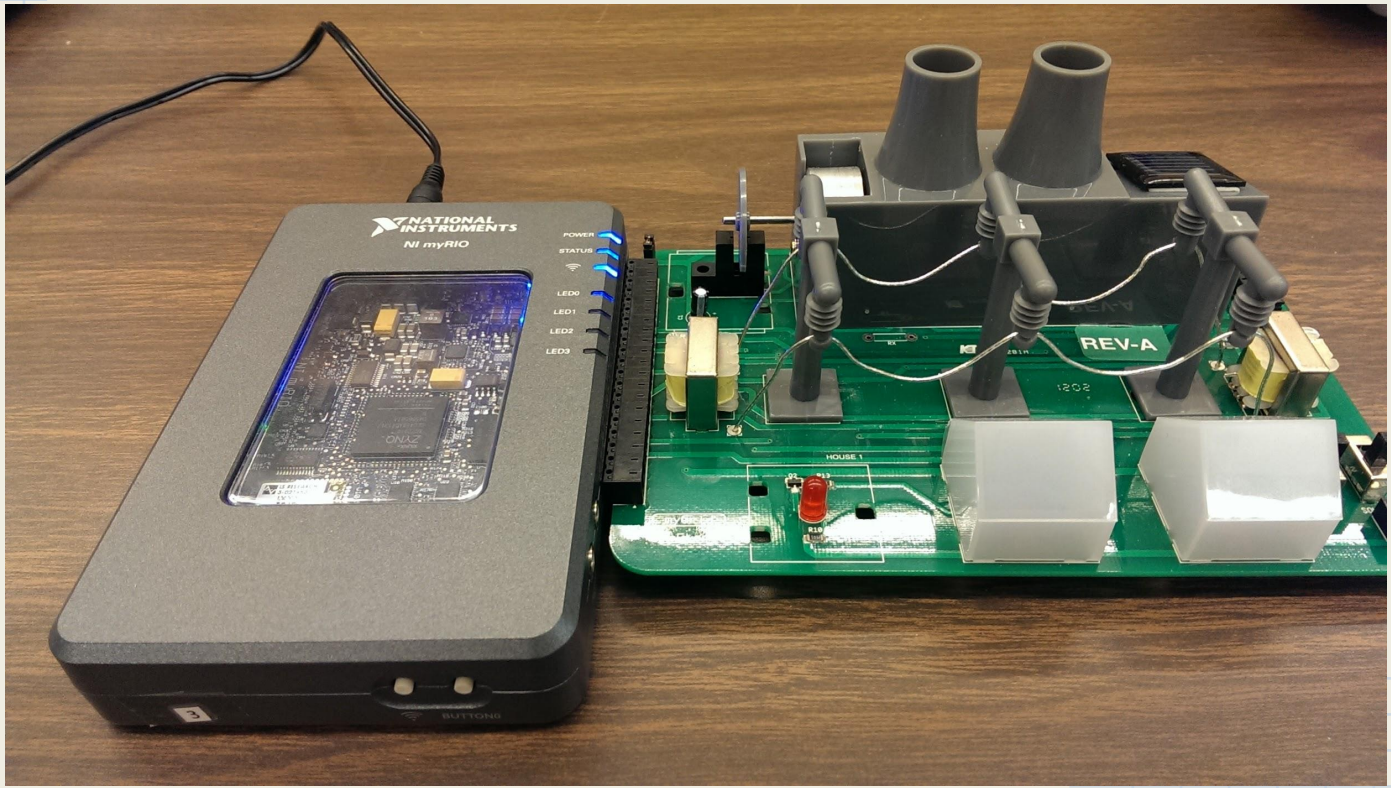
# Design-Hardware

- Two Major Design Requirements
  - Able to communicate between the myRIO and the PowerCyber Lab using OPC communication
  - Easily deployable, minimal setup time with no prior experience necessary
- For the majority of the design process we focused on integrating the myGrid board with the myRIO
- Given an older version of the myGrid GUI software, we reverse engineered a solution to get the current myGrid board functioning normally
  - Helped us learn about LabView and troubleshoot through many challenging roadblocks
- Designing the OPC communications link was much more straightforward
  - OPC is versatile, so it took many iterations to find the best setup for our spec.

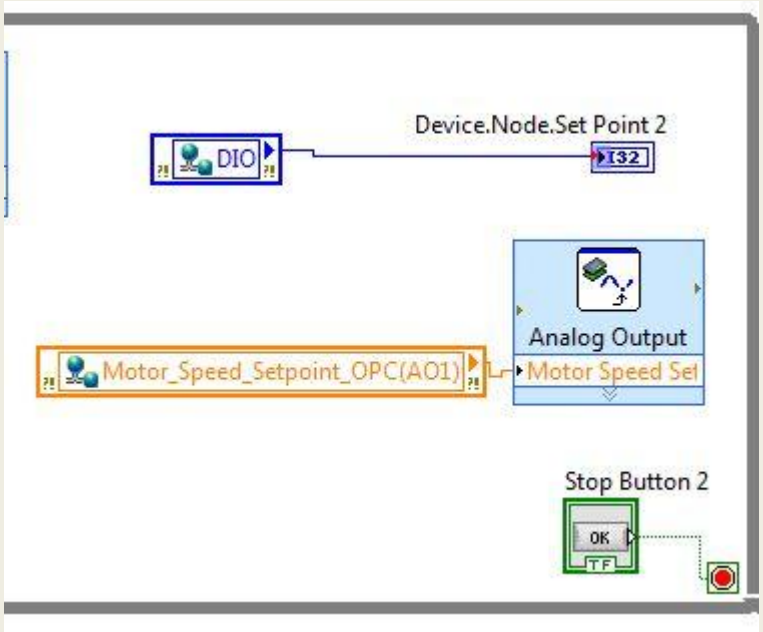
# Iterations-myDAQ



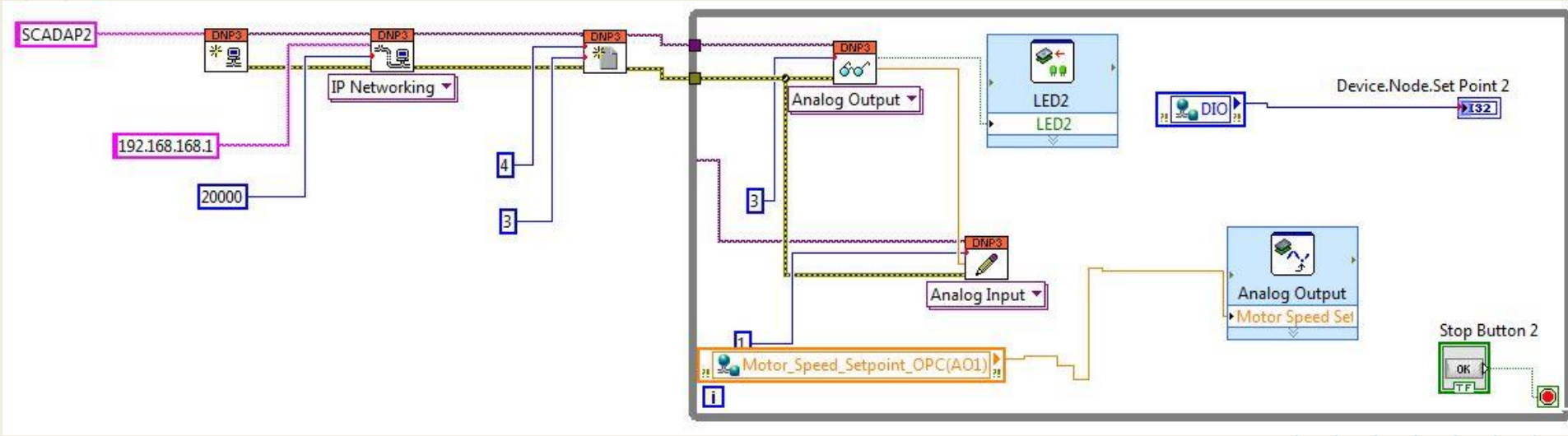
# Iterations-myRIO



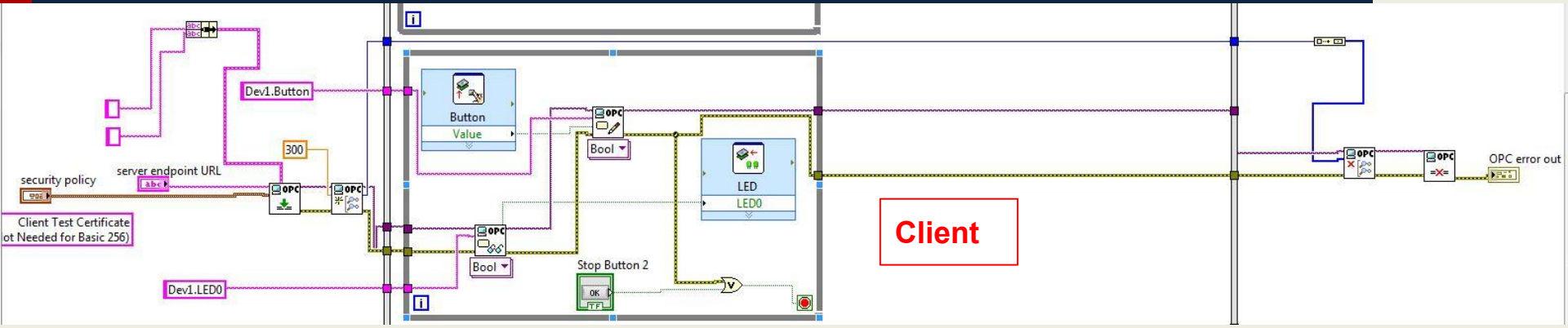
# Iterations-Shared Variables

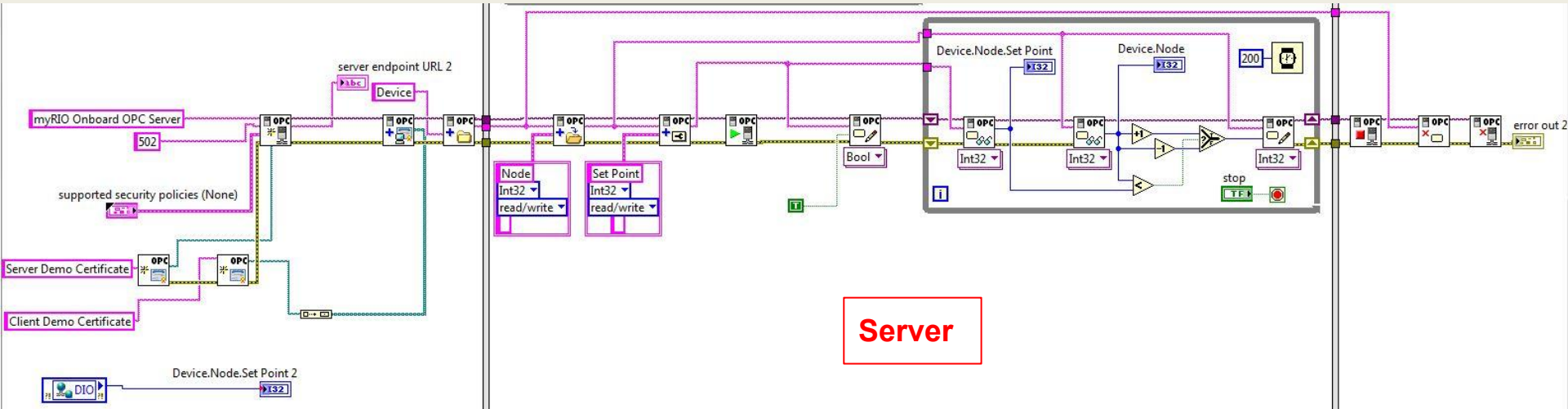


# Iterations-DNP3



# Iterations-OPC UA



# Scope & Changes

| 1st Semester | 2nd Semester |
| --- | --- |
| Create Cyber-Physical System Cyber Defense Competition (CPS-CDC) | Virtualized Environment<br>Virtualized components of the PowerCyber Lab ISERink |
| Add communication between the devices, model, and control center | Integrate National Instruments (NI) equipments myRIO-myGrid into PowerCyber Lab using local network |
| Implement a protection scheme for the existing 39 bus model | Furthermore, integrate NI equipments to ISERink and CPS-CDC as well |
| Integrate physical relays into existing 39 bus model | Interface between myRIO and myGrid so that myRIO receives the correct data from myGrid |

# PowerCyber

## Questions?

### None?

Okay good