ICS-CAPE

Industrial Control Systems –
Cyber Attacks and their Physical Effects

Mary Klett
Idaho National Laboratory

ICS-CAPE

- Idaho National Laboratory Directed Research and Development (LDRD)
- Library of process maps
- Identify data points in order to examine the functional consequence of a cyber attack
- Tie into existing technology and methodologies in order to determine the cumulative consequence

ICS-CAPE

- Idaho National Laboratory Directed Research and Development (LDRD)
- Library of process maps
- Identify data points in order to examine the functional consequence of a cyber attack
- Tie into existing technology and methodologies in order to determine the cumulative consequence

Innovative Aspects

- This research will assess and enhance applicability of using a universal model to delve into components typically used within an industry to enable detailed evaluation of the impact of an attack or failure of a specific asset.

- The universal model will allow for rapid analysis of metrics

- It will identify concrete consequences of a cyber attack

- It will enhance understanding of the potential for cascading impacts of a cyber attack on a specific component or asset

Process Mapping

- Identification of Industry and Infrastructure Type
- Open Source Research
- Subject Matter Expert Interviews
- Identification of Critical Components
- Subject Matter Expert Approval

Substations

Circuit Breakers and Switches

Air circuit breakers
Carbon Dioxide circuit breakers
Gas circuit breakers, SF6
Hybrid circuit breakers
Oil Circuit breakers
Vacuum circuit breakers
Circuit Switchers
Disconnect switches

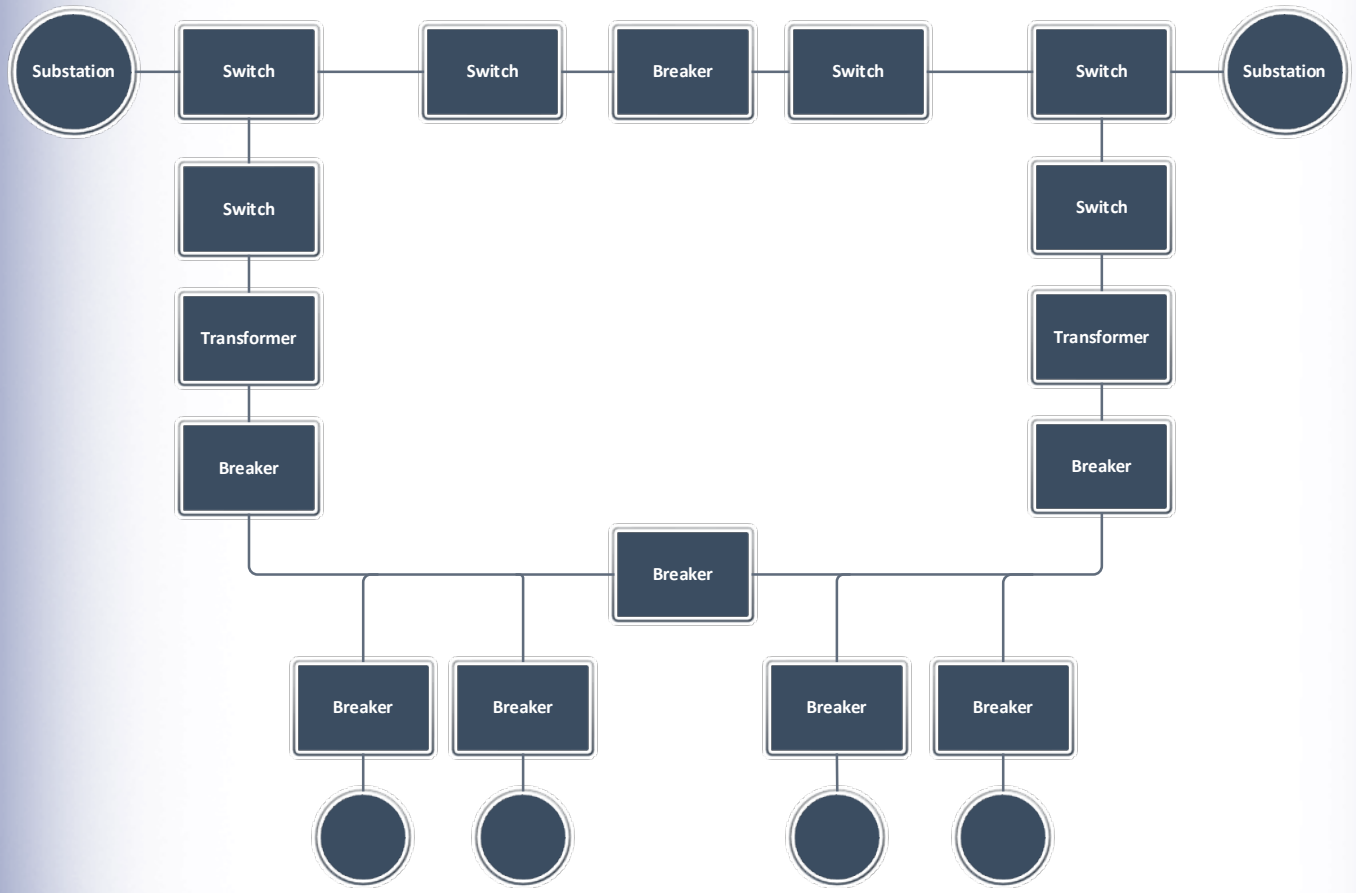
Relays

Distance Relay
Differential relays
Reverse Power Relay
Overcurrent Relay
SEL 421
SEL 3620
SEL 451

Characteristics Reviewed

- Criticality to operations
- Inside or outside SCADA
- Function
- Functional impact
- Typical redundancies
- Common safeguards
- Impact of short term shut down
- Long term consequence if destroyed

Mapping Profile



Data Points

1 Is this component critical to operations?
- No
  - Does this component support other components that are critical to operations?
    - No
      - Exit questions for this component
    - Yes
      - Continue to Q2
- Yes
  - Continue to Q2

2 Are there redundancies in place?
- No
- Yes
  - Is the redundancy on the primary network, a separated parallel network or both?
  - Is the redundancy accessed: remotely through an HMI, locally through an HMI, or locally physical?
  - What is the length of time it takes to get a redundancy operational?
  - What is the length of time it takes to get the component back to operational?

3 Are there safeguards or countermeasures in place?
- No
- Yes
  - Is the safeguard on the primary network, a separated parallel network or both?

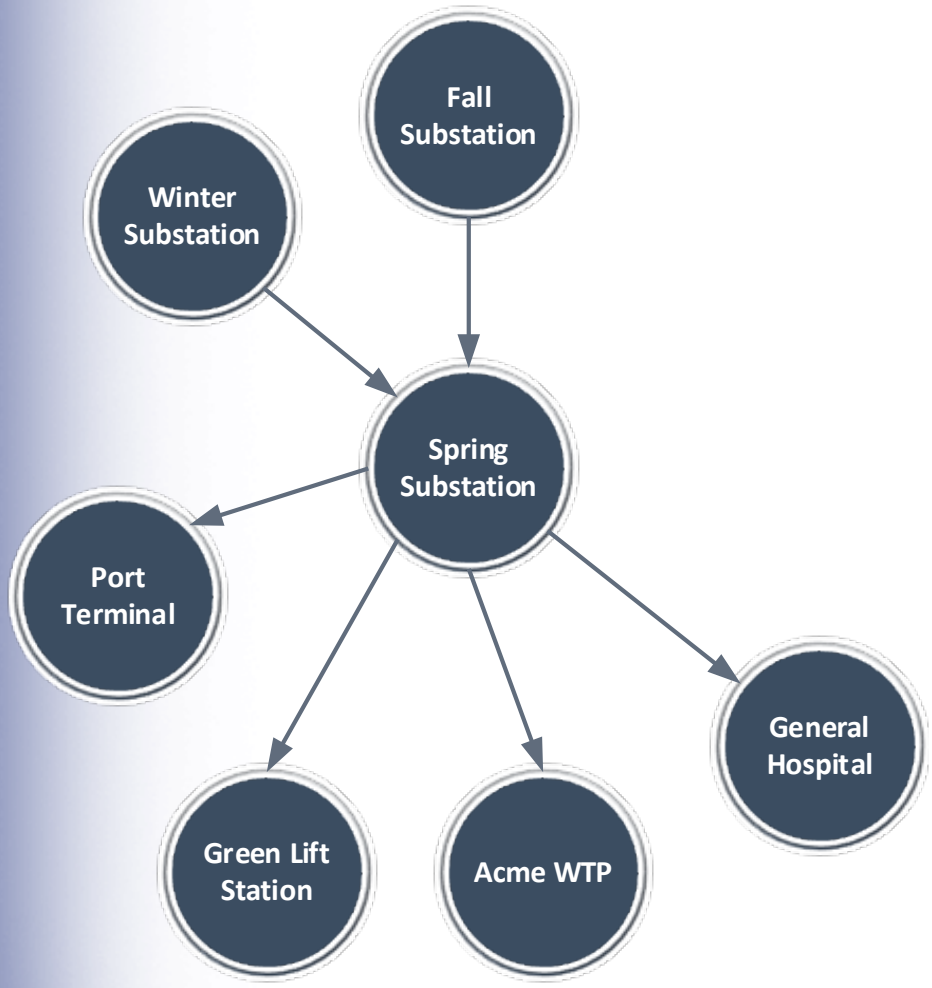
Assessment

- Assess an actual facility
- Select most accurate mapping profile for asset type
- Make updates as appropriate
- Collect data points
- Determine functional consequence

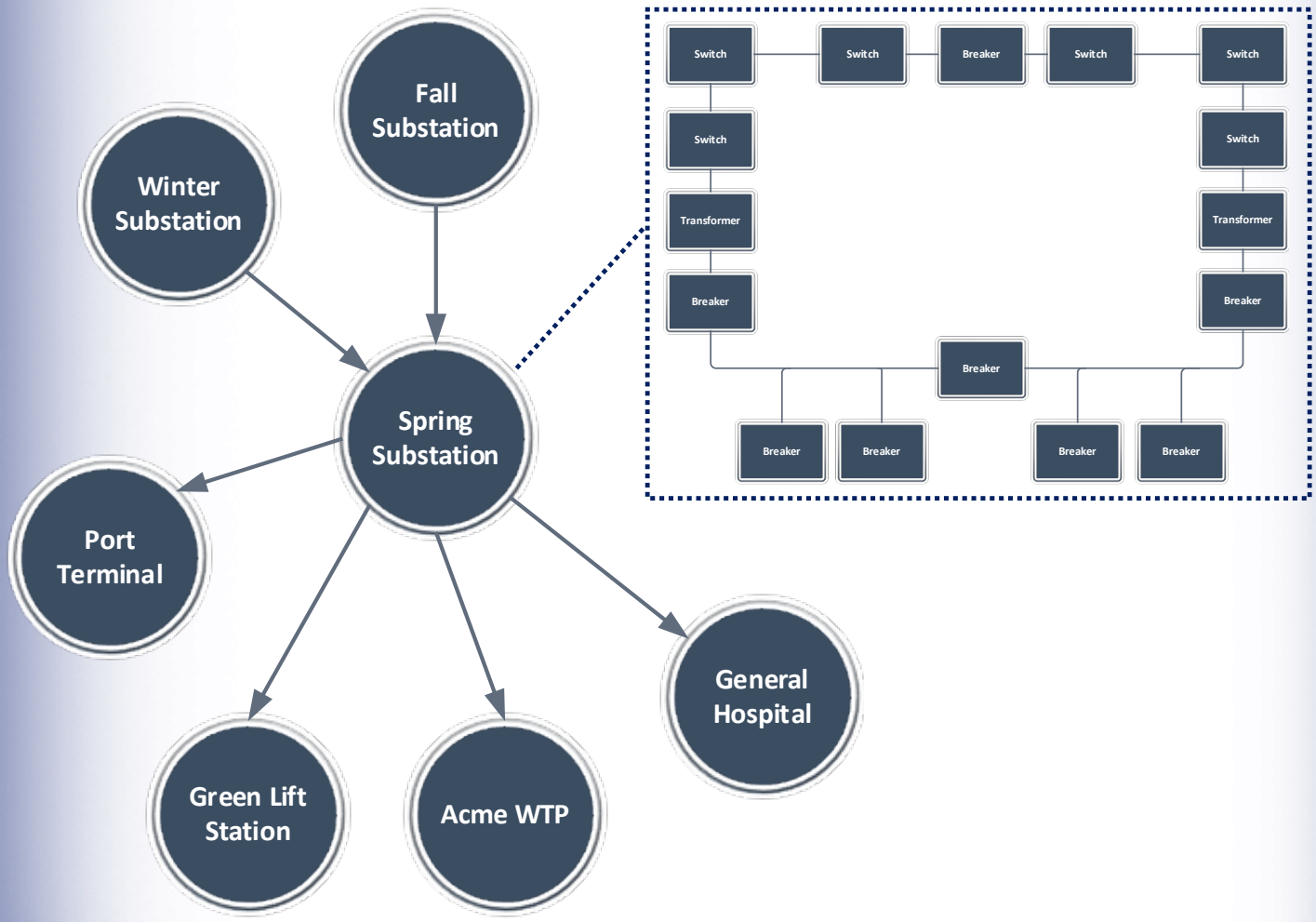
Cascading Consequence

- Leverage existing technology and methodology used for dependency analysis
- Dependency profiles exist and are applied to specific facilities in order to determine the strength and confidence of a dependency
- Mapping Profiles are built using the same concept as the dependency profiles and allow us to go one level out and then down which leads to calculating cumulative consequence

Cascading Consequence



Cascading Consequence



Collaboration

- University of Illinois at Urbana-Champaign
  - Expand and utilize existing ontology library
  - Integration with Cyber-Physical Topology Language (CPTL)

Next Steps

- Build library
  - Substations nearing completion
  - Water treatment plants in progress
  - Additional industry and infrastructure types to be researched
- Conduct actual assessment for feasibility review
  - Refine and review functional consequence calculations that are currently being developed
- Develop user interface
  - Translator from CPTL to AHA

Questions or Comments

Mary Klett
Homeland Security Division
Idaho National Laboratory
mary.klett@inl.gov