Iowa State University

Cyber Security Smart Grid Testbed

Senior Design, Final Report

<u>Dec 13 - 11</u>

Derek Reiser

Jared Pixley

Rick Sutton

Faculty Advisor: Professor Manimaran Govindarasu

Table of Contents

Definitions

EMS: Energy Management System

ISEAGE: Internet-Scale Event and Attack Generation Environment

PAS: Power Automation System

PDC: Phasor Data Connect

PMU: Phasor Measurement Unit

RTDS: Real Time Digital Simulator

RTU: Remote Terminal Unit

SCADA: Supervisory Control and Data Acquisition

SEL: Schweitzer Engineering Laboratories

Smart Grid: An electrical grid that uses information and communication technology to gather and act on information

Testbed: A platform for experimentation of large development projects

Executive Summary

Supervisory Control and Data Acquisition (SCADA) is a type of industrial control system used to monitor and control industrial processes in the world such as power generation, water treatment, oil and gas pipelines and many other critical systems. The electric power grid is a highly automated and complex network comprised of a variety of control systems, sensors, communication networks and many other forms of information all with the purpose of monitoring, protecting and controlling the power grid. Due to the continuous development of this automated network and many other critical systems, the threat of cyber-based attacks are becoming more and more of a reality. These attacks could stop and damage many important systems that most of us take for granted. Therefore, security of the power grid and other critical automated networks (through the SCADA system) is one of the most impatient developmental issues we have today.

To conduct this research, a PowerCyber testbed has been developed in recent years by other graduate and undergraduate students resulting in a properly functioning testbed network. This testbed allows us to simulate power systems and the communication protocols they use and attempt cyber attacks on the system. The current testbed in composed of Real-Time Digital Simulator, industry-grade power system control center software, substation automation systems, communication protocols, security devices, relays, and a fuzzer device (for vulnerability analysis)..

The previous senior design teams have created and continuously improved upon a SCADA testbed. This includes a control center, relays, RTU's communications devices, a web server and a DTS. The goals of this year's design team is to further enhance the test bed by incorporating more relays from a different vendor, a new simulator and to also incorporate a remote access feature which will allow people to run simulations of the test bed from anywhere.

Problem

Our goal is to improve the current SCADA testbed. The previous design teams have done testing on the system that is currently in place. Once we have added in the new devices we will run the tests that they have provided seeing the difference in the results from the old test be to the enhanced testbed and also run new cyber security attacks to see how the different types of relays will respond.

Operating Environment

The operating environment for the test bed is a lab in Coover Hall. The SCADA system has been an ongoing project and we are the fourth senior design team to work with and improve the functionalities of the system. A functioning testbed (Figure 1) was already implemented when we began our project. We intend on expanding the system by adding a few additional components to create a more improved SCADA system (Figure 2)

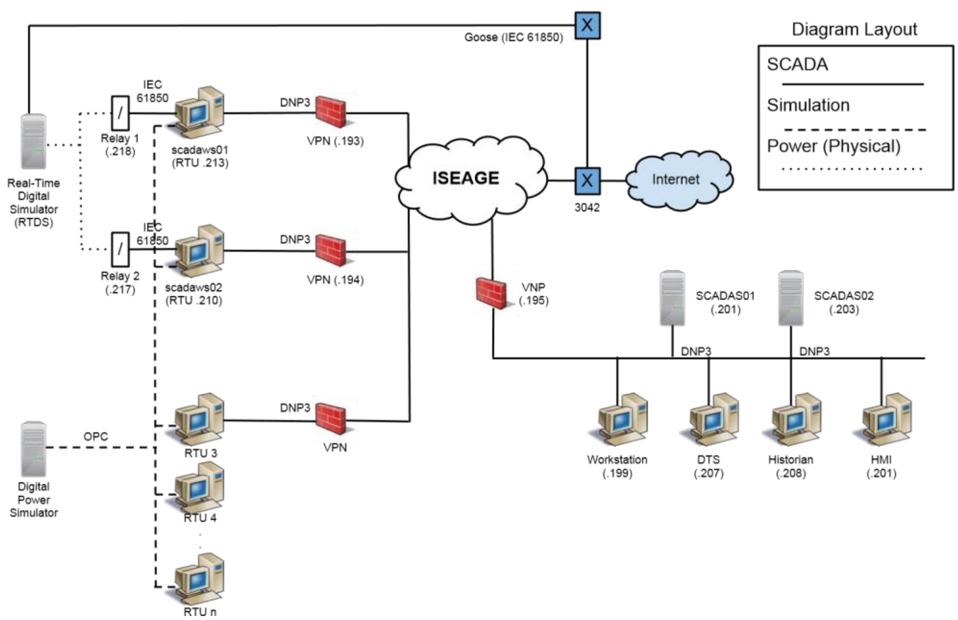


Figure 1: Previous Testbed

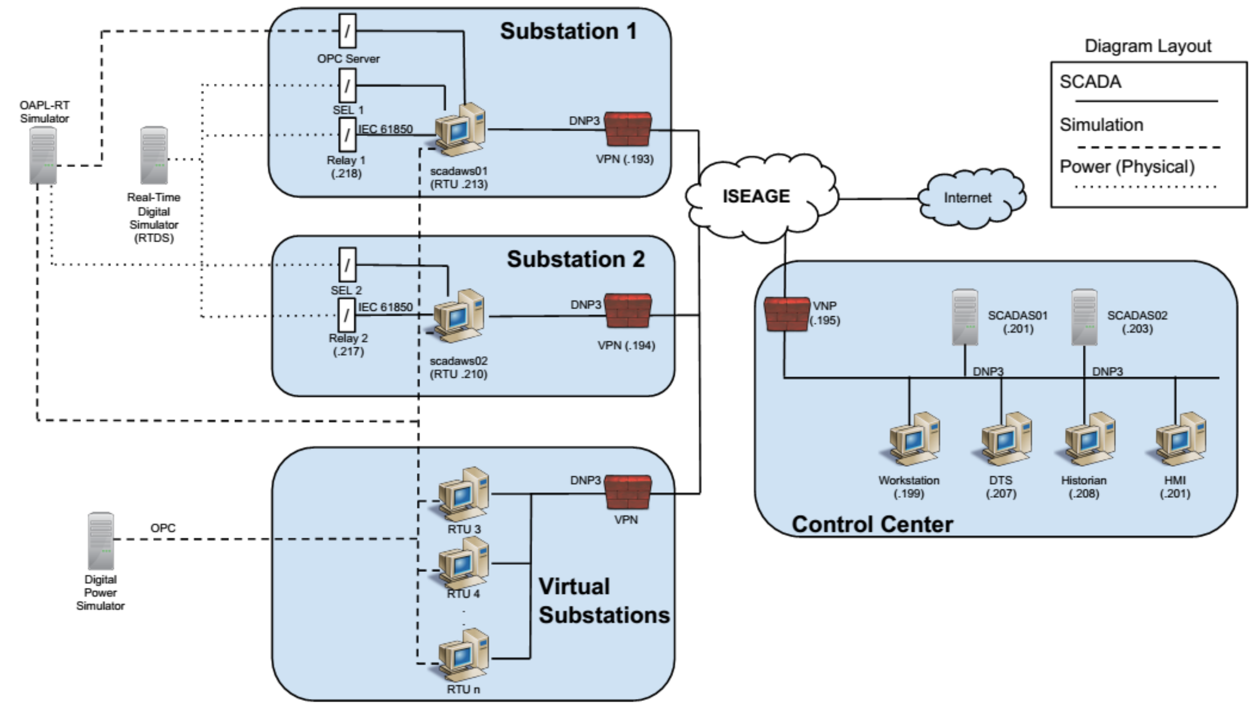


Figure 2: New Testbed

Intended Users and Uses

The primary users of this system will be graduate and undergraduate students in computer engineering or electrical engineering who are researching the cyber security of SCADA systems. Other users of this system might be researchers or companies interested in learning more about the test bed and its functionality.

The primary uses of this system will be the creating and testing of cyber-attacks and researching the effects that a cyber-attack could have on a SCADA system, especially in regards to power flow. Another use of this system might be showing people the basics of how a SCADA system works.

Assumptions and limitations

Assumptions List:

- All test equipment will function properly.
- Simulated devises function identical to physical devises
  - Such as the physical RTU's and the simulated RTU's.
- The test bed is similar to a real-world SCADA system.
  - 15 substations in the test bed will be enough to simulate a real-world system.

- Systems protocols provide the test bed system to accurately portray real-world protocols.
- The test bed will be demonstrated to those interested in SCADA systems and cybersecurity.
- Industrial companies/providers are interested in vulnerabilities found through the test bed analysis.
- The test bed will be used and continuously improved upon in years to come for continuation of cyber-security attacks on a SCADA system.

Limitations List:

- We have two semesters to complete the project.
  - In our second semester, we lost one of our team members.
- Only 120V will be used by the relays.
  - Real-world systems exceed more than 230kV.
- Only 2 physical relays will be used due to physical, financial and time limitations.
  - Other relays will be simulated.

Expected End Product

At the end of this senior design project period, we expect to add multiple components to the current test bed. We shall integrate an Opal-RT simulator and two SEL PMU's which will enable us to more accurately analyze an attack on the SCADA system. Once the devices are properly integrated into the system, we will run multiple cyber-security analysis tests using standard nine and thirty bus systems we have created. However, due to complications, we will no longer set up a remote access capability to run multiple types of simulations and attacks using previously formatted demo cases.

Approach

Design Objectives

- Continue to improve the current SCADA testbed that can be used to simulate cyber attacks.
  - This testbed will allow us to mimic real-world power systems and demonstrate the effects of a cyber-attack on a SCADA system.
- Add new components to the SCADA testbed ○ This will allow further attack analysis and more realistic testing scenarios.

Functional Requirements

Power System Integration

- Have ePhasorSim model running on Opal-RT simulator
    - The provided ePhasorSim model will be used with the New England 39 bus model to run simulations. The inputs and outputs of the model will be specified in the excel input document that is loaded into the ePhasorSim block. Special Op-Com blocks will allow communication with Opal-RT and the physical components.
- Connect the OPAL-RT simulator to the physical components in the testbed
    - Adding the OPAL-RT simulator to the testbed will consist of connecting the physical components via cables. The physical connections will allow for the transfer of data values for the measurements that are important to the testbed. Once connected successfully, the simulator will be able to be used as the central point for running real time simulations on the testbed.
- Add the PMU's to the current testbed
    - Adding the PMU'S will allow for the measurement of more data during tests. The PMU's will run alongside the current relays at the RTU stations. Connection of the test ports to the OPAL-RT simulator will give us actual voltage and current levels while running a test

Cyber Integration

- Understand the functionality of the MU Security Analyzer
    - The MU Security Analyzer is automated network security tester. This device has a selection of pre-set attacks and the ability to create custom attacks as well. Using this device for fuzz testing can allow us to discover unknown vulnerabilities in the system. Our hope it to be able to incorporate this device into the automated system as offering different types of fuzz testing and denial of service attacks.
- Understand Scada Attack Options
    - Once access is gained to a Scada system, there are different protocol that can be used to attack system components. By understanding what procols are available, attacks can be formulated to attack a specific component within the system.

Non Functional Requirements

Power System Constraints

- Connect the OPAL-RT simulator to the PMU test ports
    - This will allow for the transmission of actual voltage to the PMU's. By using actual values, more measurements can be made during operation of the testbed.

Technical Considerations

- OPAL-RTSimulor
    - Advantages
        - Already Purchased for the testbed
        - Allows for real time simulation of modeled systems
        - Can connect and work with components currently in testbed
        - Models are created in Simulink which 2 of the group members are familiar with
        - Vendor is willing to provide support as well as training on the simulator
    - Disadvantages
      Model designs are limited due to the number of cores in the simulator
- IEC PMU's
    - Advantages
        - Already Purchased for the testbed
        - Can connect and work with components currently in testbed as well as the OPAL-RT simulator
        - Allow for the measurement of more values during testing
        - They are industry grade equipment
    - Disadvantages
        - Test ports may not be able to be used for voltage levels during testing
        - Not familiar with setup of devices

Since the OPAL-RT simulator and IEC PMU's were previously purchased for the testbed, we were not involved in the decision process. The OPAL-RT simulator was purchased due to its real time simulation capabilities as well as the fact that it will work with the current testbed. The IEC PMU's were purchased because they will work with the current testbed and are industry grade components.

Integration/Attack Testing

- PSSE Simulations
    - Using PSSE 33, we can simulate a power system that can later be run on the ePhasorSim model. This allows us the ability to look for vulnerable areas of the power system and get data to check the ePhasorSim model against once it is run.
- ePhasorSim Model
    - The ePhasorSim model can be run within Simulink to check for errors in operation. Connecting a computer with the Opal-RT simulator will allow us to run ePhasorSim models on Opal-RT. Once the model is running correctly, and the simulator is connected to the testbed, the model will be run on the testbed to work out issues that arise.
- OPAL-RT Simulator Integration
    - All OPAL-RT simulator testing will take place in the lab. Measurements to and from the other testbed components will need to be monitored to ensure they are being transmitted correctly. Monitoring of the model will be needed to be sure it is running correctly. At a minimum the OPAL-RT simulator will need to be able to run the same tests possible on the current testbed.
- IEC PMU Integration
    - Once the PMU's are connected to the simulator and system and are set up correctly they can be tested. By running simulations, values can be transferred to and from the PMU's to ensure proper operation.

Detailed Design

Power System Software and Equipment

- Opal-RT – Real Time Simulator (Figure 3)
  - Allows us to run and solve our ePhasorSim models through the RT-Lab software, providing a real time analysis and functionality
  - Allows for physical connection to current testbed and components gaining us access to real time data transfer and analysis with the connected comments throughout the system

Figure 3: OPAL-RT

- RT-Lab/ePhasorSim software
  - Power system models (Figure 4) are created in by importing excel files with input and output information for the model into the ePhasorSim blocks.
  - The created models are imported into RT-Lab which then runs the models on the Opal-RT simulator in a real time environment.
  - The New England 39 Bus Model (Figure 5) will be used as the system modeled by ePhasorSim.

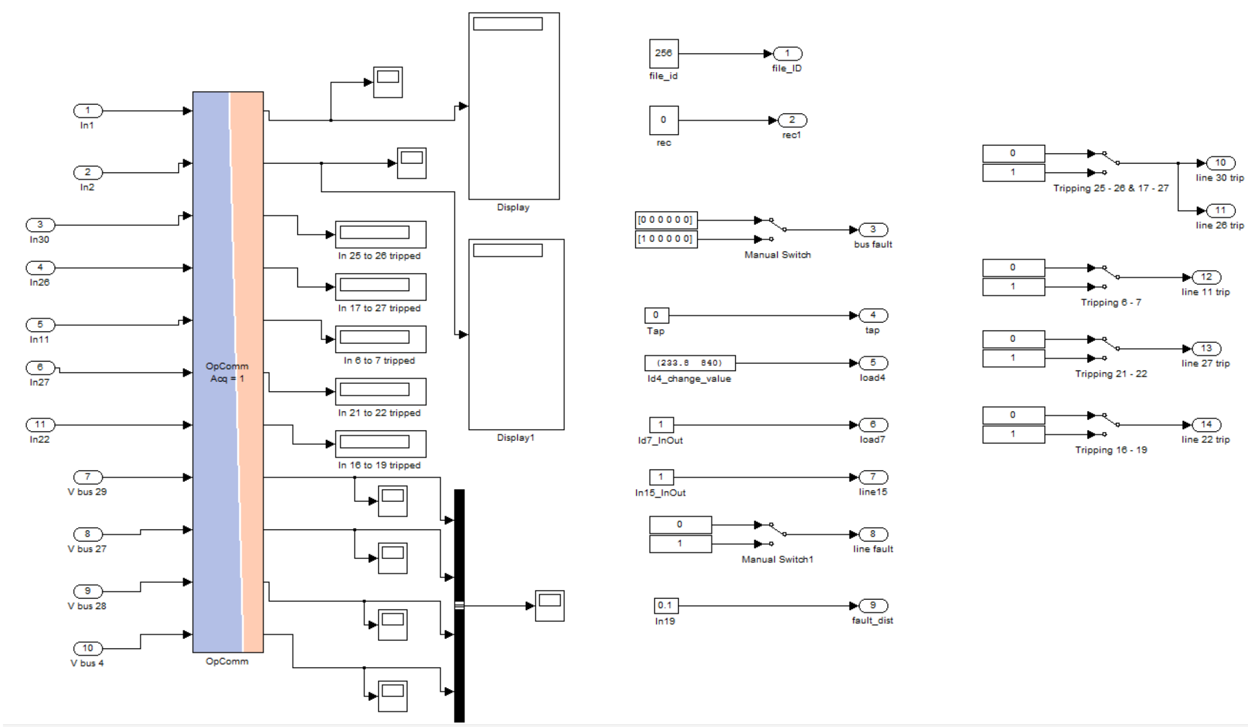


Figure 4: ePhasorSim Model

Network

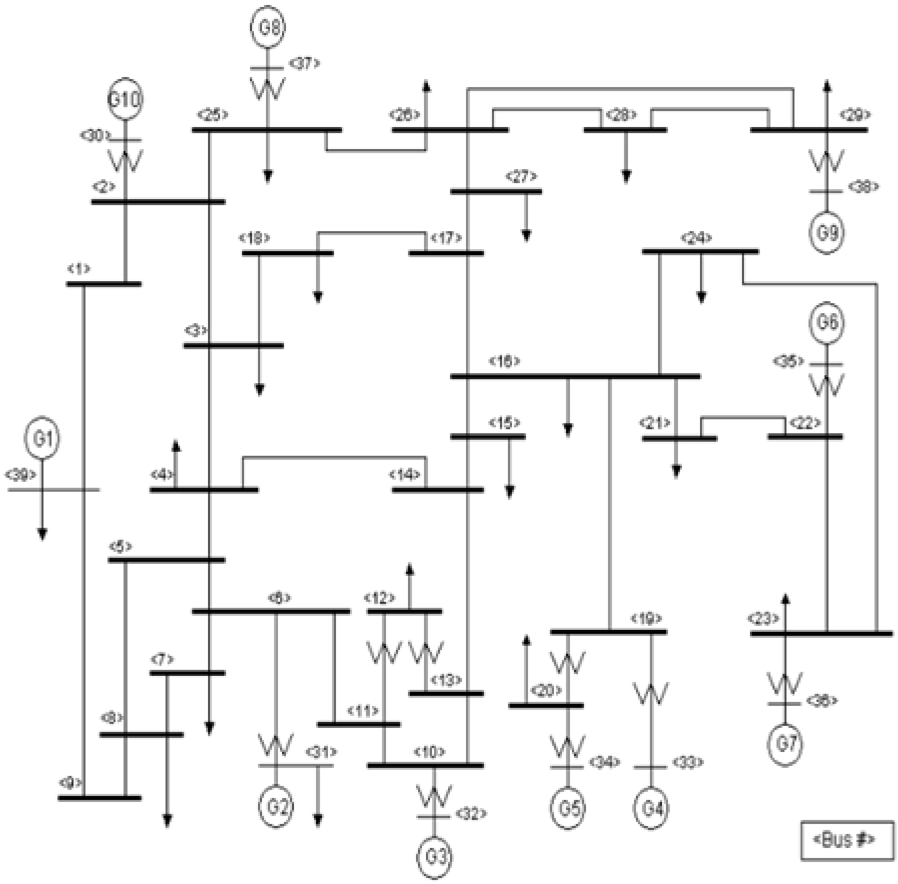


Figure 5: 39 Bus Model

- SEL Devices
  - SEL-421 (Protection Automation Control) (Figure 6) provides simple control of circuit-breakers and automation functions.
  - SEL-3378 (Syncrophasor Vector Processor) (Figure 7) acts as a logic engine between all of the SEL PMU's taking incoming data and sending predefined actions.

Figure 6: SEL-421

Figure 7: SEL-3378

Cyber System Software and Equipment

- MU Security Analyzer
  - The MU Security Analyzer (MU-4000) (Figure 8) gave us the ability to run automated denial of service and fuzz testing attacks on any device on the network. While the device is currently without a license, it could be used in the future to run attacks on the testbed.

Figure 8: MU-4000

Closing Summary

The goal of the SCADA testbed is to mimic real world SCADA systems and to analyze and document vulnerabilities that the industrialized SCADA system may have. These industrial control systems are used to monitor and control industrial processes in the world such as power generation, water treatment, oil and gas pipelines and many other critical systems. The electric power grid is a highly automated and complex network comprised of a variety of control systems, sensors, communication networks and many other forms of information all with the purpose of monitoring, protecting and controlling the power grid. Due to the continuous development of this automated network and many other critical systems, the threat of cyber based attacks are becoming more and more of a reality. These attacks could stop and damage many important systems that most of us take for granted. Therefore, security of the power grid and other critical automated networks (through the SCADA system) is one of the most impatient developmental issues we have today.

Implementation and Testing Results

Implementation

Both the Opal-RT simulator and SEL-421 relays have been implemented into the testbed. The Opal-RT simulator is operational and has been used to run tests of the ePhasorSim 39 Bus Model. Integration of the SEL-421 relays was also achieved. They are now connected to the system and can be tripped on and off.

The ePhasorSim 39 Bus Model we are using has been compiled and successfully run on the Opal-RT simulator. This allowed us to run tests on the operational model and simulator whose results will be show in the testing section following.

PSSE Testing

To allow for work to be done while we were waiting for the ePhasorSim 39 Bus Model, Siemens PSSE software was used to virtually simulate the 39 Bus Model. Initial values and limits were put into PSSE and tests were run on the model. We simulated line outages that would remove as much generation or load from the system with as little lines as possible.

- **N-1 Contingencies**

  For an N-1 contingency only one line is taken out of service at a time. This is the type of contingency that power transmission networks must plan and account for when designing or modifying a power system. The plot below shows voltage levels at connection points (busses) in the system after such a line outage.

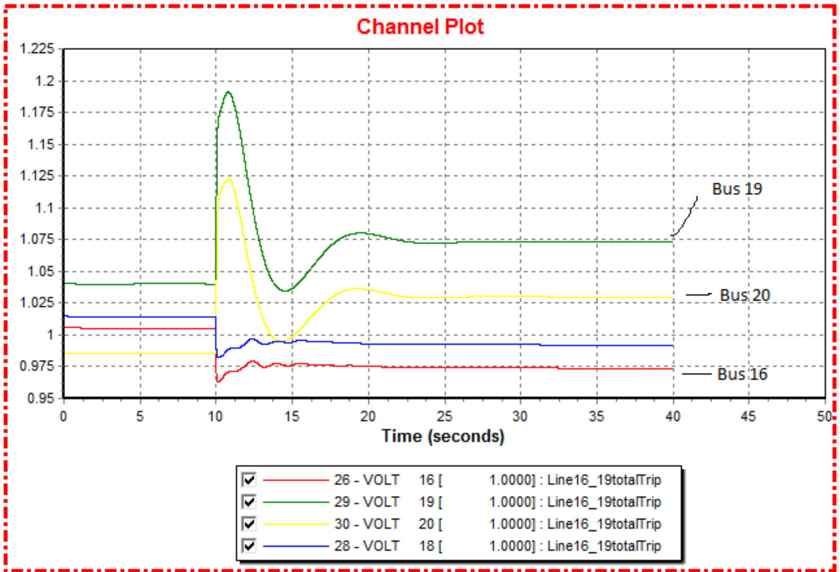


Figure 9: N-1 Bus Voltages

Notice how the voltage levels at the different busses either increase or decrease rapidly after the line is taken out of service. Because this system was designed with N-1 contingencies in mind, the voltages level out or "return to stability" after a short period of time. It is also important to look at how high or low the voltages go after the initial disruption. Voltages must stay within voltage limits set by NERC (North American Electric Reliability Corporation), and in this case they do remain in the set limits.

The next parameter to look at is generator rotor angles. These show whether a power generator is speeding up or slowing down to match the system load.

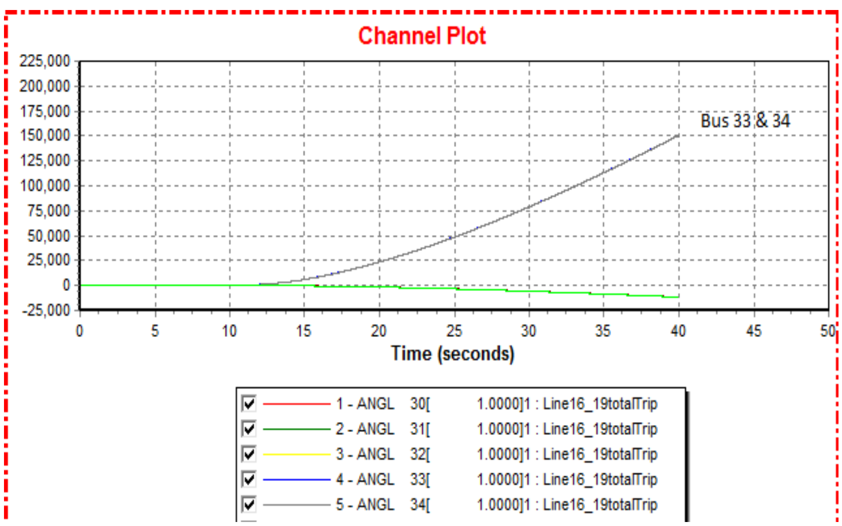


Figure 10: N-1 Generator Rotor Angles

It is obvious that two of the generators are accelerating while the others are slowing down. This is because in this case those two generators were cut off of the rest of the system and are generating too much power for the one load they are both serving. In a case like this, the generators would most likely be taken out of service to prevent damage to them. As a result the load being served by them would lose power. The rest of the generators in the system manage to slow slightly on account of the loss of load. Service to the rest of the system would be maintained.

- **N-2 Contingencies**

In a N-2 contingency, two line are taken out of service from the system. Most power systems are mot set up for this kind of contingency due to the costs necessary to prepare for it. The figure below shows the voltage levels during a N-2 contingency we ran in PSSE.

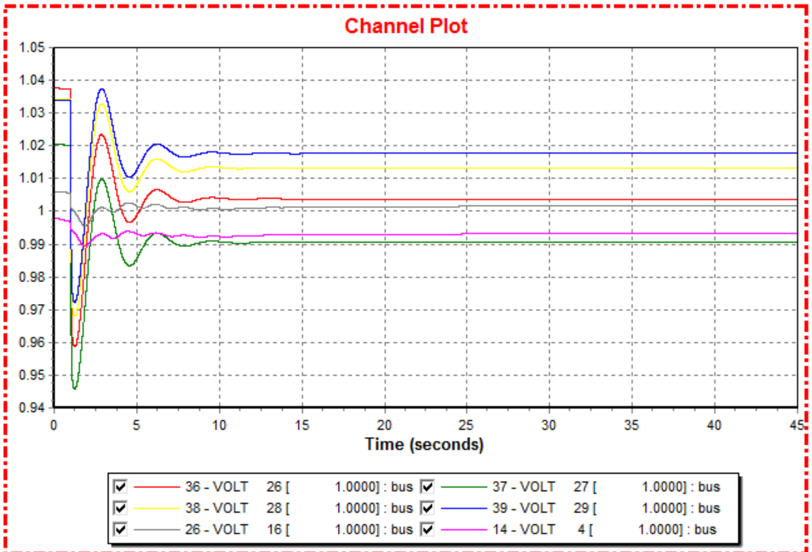


Figure 11: N-2 Bus Voltages

In comparison with the N-1 results from before, the voltages change more drastically and take longer to stabilize. The bottom voltage level drops below the 0.95 per unit (PU) value for a short period of time. This is outside of the voltage criteria and would be considered unstable. Looking at the rotor angles helps to better understand the effect of the line outages.

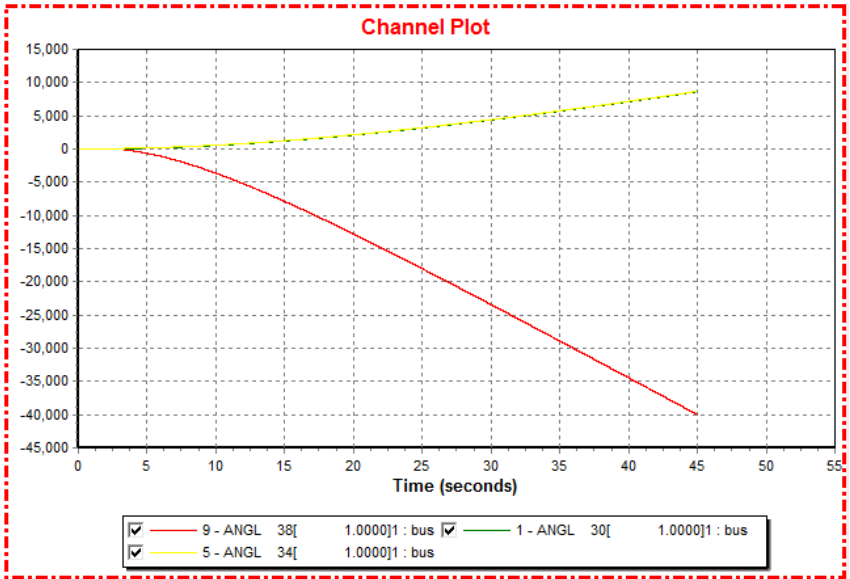


Figure 12: N-2 Generator Rotor Angles

Here the rotor angles of the generators separated from the main system slow down quickly. This is due to the fact that there was more load than generation in the section separated from the system. Again these generators would most likely be taken out of service to prevent damage, resulting in power outages to the loads on the separated section. The rest of the system remains stable despite the removal of the loads.

Opal-RT/ePhasorSim Simulations

Once we had a working 39 Bus model for ePhasorSim, we performed tests similar to those done with PSSE. Due to some differences in values between the PSSE model and the ePhasorSim model, the results were different for similar tests. These tests were performed while running the model on the Opal-RT simulator.

- **N-1 Contingencies**

  The first tests performed were again N-1 contingencies. The same lines were taken out of service as before and the results were analyzed after. Below are the voltages after the same single line trip as before.

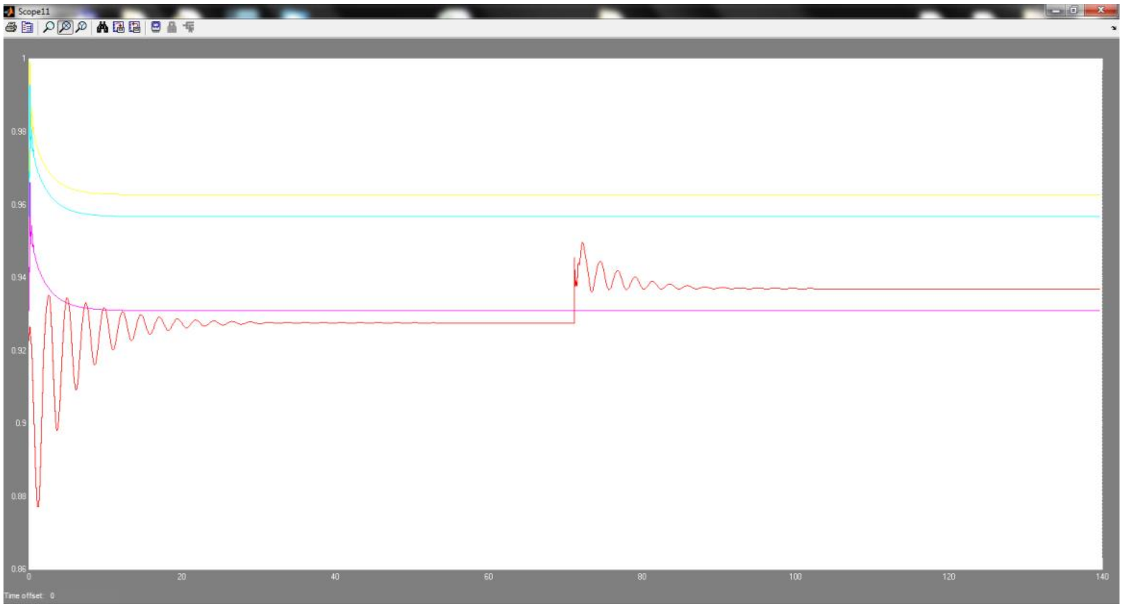


Figure 13: N-1 Bus Voltages

Initially the voltages level off to stability and then the line trip event is the spike in voltage in the middle of the plot. All of the values are within the NERC limits. The rotor angles are the real point of interest.

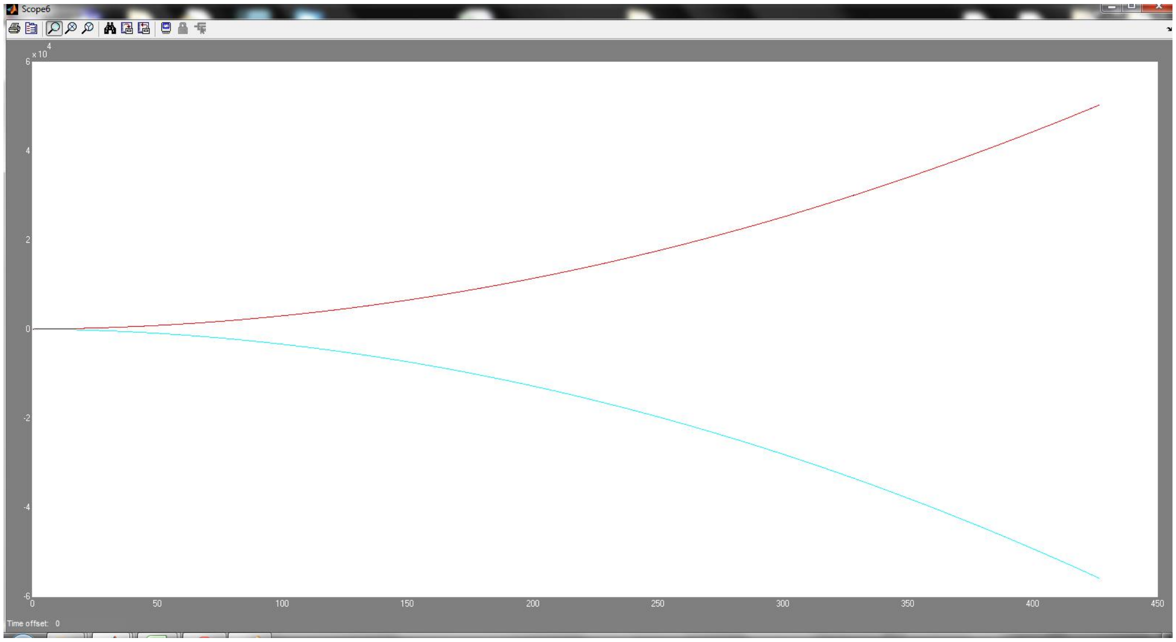


Figure 14: N-1 Generator Rotor Angles

This plot shows a major divergence of the rotor angles within the system. The system is definitely unstable would potentially result in a partial or whole system crash and loss of power.

- **N-2 Contingencies**

  As with the N-1 contingencies, the N-2 contingencies were repeated while running the 39 Bus model through ePhasorSin and Opal-RT. Results here were also quite different due to input differences. Here we can see the bus voltages when the same two lines as before were tripped.

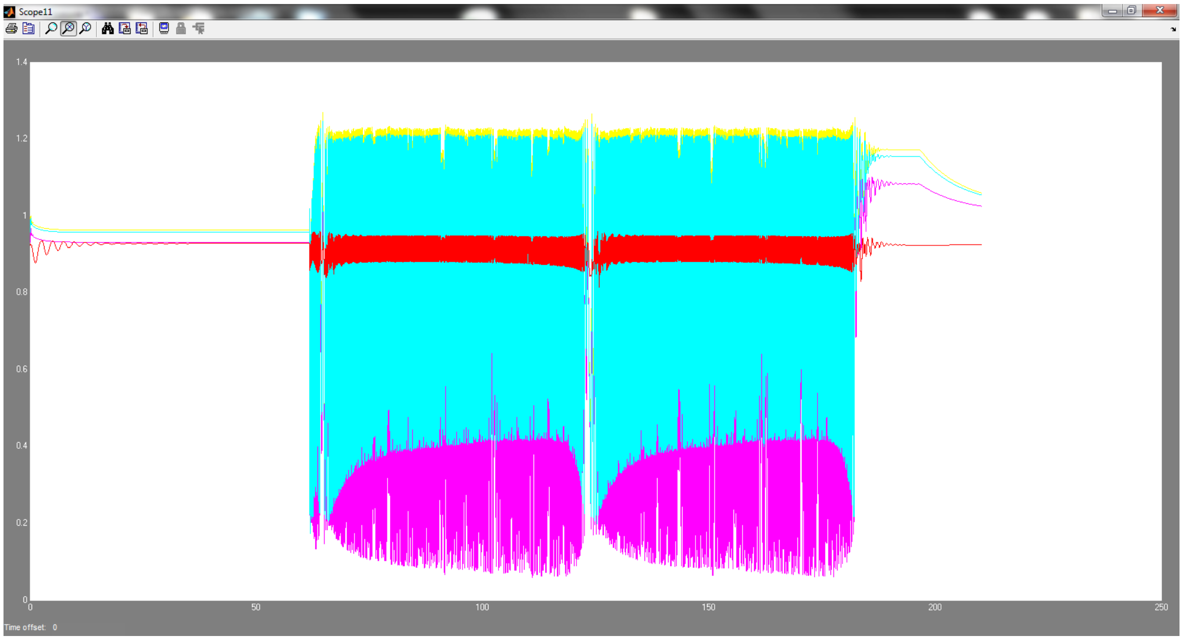


Figure 15: N-2 Bus Voltages

In this case there is major voltage instability within the system. The voltages are definitely beyond the limiting criteria for a period of time. At the end the voltages can be seen going back to stability after two oscillations. With voltage swings as severe as these, the system would most likely never reach that point. Either transmission operators would trip lines to correct the system, or left on its own the system would damage components and crash causing a loss of electrical service. Rotor angles in this case are not as drastic as seen below.

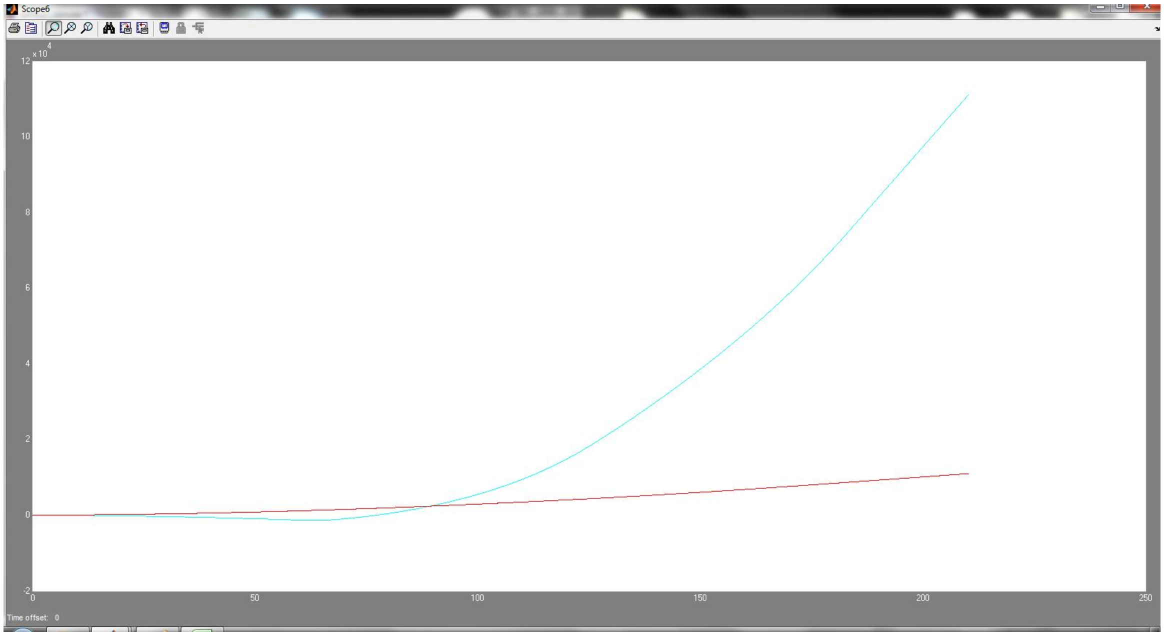


Figure 16: N-2 Generator Rotor Angles

While some of the generators are accelerating faster than others, the voltage instability in the previous plot would be the first to cause problems. Therefore the divergence is relevant, but in a real system it would be unlikely.

Appendix A

Step by Step Guide to Running a Simulation with ePhasorSim

This guide will go through the steps required in running the ePhasorSim 39 Bus model on the Opal-RT simulator. The steps are identical to how tests were run and results obtained for this project.

Configure Input File: Make sure the ePhasorSim input file is set up for the inputs and outputs you require.

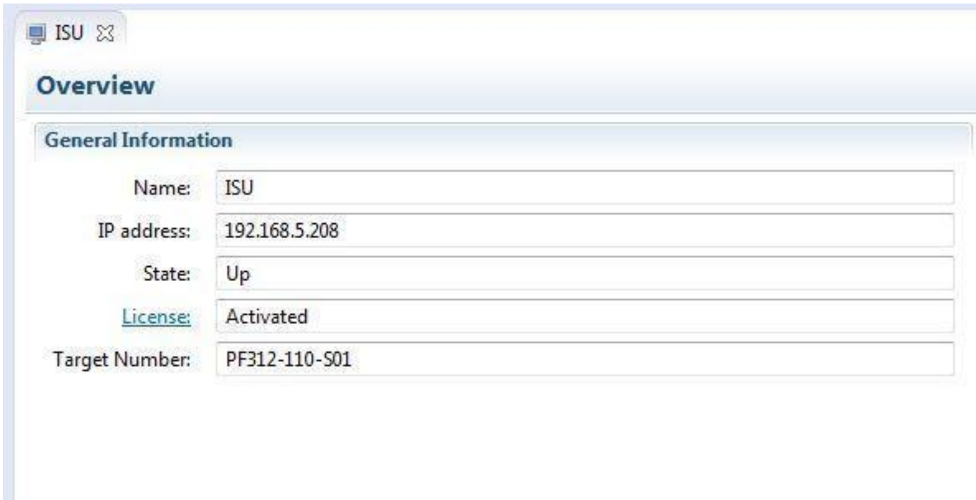
incoming	Line Trip	ln1/status
outgoing	Line Trip	ln1/status
incoming	Line Trip	ln30/status
outgoing	Line Trip	ln30/status
incoming	Line Trip	ln26/status
outgoing	Line Trip	ln26/status
incoming	Line Trip	ln11/status
outgoing	Line Trip	ln11/status
incoming	Line Trip	ln27/status
outgoing	Line Trip	ln27/status
outgoing	Bus_voltage	29/Vmag
outgoing	Bus_voltage	27/Vmag
outgoing	Bus_voltage	28/Vmag
outgoing	Bus_voltage	4/Vmag

Here the line trips you want to run must have an incoming and outgoing associated with them. Also any voltages or rotor angles you want to observe must be specified in this file. Once the excel file is configured properly one can continue.

Start RT-Lab: Start the program to be able to run models on Opal-RT.

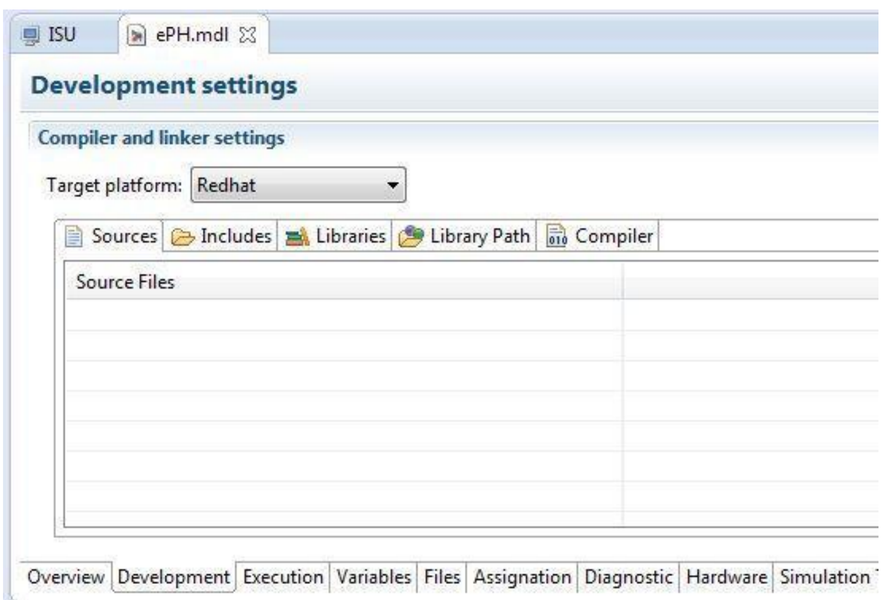
This program will allow a user to not only run an ePhasorSim model on the Opal-RT simulator, but also modify the model.

Step 3: Make sure target system is running.



Shown here is the target name, IP address, and status. Models cannot be run on Opal-RT unless the simulator in "up" and has an active license. If RT-Lab matches what is shown above, the simulator is ready.

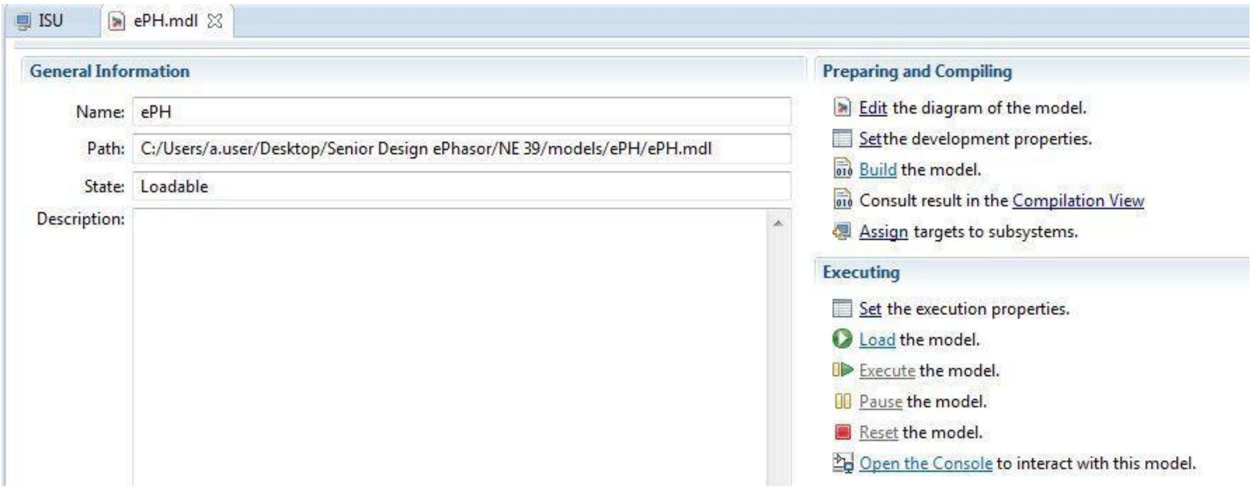
Step 4: Verify model is set up for Redhat.



The menu above can be viewed by clicking on your model from the left hand side in the RT-Lab navigation window. Once here select the "development" tab shown in the image above.

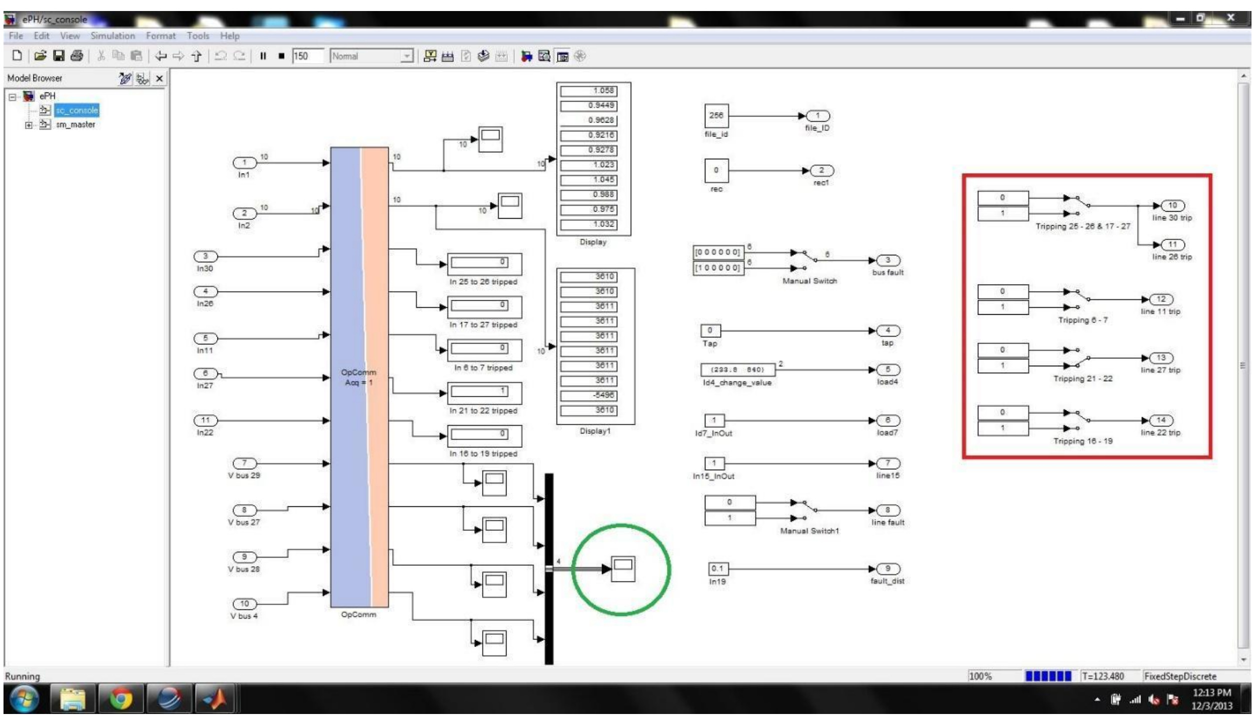
Verify that the target platform is Redhat as this is what operating system is running on the Opal-RT simulator. Next click on the "overview" tab.

Step 5: Build, Load, and Execute the model.



Now that the "overview" tab is selected, choose the "Build" option from the preparing and compiling selections. This will convert the model so that Opal-RT can run it. Then choose "Load" from the executing options to load the model onto the simulator. Finally, select the "Execute" option under executing to run the model.

Step 6: Performing tests on the model.



The console shown above should have opened on its own. Here you can specify which line to trip depending on how you set up the input file. Our line trips are shown in the red square. Once a line is tripped, let the system run for as long as you want to simulate as this a real time simulation. When running is complete select the display circled in green to view the parameters specified. This is where the voltage plots were taken from during testing.