Attack Graph Based Metrics for Identifying Critical Cyber Assets in Electric Grid Infrastructure

Chen Huo
Panini Sai Patapanchala
Dr. Rakesh B. Bobba
Dr. Eduardo Cotilla-Sanchez

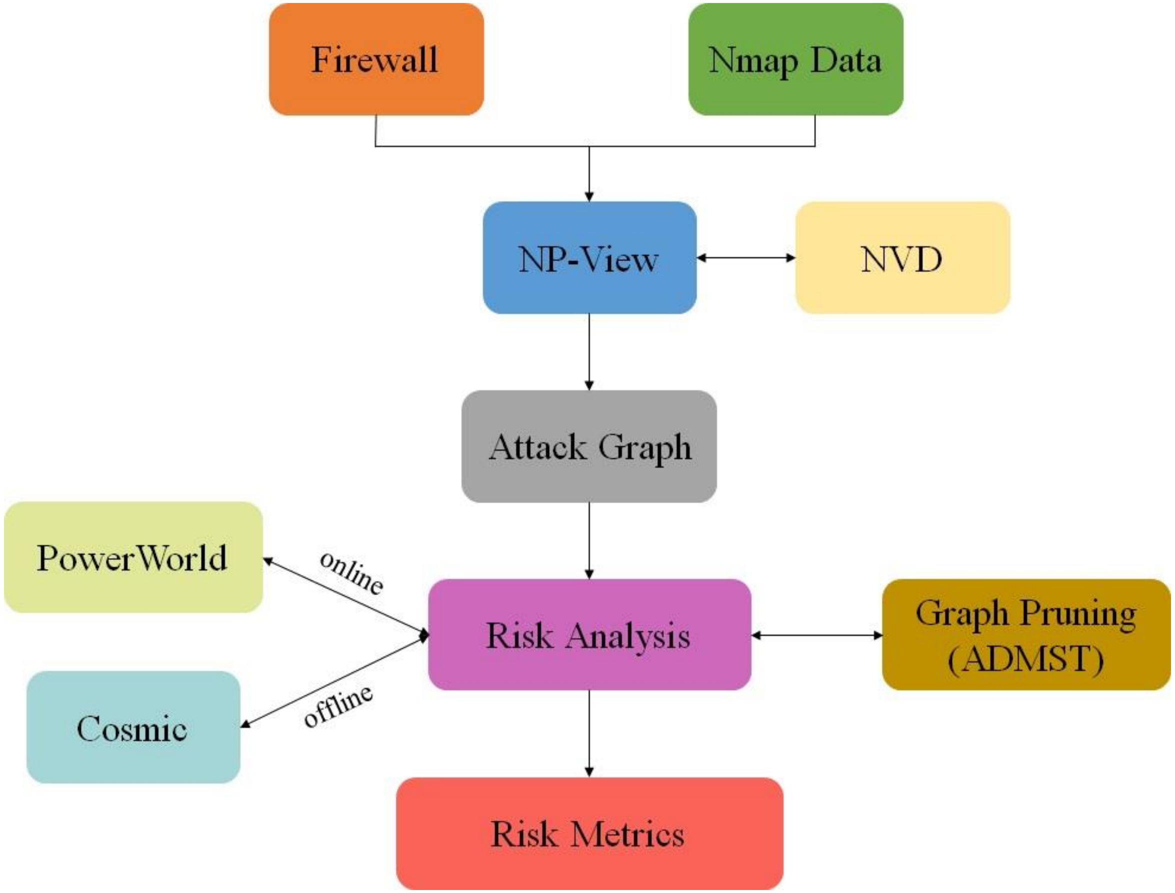
Oregon State University

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Our Goal

- **Short-term**: Developing a method that takes cyber-physical dependency into account and assesses the risk of cyber-attack induced cascading failures.
- **Long-term**: Providing real-time situational awareness of threat to the system by characterizing "how far or close" a given grid system is to a cyber-induced cascading failure, and how to mitigate it.

Research Overview



Data Needed

- Physical Model
  - Bus-Branch -> Node-Breaker
  - Protection Schemes
- Cyber Model
  - Network Topology
  - Access/Firewall Rules

Previous Work

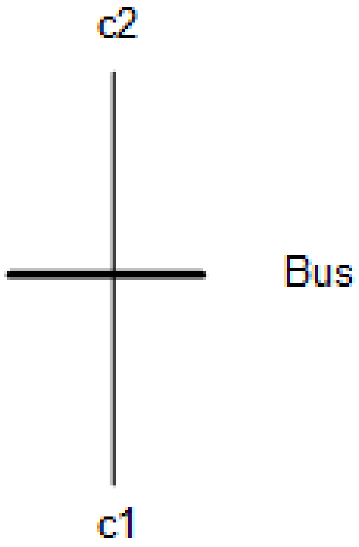
- Cosmic-based Cyber Physical Models for IEEE 9-bus and 39-bus cases.
- Risk Metrics for:
  - Target Nodes (Ex: Relays)
  - Intermediate Nodes (Ex: HMIs)
  - Source Nodes (Ex: Attack Origins/Jump Hosts)
  - Total Security Exposure

Current Focus

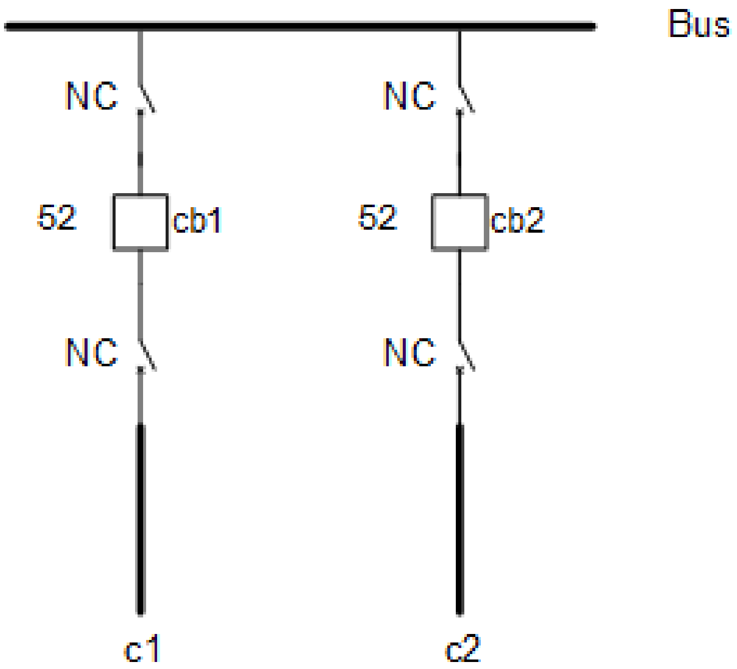
- Risk Metrics for Cascading Outages
  - Compare configurations with respect to cyber risk for cascading outages

Single-bus-single-breaker Configuration

Bus-branch model

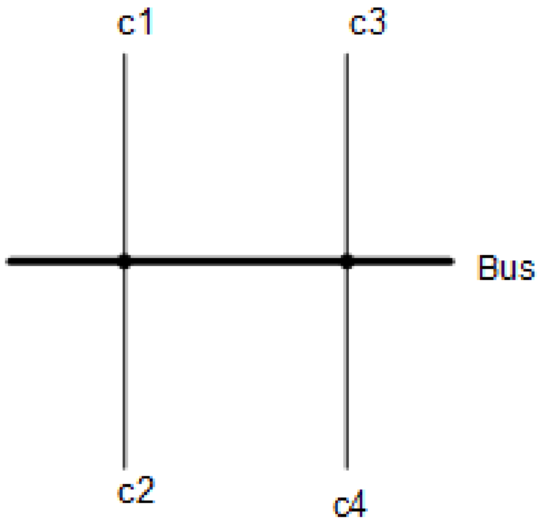


Node-breaker model

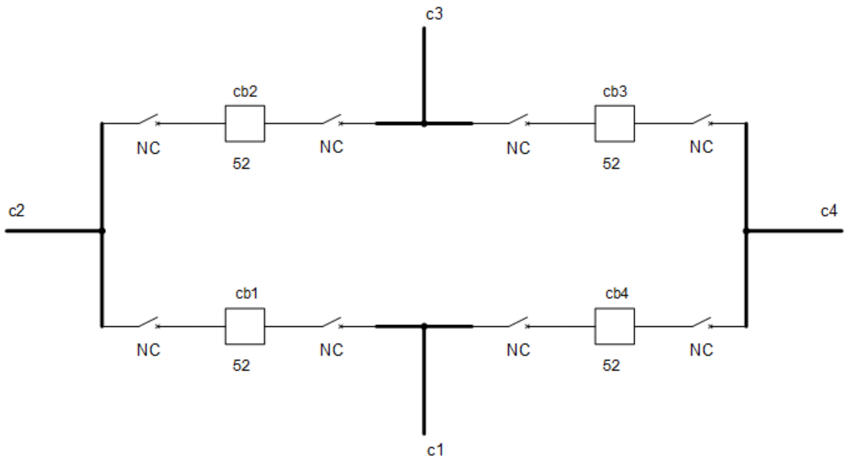


Ring-bus Configuration

Bus-branch model

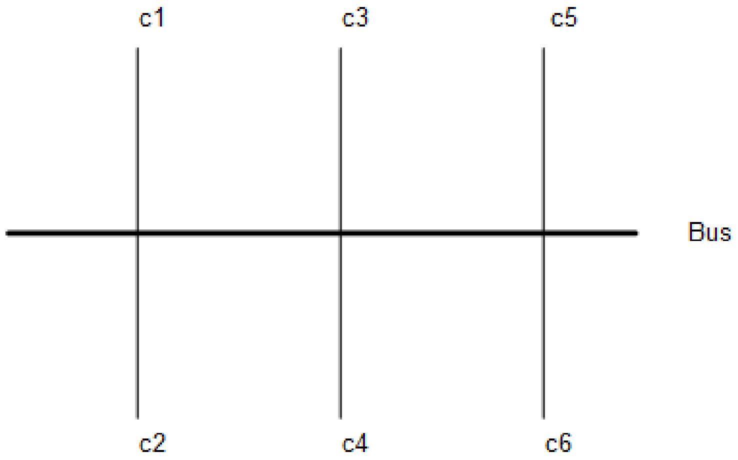


Node-breaker model

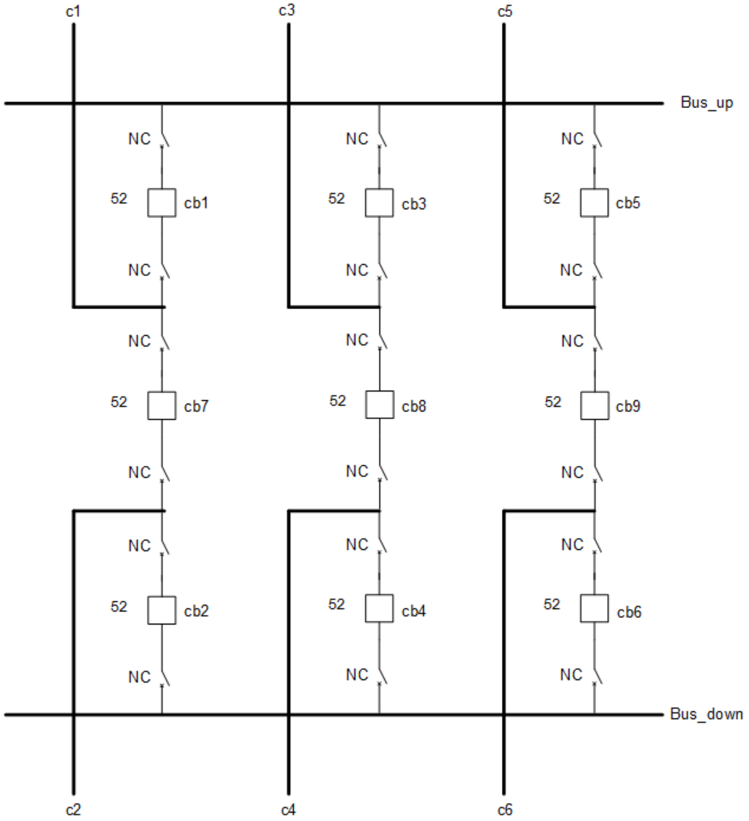


Breaker-and-a-half Configuration

Bus-branch model

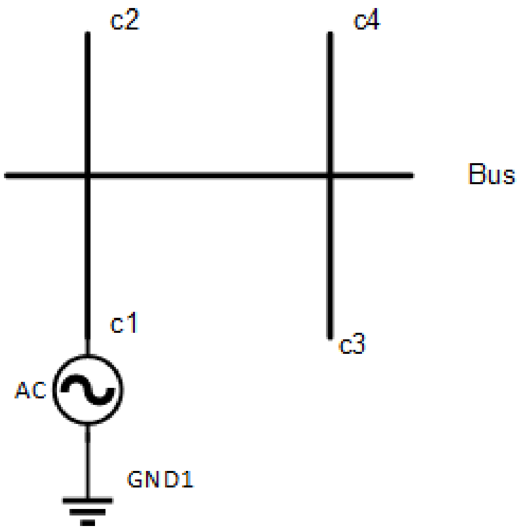


Node-breaker model

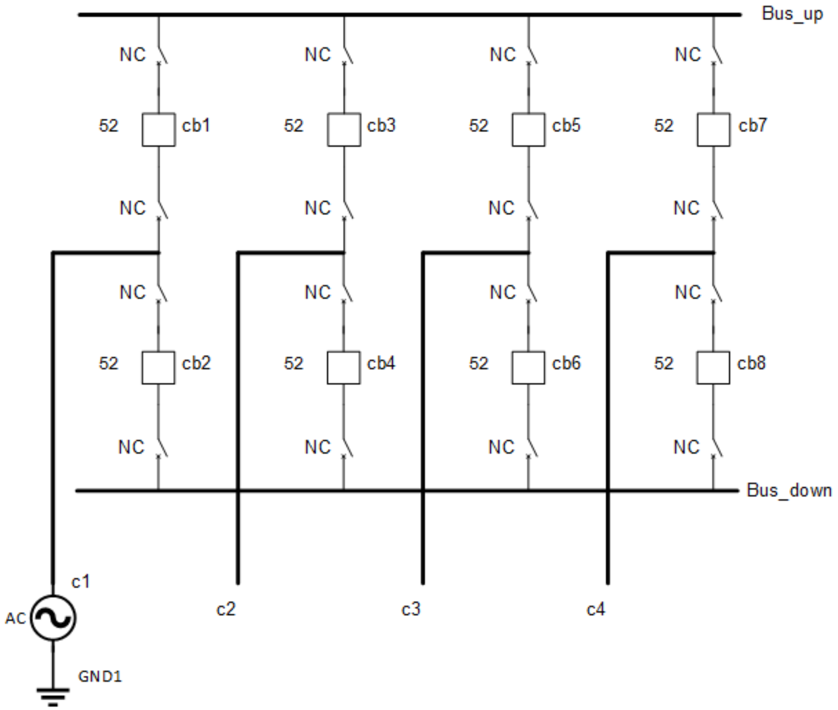


Double-bus-double-breaker Configuration

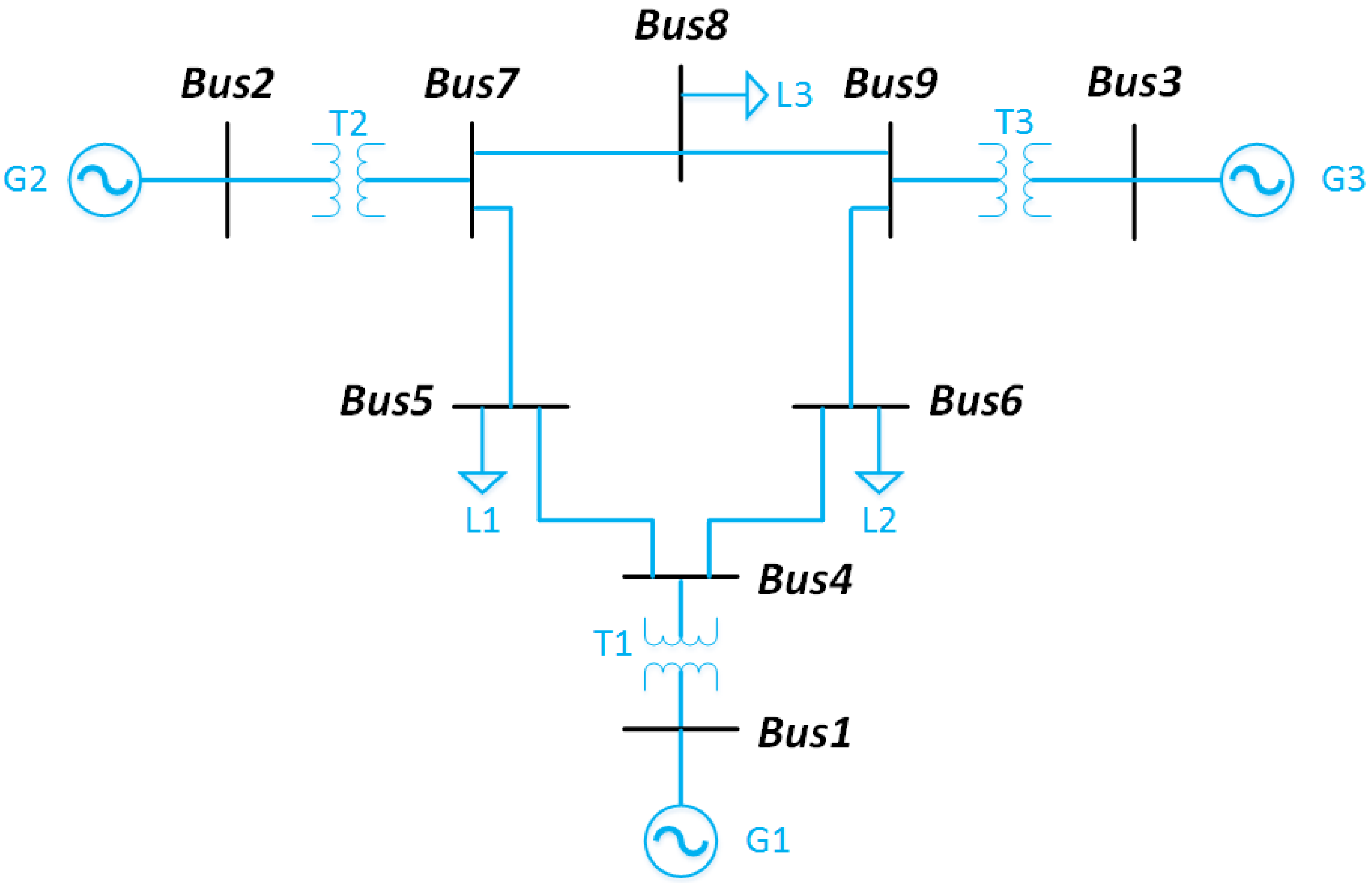
Bus-branch model



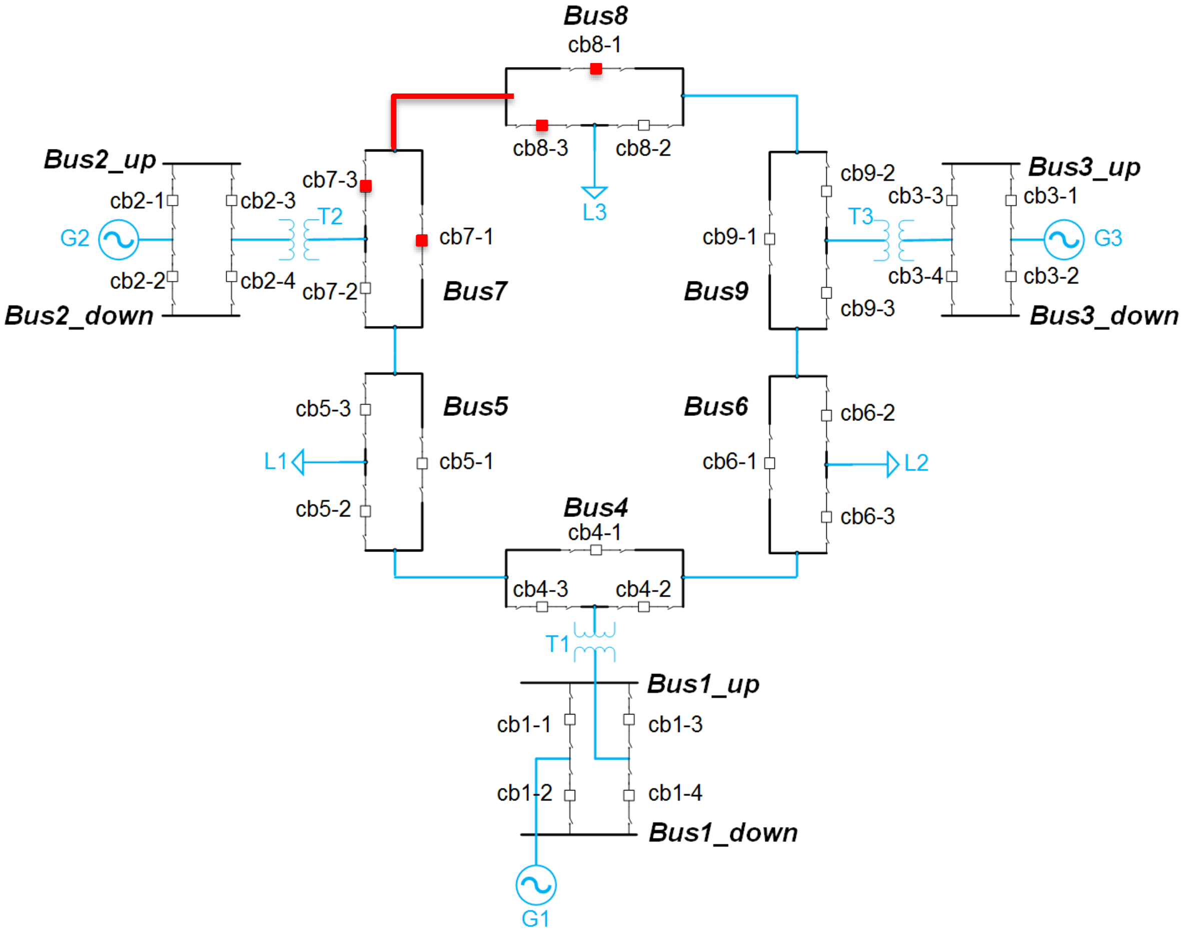
Node-breaker model



Example: IEEE Case 9



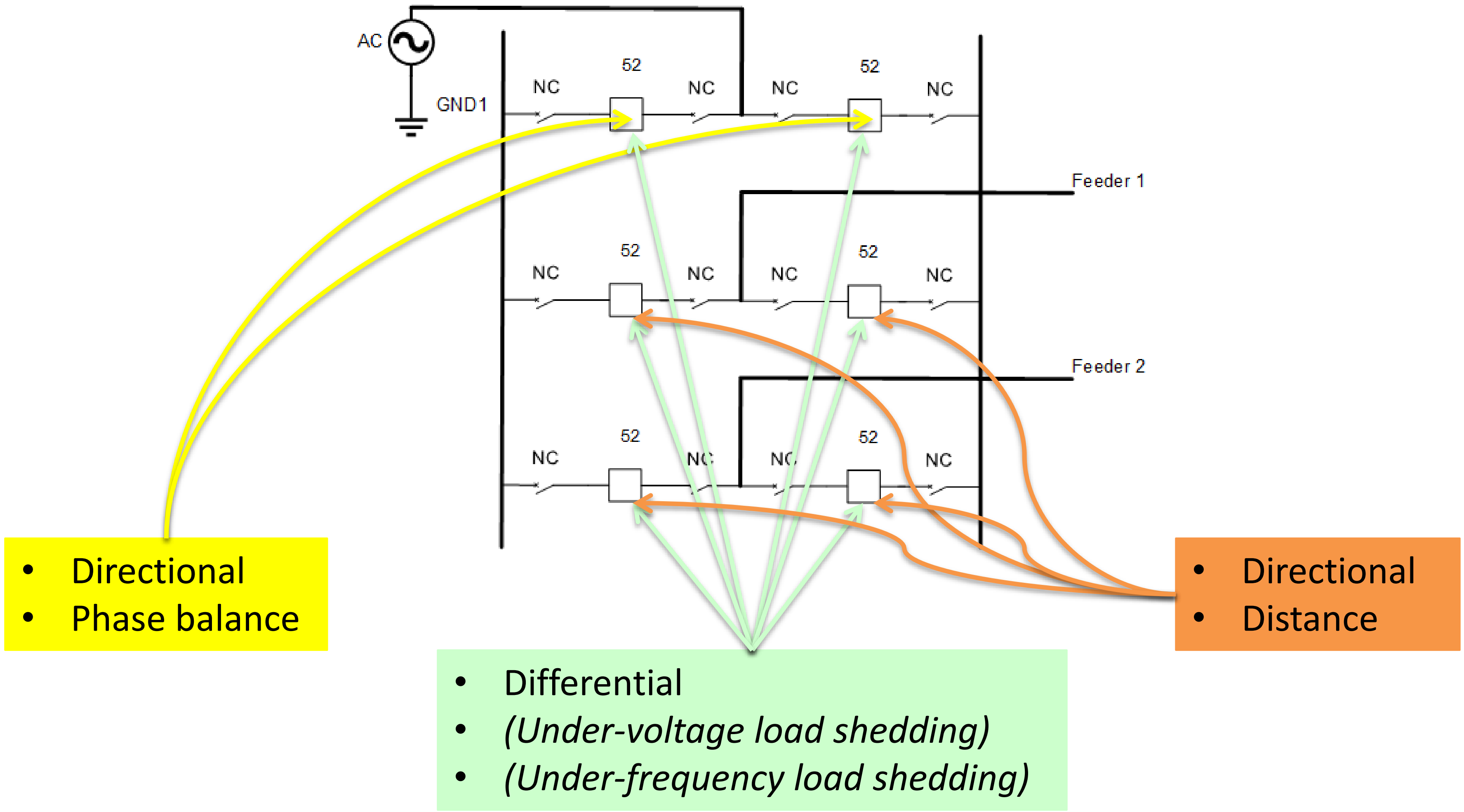
Example: IEEE Case 9



Types of Protection

- Overcurrent & directional overcurrent
- Under-voltage load shedding
- Under-frequency load shedding
- Distance
- Differential
- Phase balance

Protection Scheme Templates



- Directional
- Phase balance

- Differential
- *(Under-voltage load shedding)*
- *(Under-frequency load shedding)*

- Directional
- Distance

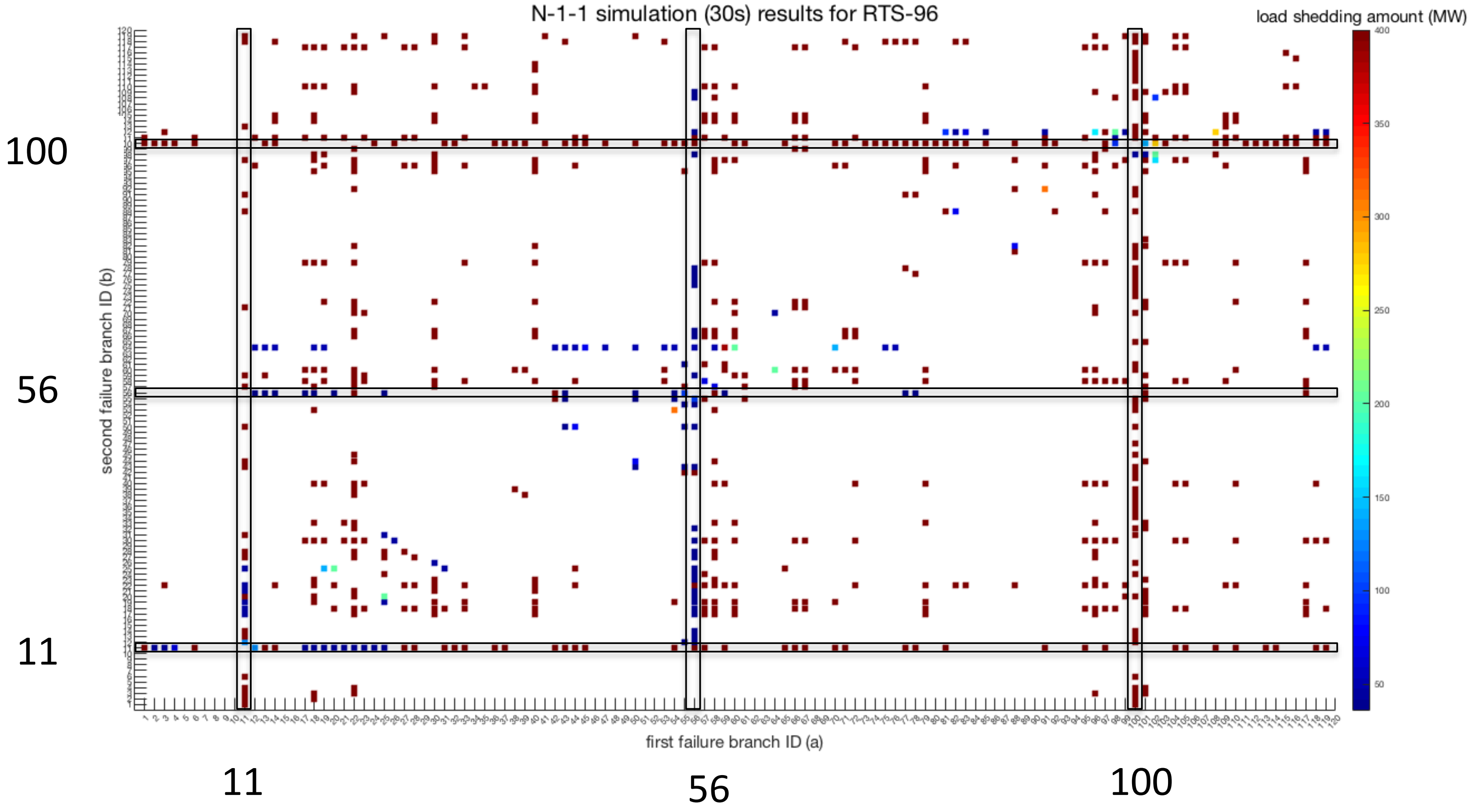
Cyber Topology

- Synthetic but realistic network topology and access rules
- Synthetic but realistic vulnerability distributions

RTS-96 N-x Simulation Procedure

- N-1 simulations:
  - Secure for 93 out of 120 branch failures (with baseline RTS-96 data).
- N-1-1 simulations:
  - There are 7,140 combinations for 120 choose 2, and therefore, 14,280 permutations.
  - From 14,280 cases choose both first and second failure belong to those 93 secure branches.
  - 798 out of 14,280 N-1-1 simulations with two N-1 secure branches failures cause a certain physical impact.

N-1-1 Results


N-1-1 simulation (30s) results for RTS-96
load shedding amount (MW)
400
350
300
250
200
150
100
50
second failure branch ID (b)
first failure branch ID (a)
100
56
11
11
56
100

N-1-1 Results

First Failure		Second Failure	
Branch ID/From-To	Count for Times	Branch ID/From-To	Count for Times
100/312-323	58	100/312-323	60
22/112-123	38	11/107-108	51
56/209-212	36	101/313-323	32
11/107-108	30	22/112-123	28
101/313-323	30	18/110-112	26

Currently, we are working on…

- Fixing Cyber topology data format for RTS-96
- Top k actions to improve network's security posture for cascading outages
- Cyber topology for Poland model (2000+ buses)

Thank You!

&

Questions?