Dec14 - 07

PowerCyber Testbed

Our Team

Ian Pierce - Team Lead
Adam Daniel - Webmaster
Derek Augustyn - Communication Liaison
Shuky Meyer - CprE Team Lead
Justin Noronha - EE Team Lead
KangHee Lee - Key Idea Holder
Brian Forsberg - Key Idea Holder

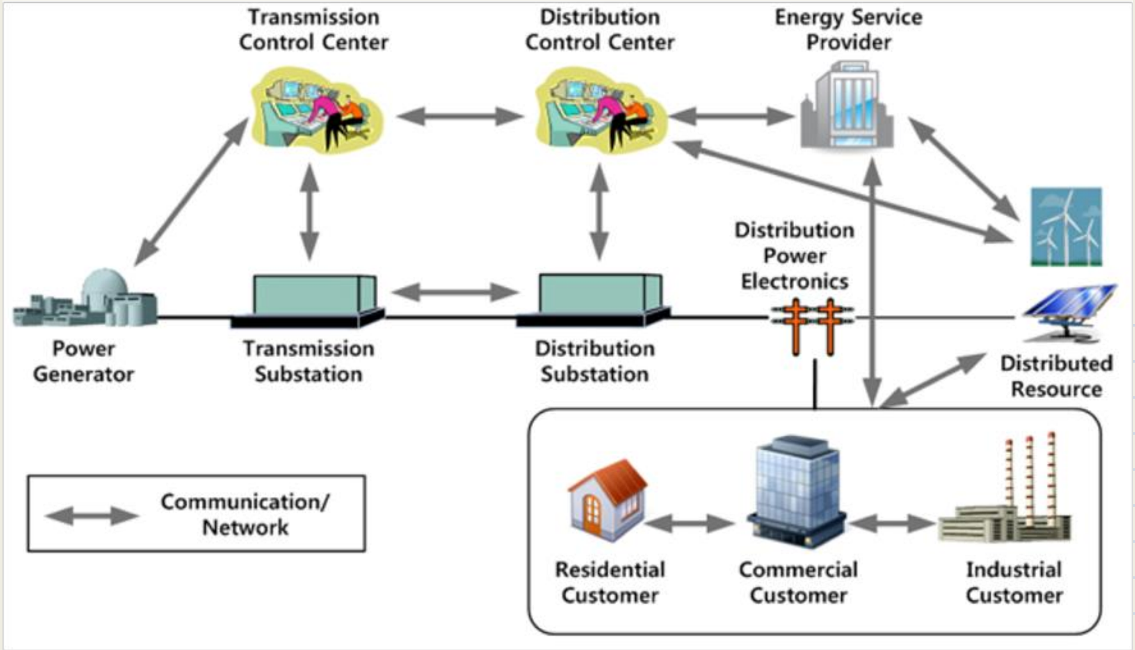
Dr. Manimaran Govindarasu - Advisor/Client

Overview

- SCADA
- Problem Statement
- Functional Requirements
- Non-Functional Requirements
- Risk and Mitigation
- Schedule
- Goals
- EE Sub Team
- CprE Sub Team
- Current Status
- Next Semester

SCADA

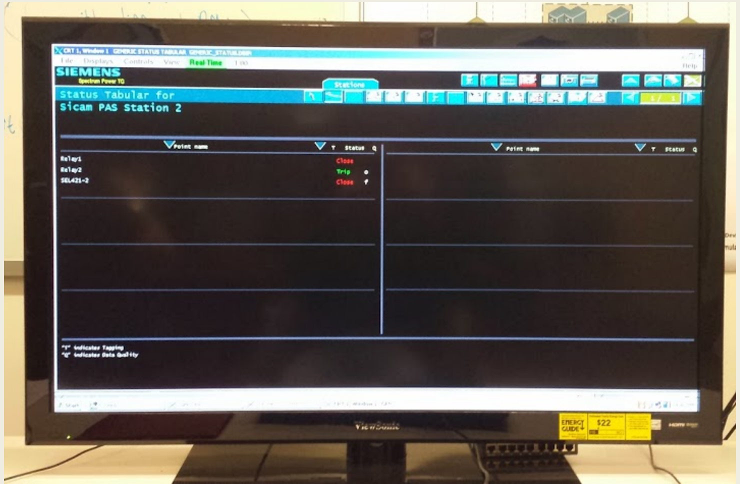
- Supervisory Control and Data Acquisition
- A computer system that monitors and controls vital industrial processes in real time
- Includes:
  - Power generation and distribution
  - Water treatment plants
  - Oil and chemical refineries

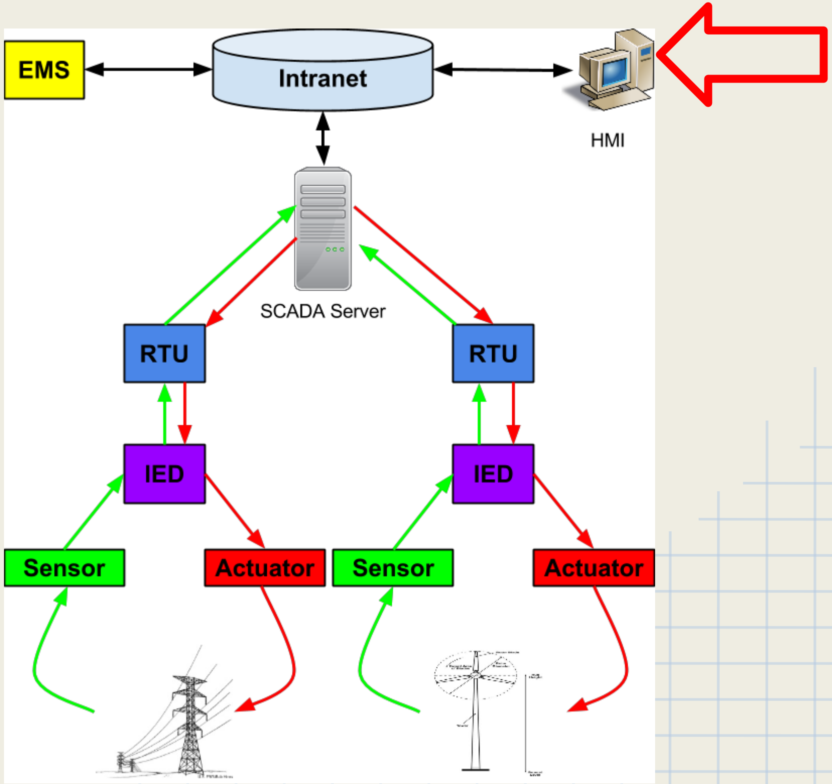


SCADA System Architecture

Control Center

- Human-Machine Interface (HMI)
- Enables the operator to monitor and control processes



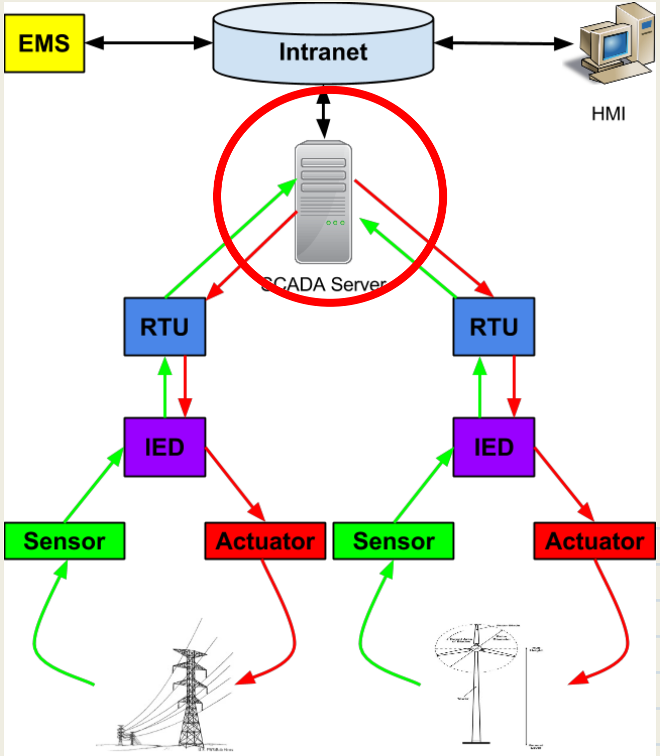


SCADA System Architecture

Supervisory Station

- Substation containing servers and computers for relaying data

- Provides the necessary path for communication between the control center and the monitored devices

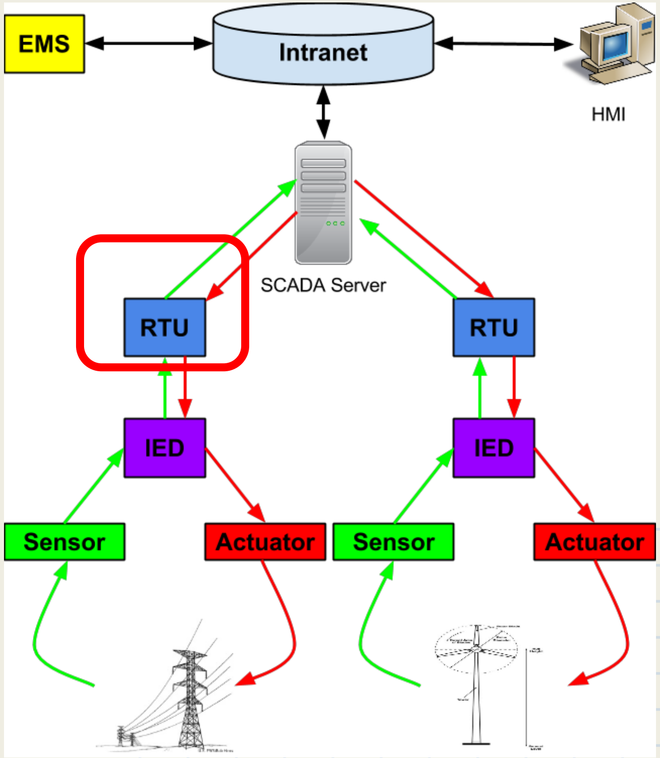


SCADA System Architecture

Remote Terminal Unit (RTU)

- Devices that are physically connected to the equipment for monitoring

- Sends data to the control center via the substation



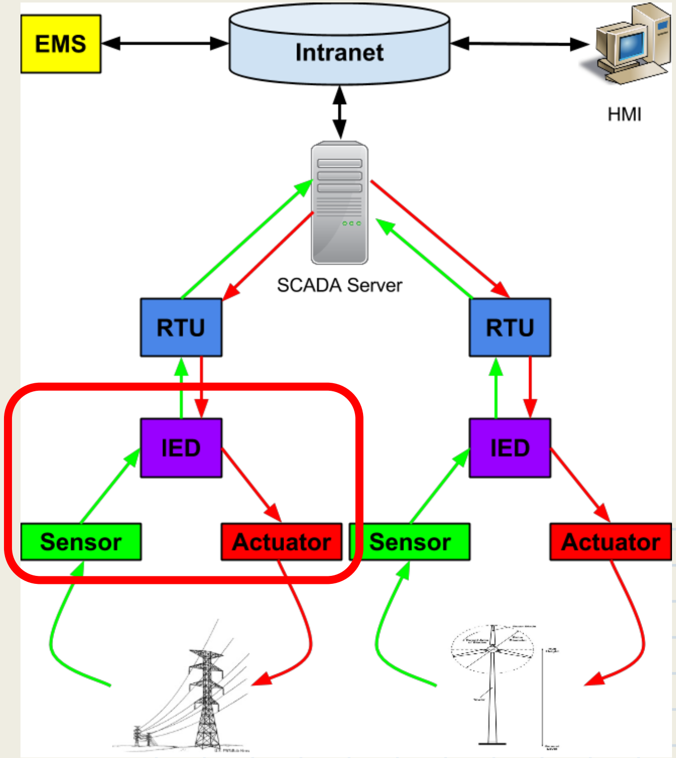
SCADA System Architecture

IED, Sensor, & Actuator

- Intelligent Electronic Devices house the actuators and sensors (in our case) to sense the power flow and trip breakers as necessary

- The sensor collects the raw process data used by the operator to make decisions about the process

- The actuator provides change to the process if and when desired



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
- A PowerCyber testbed has been recently developed at ISU to remedy this situation

Functional Requirements

- Increase the capacity of the current Power Grid Model
  - Modify the current 39-Bus Model to communicate with the physical devices
- Implement a Power Protection System for the previous 39-Bus Model
- Send/Receive Commands using IEC/GOOSE Communication Protocol between Relay and Simulator
- Transmit Simulated Analog Values to Command Center via OPC Communication Protocol

Functional Requirements (cont.)

- Create project plan and design document for CPS-CDC
- Discover System Vulnerabilities
  - Design and Verify countermeasures for new vulnerabilities
- Develop patches to previously discovered system vulnerabilities
- Develop attack scenarios for the competition
- Setup virtualization environments for CPS-CDC simulations
- Designate a scoring system for the different scenarios/modules

Non-Functional Requirements

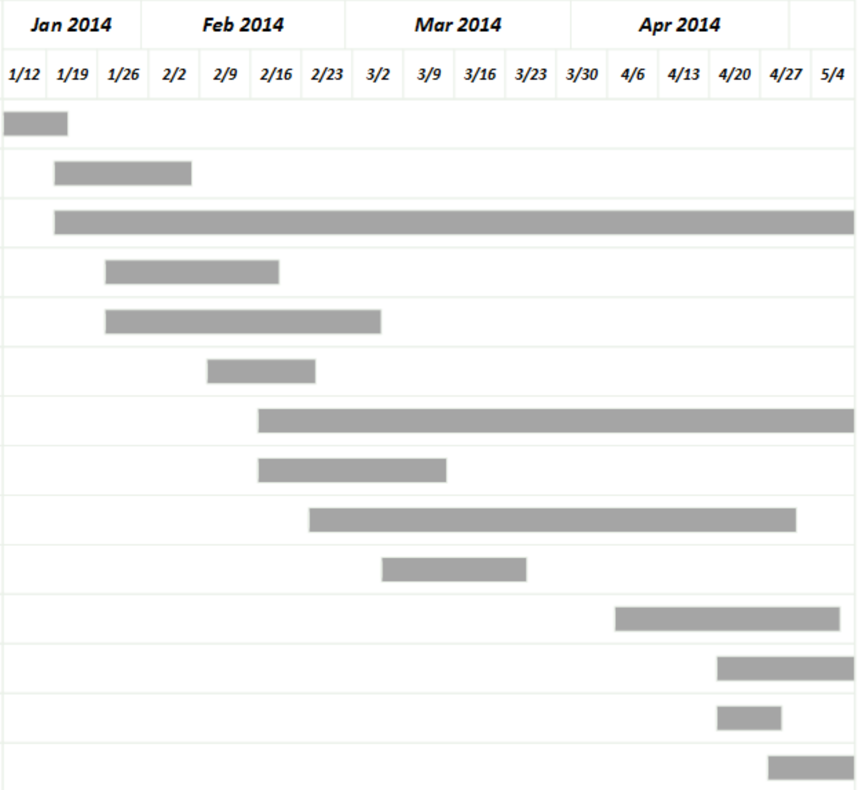
- Document past work and all future work to improve project handover time
- CPS-CDC should be scalable and portable
- Develop learning materials to quickly immerse students in control systems
- Improve the SEL PMU
  - Check interfacing with SCADA system
  - Thoroughly test for vulnerabilities
- Clean and make model easier to read

Risk and Mitigation

	Risk	Mitigation
1	Implement a power protection system to the entire 39 bus model may induce numerous errors	Support from the graduate students who are familiar with power protection. We will also research and expand our knowledge about power protection
2	There is a possibility that 39 bus model may no longer be functional because of unexpected errors	We Made sure to save a copy of original model so that we can always go back to the previous version
3	Since the CPS-CDC is the first of its kind, a large number of students will be unfamiliar with SCADA systems	Provide online tutorials, open forums, SCADA workshops, and an online chat help room to educate participants in the CPS-CDC
4	Licenses & availability of different virtual systems (relays/substations/vpn/etc...) may have time limits (ie: Remote IEDs currently have a 30 minute limit)	If persistent risk develop CPS-CDC that utilizes virtual components around given restraints or scale down and use physical components as replacement

Schedule

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



Goals

- Integrate physical relays into existing 39 bus model
- Add OPC & IEC communication between the devices, model, and control center
- Add additional functionality to the existing 39 bus model
  - Clean model to make it “easier to read”
- Implement a protection scheme for the existing 39 bus model
- Create Cyber-Physical System Cyber Defense Competition (CPS-CDC)
  - Organize attack/defend scenarios for the competing teams

Questions

- SCADA
- Problem Statement
- Functional/Non-Functional Requirements
- Risks & Mitigations
- Goals

EE Team

- Opal-RT Technologies OP5600 HIL Box
- Target node used to simulate power system models
- Provides Real Time Digital Simulation (RTDS) of a power system model
- Advanced monitoring capabilities with scalable I/O for future expansion

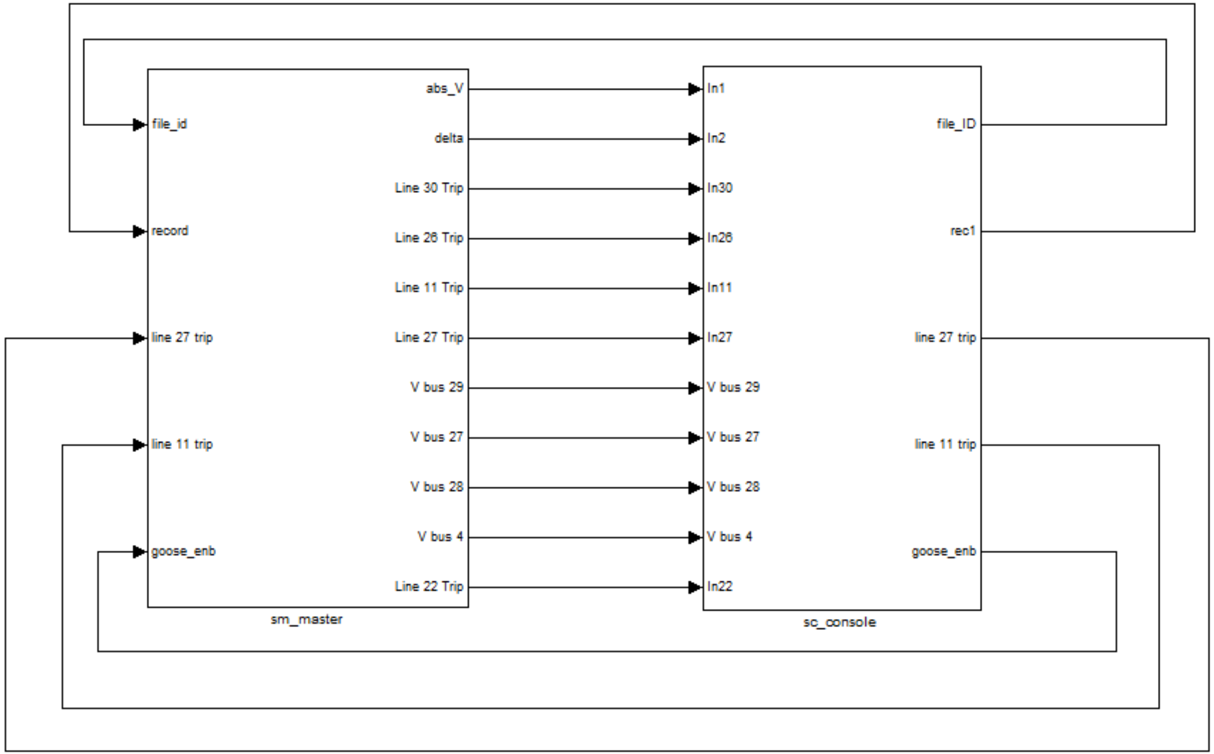
Power System Model

RT-Lab

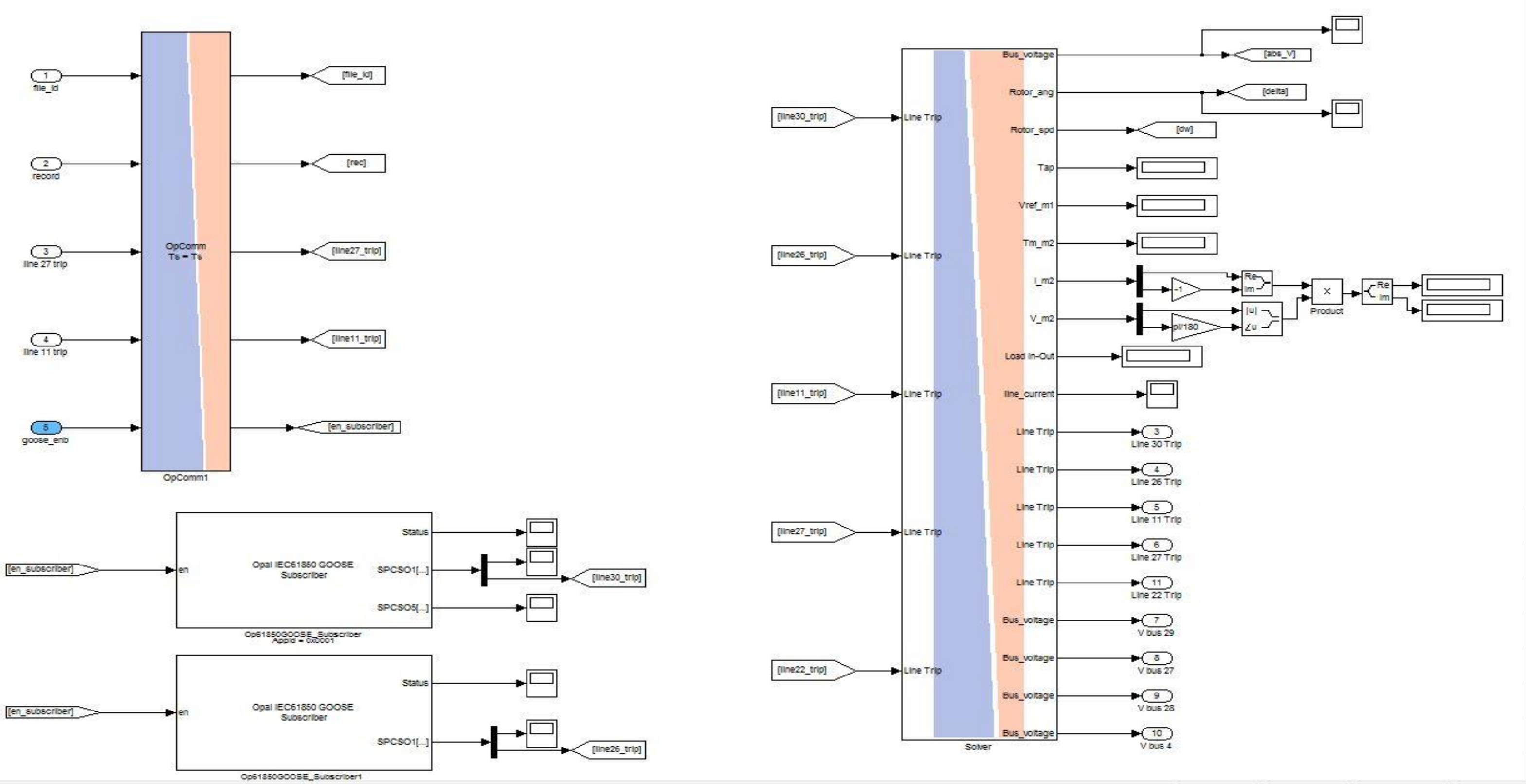
- Based on Mathworks Simulink software
- Runs a specified model on the Opal-RT target node
- Uses special “OP-COMM” blocks to monitor and control the model
- Model is created using block sets for inputs, outputs, and line tripping

RT-Lab Model

- Two main subsystems
  - Master
  - Console

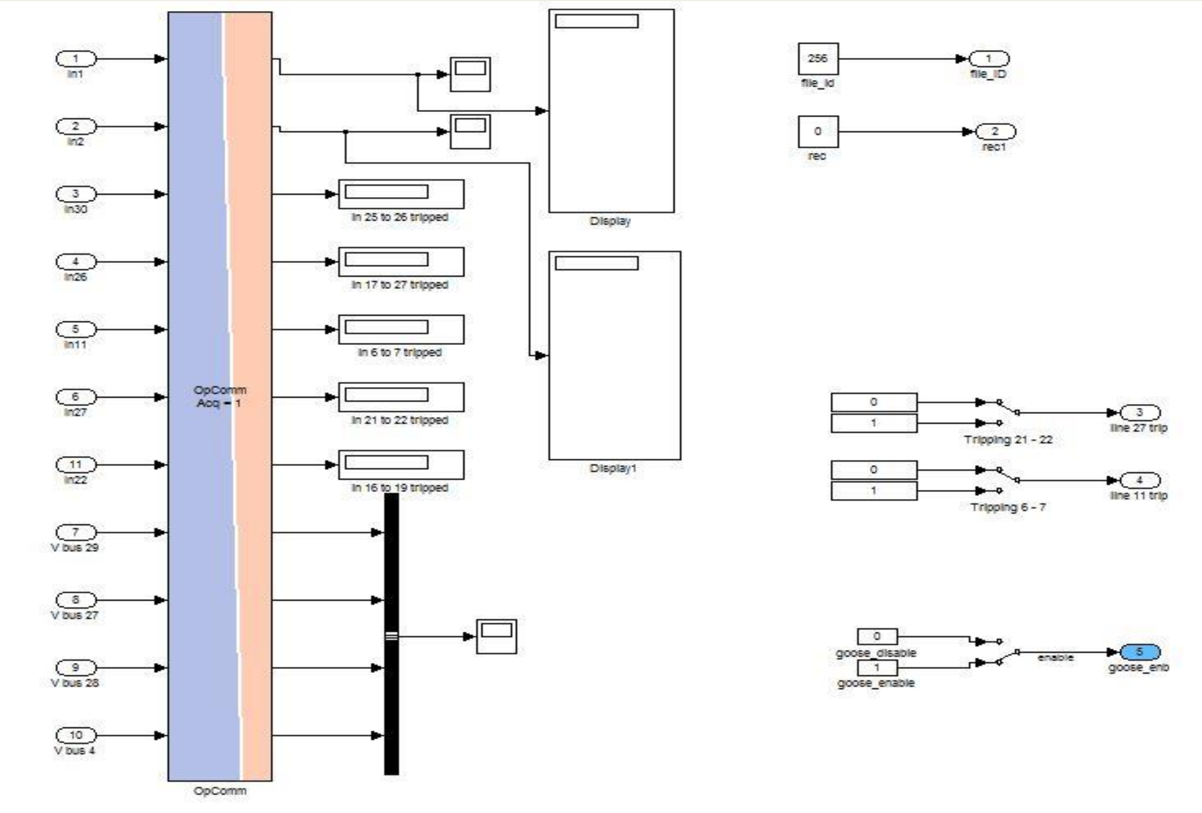


Master Block



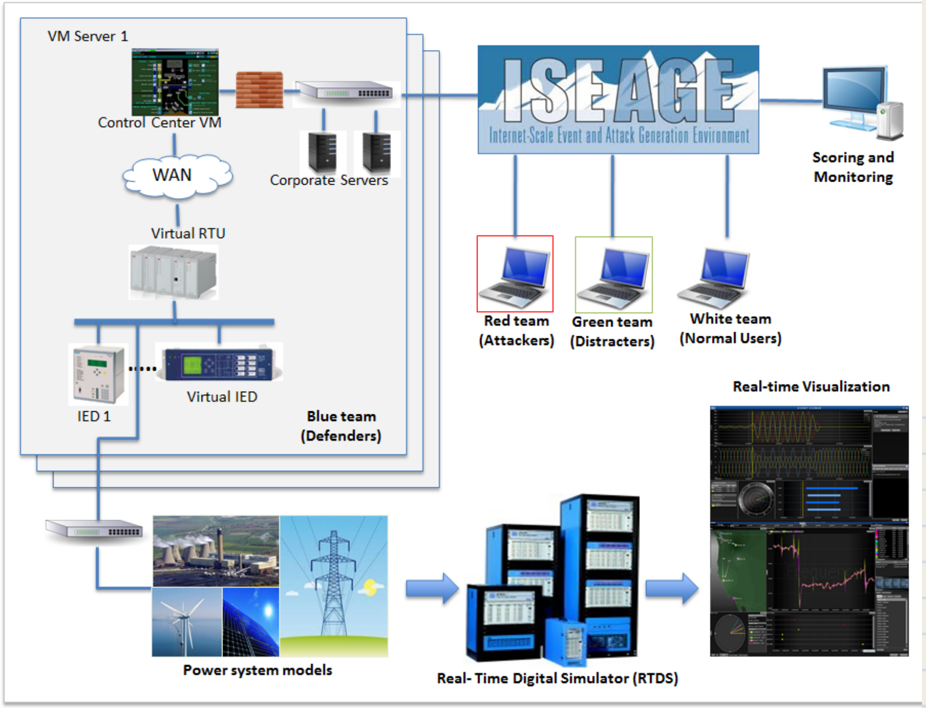
Console Block

- Control block features manual switches for tripping, scopes and displays for viewing real time data
- Only observable part of model while simulating



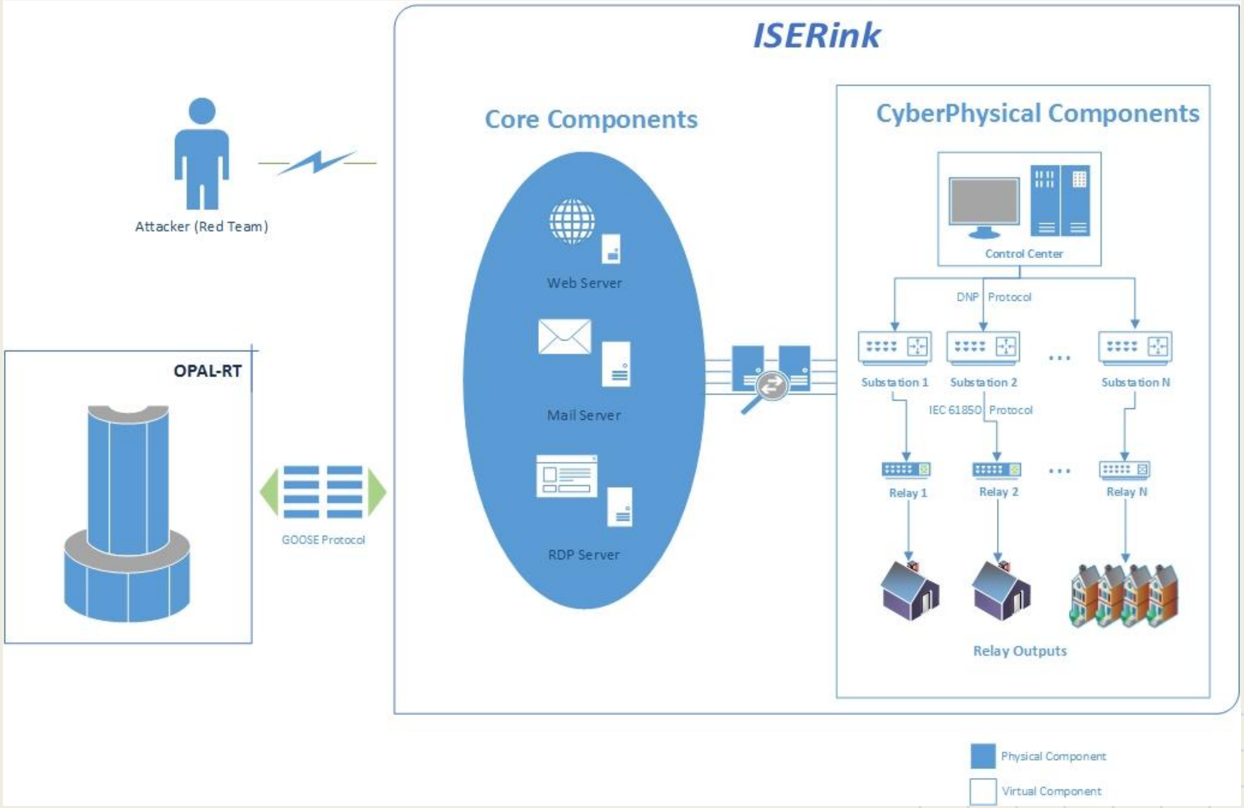
CprE Team CPS-CDC

- Integration of CDC and PowerCyber Testbed
- Mostly virtualized environment with some possible physical components
- Includes learning resources for those inexperienced with SCADA system security
- Includes a variety of scenarios of increasing complexity



Dec14-07

CPS-CDC Architecture



CPS-CDC Integration Tests

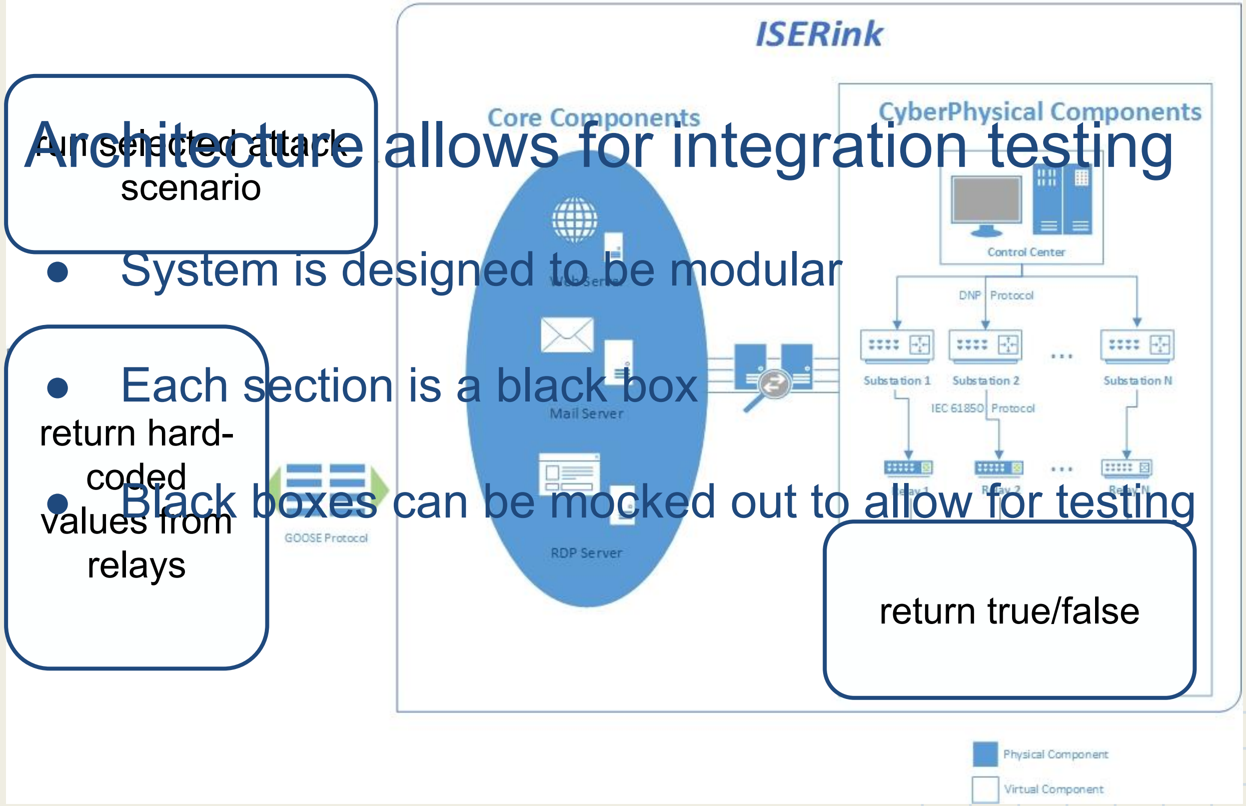
Architecture allows for integration testing

- System is designed to be modular
- Each section is a black box
- Black boxes can be mocked out to allow for testing

run selected attack scenario

return hard-coded values from relays

return true/false



Attack Scenario Example

- The Teams
  - Blue team - defends substation, web server, RDP server, etc.
  - Red team - attacks substation, web server, RDP server, etc.
  - Green team - general users test web server, RDP, and availability

- *Massive Electric, LLC*
  - Previous employees were fired because of corporate espionage
  - Your job is to patch our system to prevent impending attacks
  - Assigned to Ames substation

Wiki & Learning Modules

- Wiki - Lab documentation
    - Assist future PowerCyber teams in getting up to speed
    - Create repository of all previous PowerCyber documents and presentations
    - Document procedures and equipment
    - Catalog known exploits and mitigation techniques

- Learning Modules
    - Help CPS-CDC teams understand testbed and equipment
    - Resources for setting up and securing SCADA systems
    - Documentation regarding how to setup a CPS-CDC event

Wiki & Learning Modules

Logged in as: chuck (chuck) Admin Update Profile Logout

PowerCyber

Recent changes Media Manager Sitemap

Trace: • start • main

powercyber:main

Table of Contents

PowerCyber Wiki Start Page

This pages is intended to provide the user some experience with the network protocols and communication requirements within the electric power grid.
For individuals without lab access, please coordinate with another student to find times when the lab is accessible.
In the future there will be a VPN setup that will allow access to the lab at any time.

Edit

SCADA

Supervisory Control and Data Acquisition

> a system operating with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station)

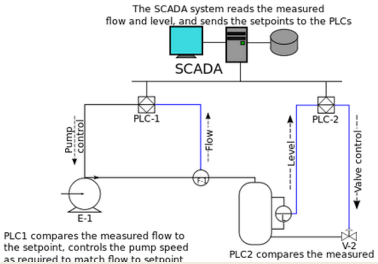
– Wikipedia

The PowerCyber lab makes use of the SCADA[1] system to communicate with the individual stations in the lab.

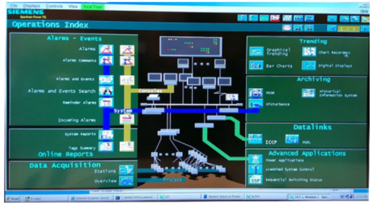
A SCADA system is usually made up of Remote terminal units (RTUs) that connect to sensors in the process and convert sensor signals to digital data.

They have telemetry hardware capable of sending digital data to the supervisory system, as well as receiving digital commands from the supervisory system. RTUs often have embedded control capabilities such as ladder logic in order to accomplish boolean logic operations.

Programmable logic controller (PLCs) connect to sensors in the process and converting sensor signals to digital data. PLCs have more sophisticated embedded control capabilities, typically one or more IEC



Setting up the attack scenario



Verify the communication between the control center and the substation is properly working. The **Siemens Spectrum Power TG** application should be running on '**SCADAs01**'.

Edit

Verify connection

1. Click on '**Displays**' on the top of the menu bar.
2. Select '**Stations Index**'
   a. A list of substations sould now be available on the screen
3. Select '**Sicam PAS Substation 2**'
   a. Click '**Status**'
      I. A list of connected devices should now be abailable on the screen
      II. The physical relay is '**Relay 2**'
4. In the '**Relay 2**' page, the '**Q**' column identifies whether the communication to the device is operational
   a. An '**f**' denotes that a device has failed and needs to be reset

Edit

Closing the relay

1. Click on '**Status**' of Relay 2 and select '**Close**'
   a. The light should then turn on
      I. at this point it is possible that the light is not physically connected, if it doesn't turn on please check the physical connection of the device

Edit

Log into the 'SCADAws02' (Scada workstation 02)

1. Open Wireshark and begin sniffing packets on the interface labelled 'Intel Pro 100/1000Mbit'

Edit

Tripping the relay

1. Back at the control center, select '**Relay2**'
2. Select the option to '**Trip**' the relay.
3. Back at SCADAws02, stop the wireshark capture session.
4. Utilize the collected traffic to determine the answers to the following questions

Edit

Questions about capture procedure

1. Inspect the communication between the control center and the SICAM

1. What protocol is used for the WAN communication?
2. Describe the communication sequence that occured and what control packets are used to cause the breaker to trup?

Questions

- Opal RT
- RT-Lab
- Master & Console Blocks
- CPS-CDC
- Attack Scenarios
- Learning Modules

Design Standards

Based on NERC Planning Standards

- Used to base stability analysis of system
- Initial bus values between .95 and 1.05 pu
- Voltage dip not to exceed 30% at any bus

A properly created system should have N-1 contingencies

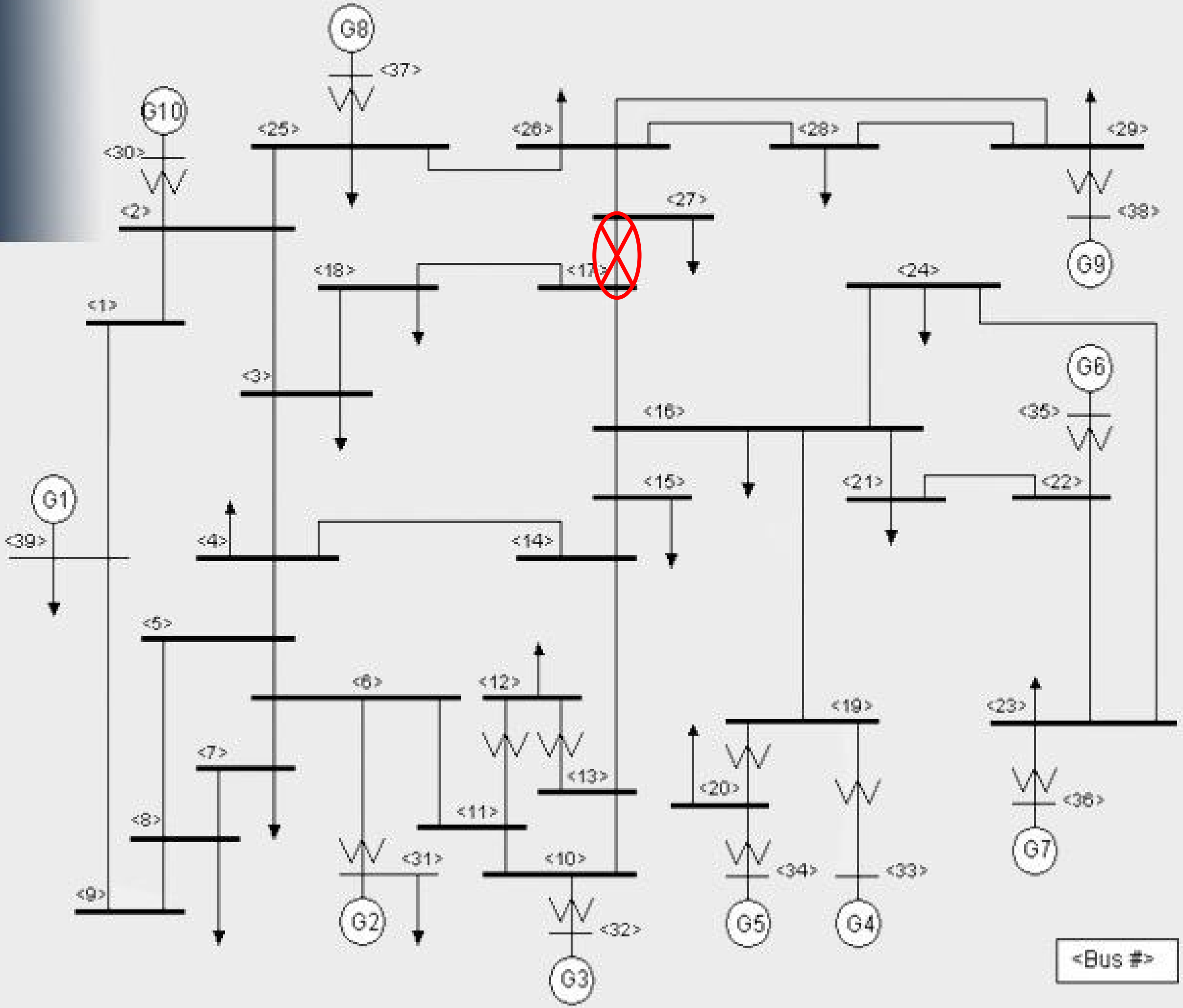
- If one line is tripped, the system should stabilize

More robust systems are able to follow an N-2 contingency

- If two lines go down simultaneously, the system will stabilize

N-1 Test

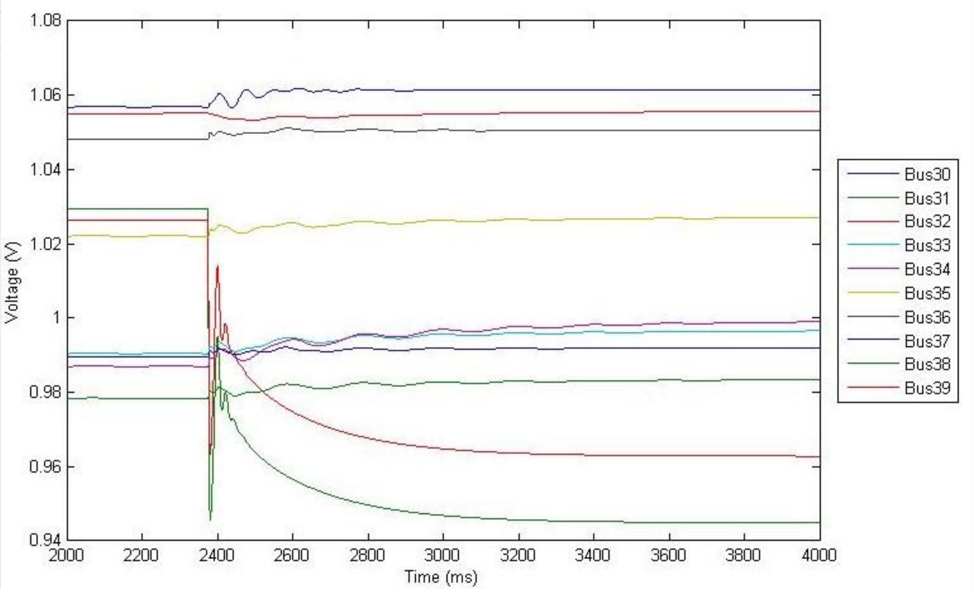
Our N-1 contingency test will trip line 26, which runs between busses 17 & 27



Dec14-07

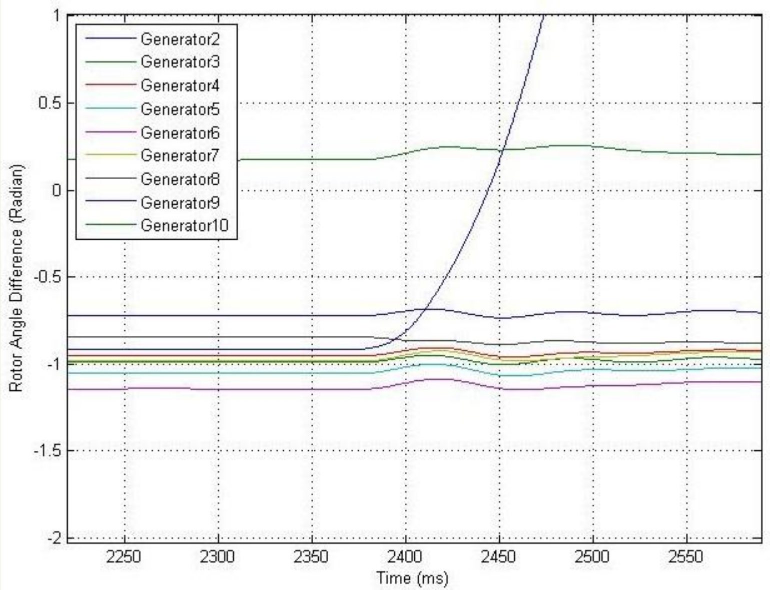
Results

Generator Bus Voltage



Voltage stabilizes and goes back to equilibrium within NERC Standards

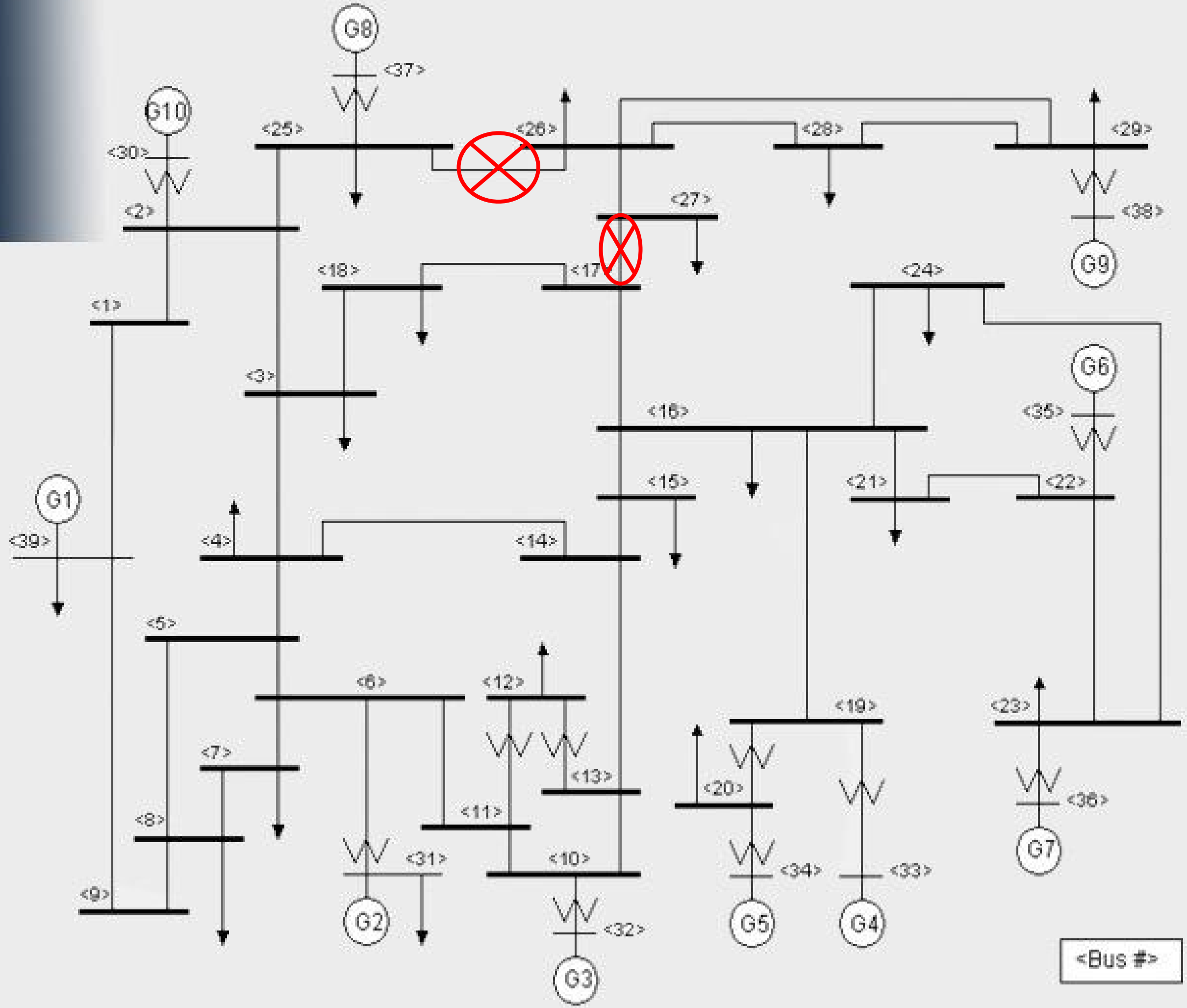
Generator Rotor Angle



Rotor angle increases rapidly because of the instance of instability

N-2 Test

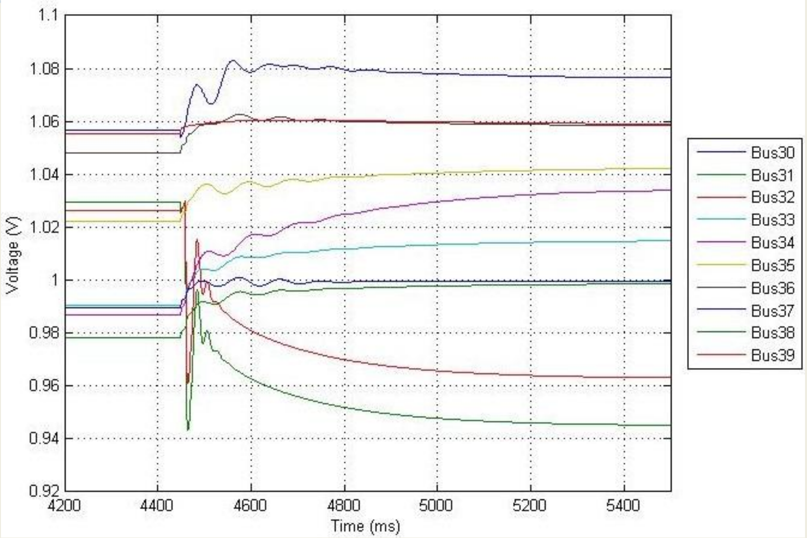
Our N-2 contingency test will trip line 26 in conjunction with line 30



Dec14-07

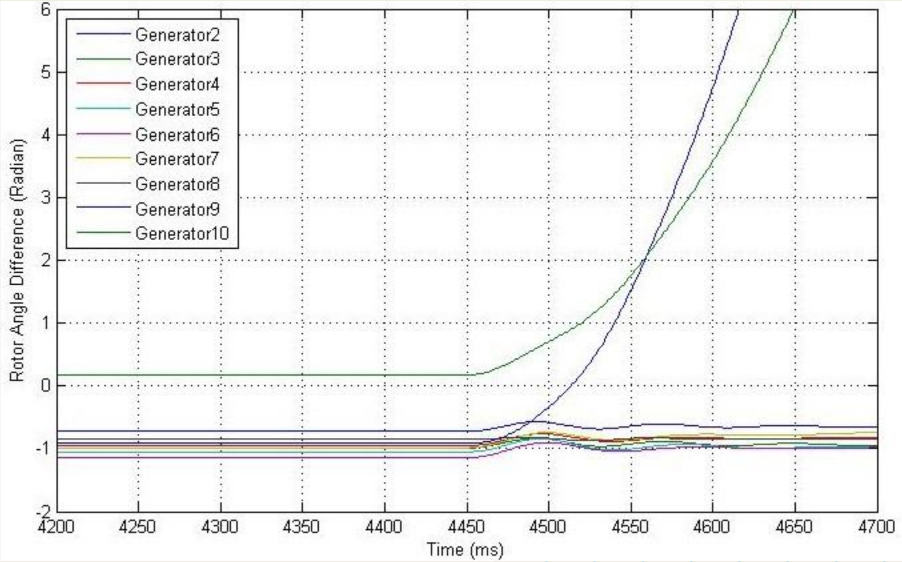
Results

Generator Bus Voltage



Voltage stabilizes and goes back to equilibrium within NERC Standards

Generator Rotor Angle



Multiple rotor angles increase rapidly because a generator has been cut off and isolated

Resources & Cost

- Mentors
  - Dr. Manimaran Govindarasu
  - Pengyuan(Bruce) Wang - Graduate Student
  - Aditya Ashok - Graduate Student
  - Anirudh Pullela - Graduate Student
- Costs
  - Shared between labs
  - Near zero

Current Status

- 39-Bus Model and relays are functioning and communicating.
  - GOOSE Communications allow physical devices to affect the Opal-RT simulation

- CPS-CDC design document complete along with scenarios
  - Varying scenario architectures provide flexibility for CPS-CDC
  - Each scenarios is designed to be modular and easily replaced with alternative scenarios

- Wiki and Learning Modules are under construction
  - We will document as necessary during the implementation stage

Next Semester

- Implement OPC communication
- Add IEC communication to SEL Devices
- Create simple power protection scheme
  - Expand to protect entire 39 bus model
- Integrate ISERink and PowerCyber
  - Configure for CPS-CDC
- Develop learning modules for CPS-CDC
- Host first CPS-CDC
- Analyze shortcomings of CPS-CDC event and improve design

Questions?

None?

Okay good