CyPSA

Cyber Physical Security Analysis

PowerWorld WECC User's Group Meeting

March 16, 2016

ILLINOIS

Oregon State UNIVERSITY

RUTGERS UNIVERSITY

PowerWorld Corporation

CyPSA Team

ILLINOIS

Kate Davis
Mouna Bamba
Robin Berthier
David Nicol
Edmond Rogers
Bill Sanders
Pete Sauer
Olivier Soubigou
Gabe Weaver

Oregon State University

Rakesh Bobba
Panini Patapanchala
Vishnu Priya Rayala

Rutgers University

Saman Zonouz
Luis Garcia

PowerWorld Corporation

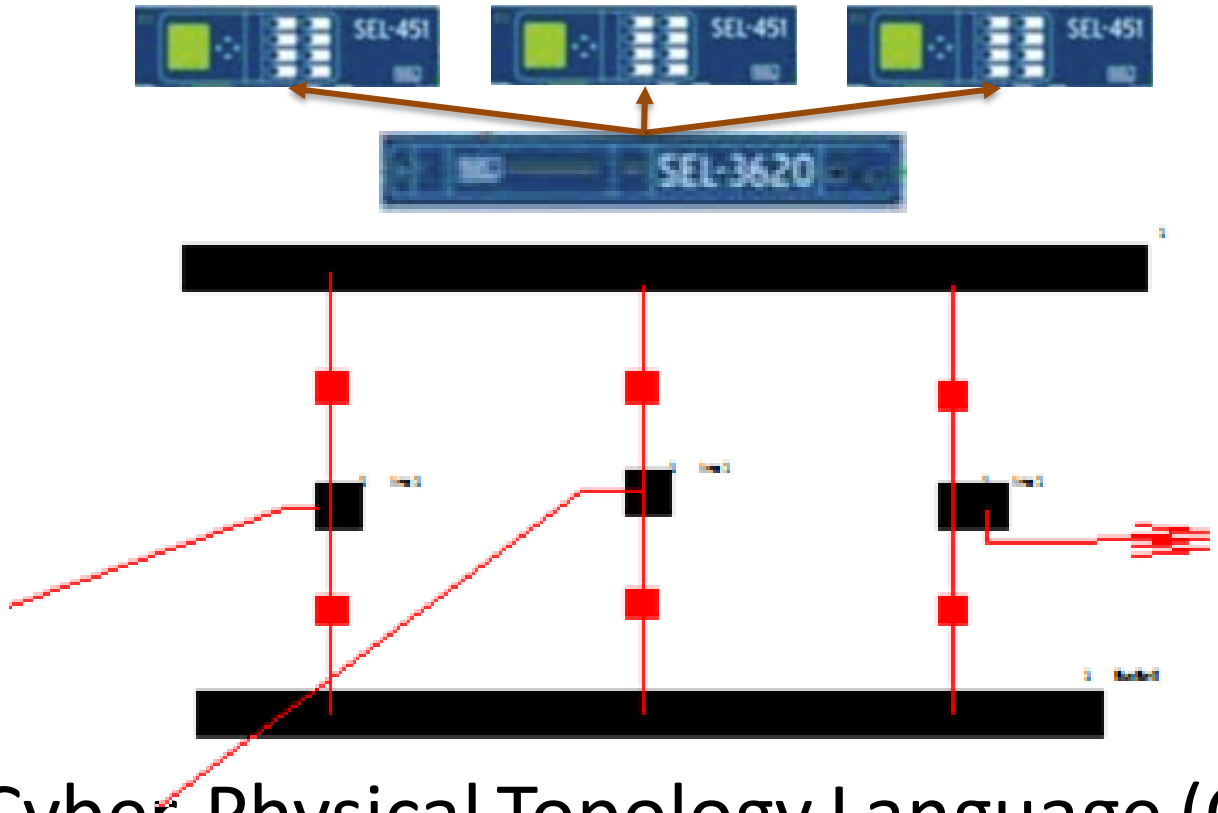
Matt Davis

ARPA-E

Sameh Elsharkawy
Josh Gould
Tim Heidel
Eric Desrosiers

http://publish.illinois.edu/iti-cypsa/

Inventory Management



Cyber-Physical Topology Language (CPTL) :
https://github.com/ITI/cptl-power/wiki

New PowerWorld Objects

- **CyberDevices**: Access breakers via their respective relays
- **CyberLinks**: Connections
- AUX format and CPTL JSON support

New PowerWorld Objects

- Process “TRIP” relay outputs and breaker connections
- Interface with CyPSA via socket protocol
- New “OpenFromCyber;” script command

OpenAllFromCyber([CyberDevice “xx.xx.xx.xx"]);

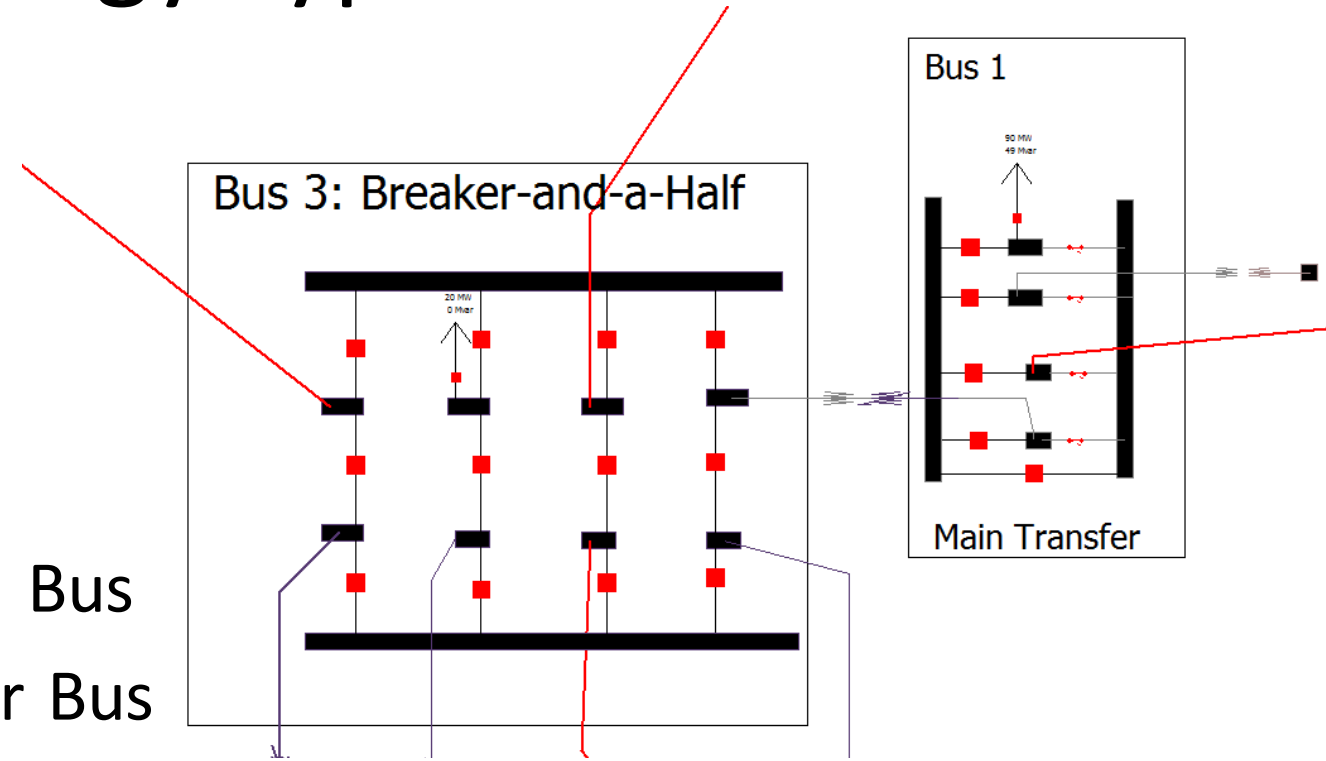
Relays, LORs, Comm. Proc. Support

- When a ***Lock-out-Relay (LOR)*** is encountered, look up its identifier in the case's cyber objects, and obtain the list of connected breakers

- ***Communications processors*** are treated similarly

- State the name or address of the device to be accessed in the output field following the "TRIP" keyword:
  - "TRIP comm procx."

Six Topology Types in Simulator



- Single Bus
- Sectionalized Bus
- Main Transfer Bus
- Ring Bus
- Breaker and a Half
- Double Bus Double Breaker

Power Topology Model Expansion

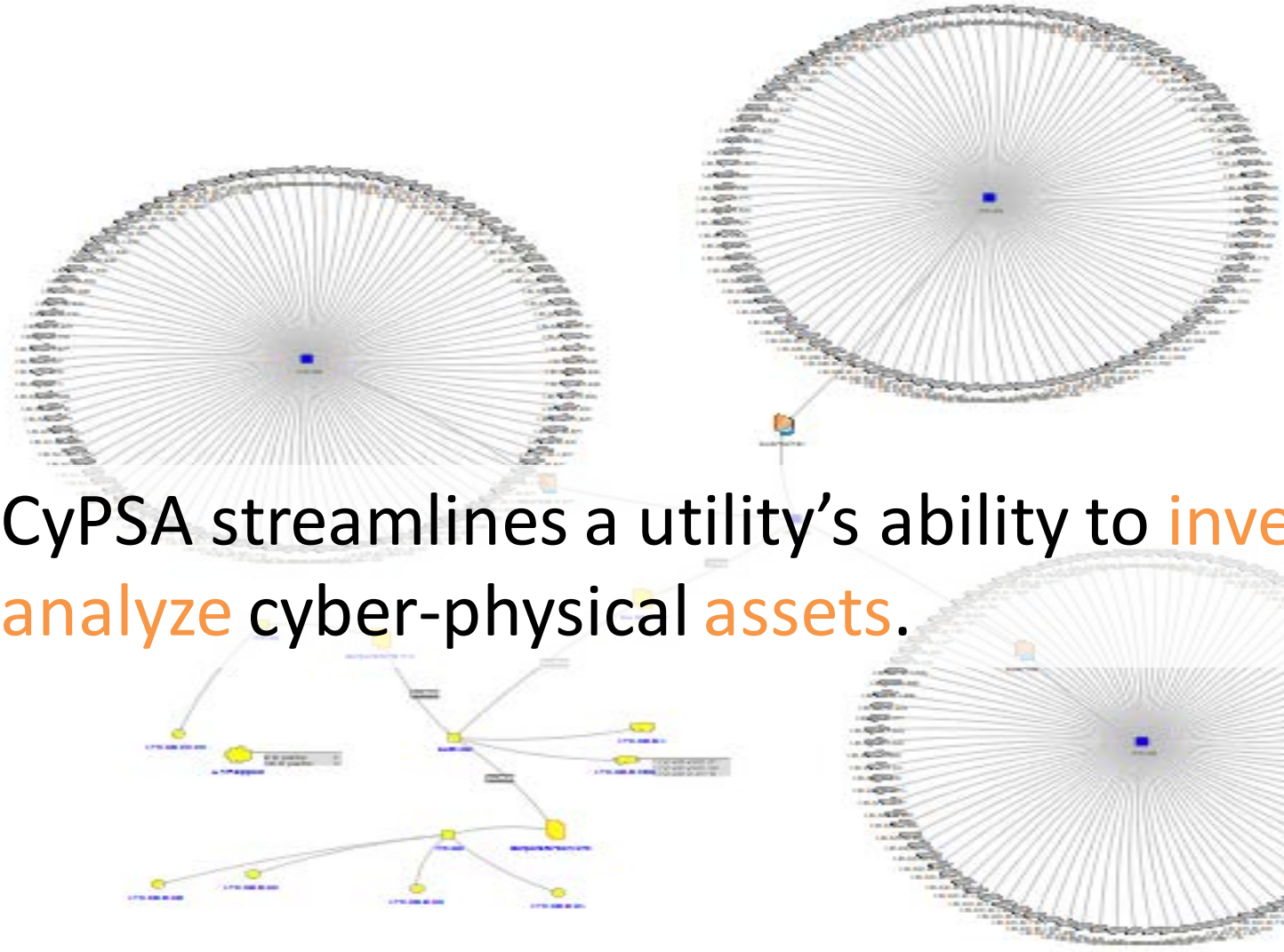
- New script commands
  - *ExpandAllBusTopology;* – convert all bus topologies to types indicated in the custom string 5 field
  - *ExpandBusTopology(Bus ID, Topology Type);* - convert single bus to the indicated type

Protection Templates for Model Expansion

- Relay configurations created for each bus topology
- Execute *ExpandBusTopology();* WITH interconnections
- Export results in any format; i.e., ***CPTL***
- Takes manual effort out of assigning interconnections for academic study

PowerWorld Cyber Connectivity

- Cyber object support is intended to help users
  - Develop and test ***realistic*** templates for protection layouts
  - ***Manually assign*** protection layouts
  - ***Map*** RTU/relay device to cyber network IP
  - Perform cyber-physical analysis and situational awareness: ***CyPSA***



CyPSA streamlines a utility's ability to inventory and analyze cyber-physical assets.

Use Case: Asset Ranking

Description	Analyze all attack paths for a given set of assets Rank based on both *impact* and *cyber exposure* • *Impact*: power system performance index based on severity metrics • *Cyber exposure*: metrics include the number of potential attack paths and ease of realizing an attack
Role	**Manager**
Inputs	• A model • A source of vulnerability information • A set of assets to be ranked
Outputs	• A list of attack paths annotated with and ordered by a ranking

CyPSA Control Panel

CyPSA Home Model Action Panin

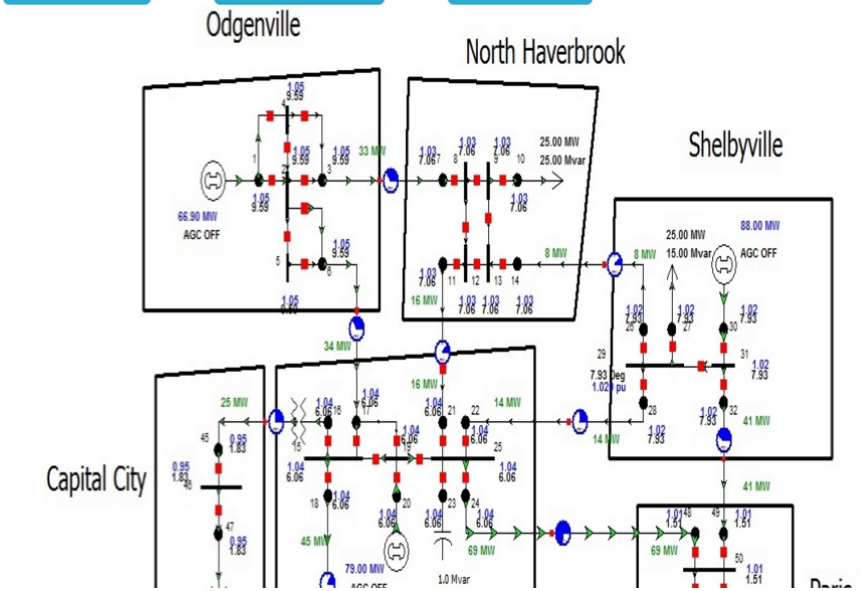
Home / Cypsa Analysis Project

IP Address	Type	Performance Index (Curr/Prev)	Cyber Cost (Curr/Prev)	Security Index (Curr/Prev)
10.31.1.103	destination	85.50/85.50	279.38/279.38	7.15/7.15
10.31.1.102	destination	49.10/49.10	279.38/279.38	4.10/4.10
10.39.1.22	intermediate	70.97/70.97	654.39/654.39	3.90/3.90
10.31.1.101	destination	30.34/30.34	279.38/279.38	2.54/2.54
10.31.1.104	destination	30.35/30.35	279.38/279.38	2.54/2.54
10.31.1.105	destination	34.57/34.57	279.38/279.38	2.89/2.89
70.32.128.171	source	11.83/11.83	67.53/67.53	1.16/1.16
70.32.128.22	source	11.83/11.83	67.53/67.53	1.16/1.16
70.32.128.74	source	11.83/11.83	67.53/67.53	1.16/1.16
10.39.1.22	source	11.83/11.83	57.53/57.53	1.23/1.23
10.31.1.203	source	10.45/10.45	54.98/54.98	0.95/0.95
10.31.1.202	source	10.45/10.45	54.98/54.98	0.95/0.95

javascript:void(0);

Select Project

View Cyber | View Physical | View Paths



Use Case: Patching

Description	Select hosts or vulnerabilities to patch and re-compute attack path rankings.
Role	IT Administrator Manager
Inputs	• A model • A source of vulnerability information • A set of assets to be ranked
Outputs	A list of attack paths whose rankings have been updated based upon which assets were patched.

Mark devices patched then recalculate ranking

CyPSA Home | Model | Action | Panini

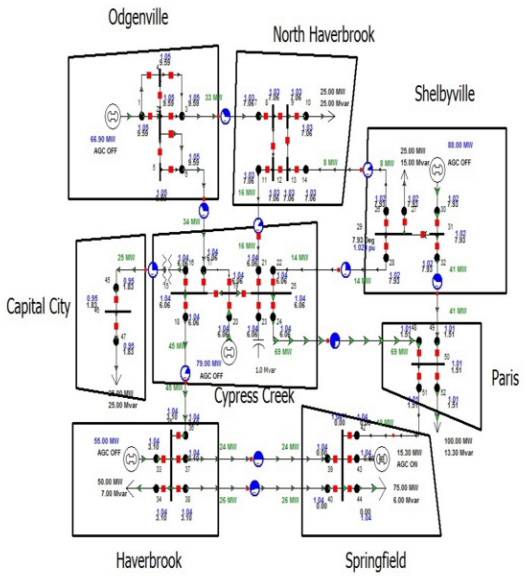
Ranked Assets

Show 10 entries Search:

IP Address	Type	Performance Index (Curr/Prev)	Cyber Cost (Curr/Prev)	Security Index (Curr/Prev)
10.31.1.101	destination	1.38/1.38	8.95/8.95	0.15/0.15
10.31.1.102	destination	2.23/2.23	8.95/8.95	0.25/0.25
10.31.1.103	destination	3.89/3.89	8.95/8.95	0.43/0.43
10.31.1.104	destination	1.38/1.38	8.95/8.95	0.15/0.15
10.31.1.105	destination	1.57/1.57	8.95/8.95	0.18/0.18
10.31.1.201	source	10.45/10.45	44.76/44.76	1.17/1.17

Showing 1 to 6 of 6 entries Previous 1 Next

View Cyber | View Physical | View Paths



Patched Hosts | Compromised Hosts | Vulnerabilities

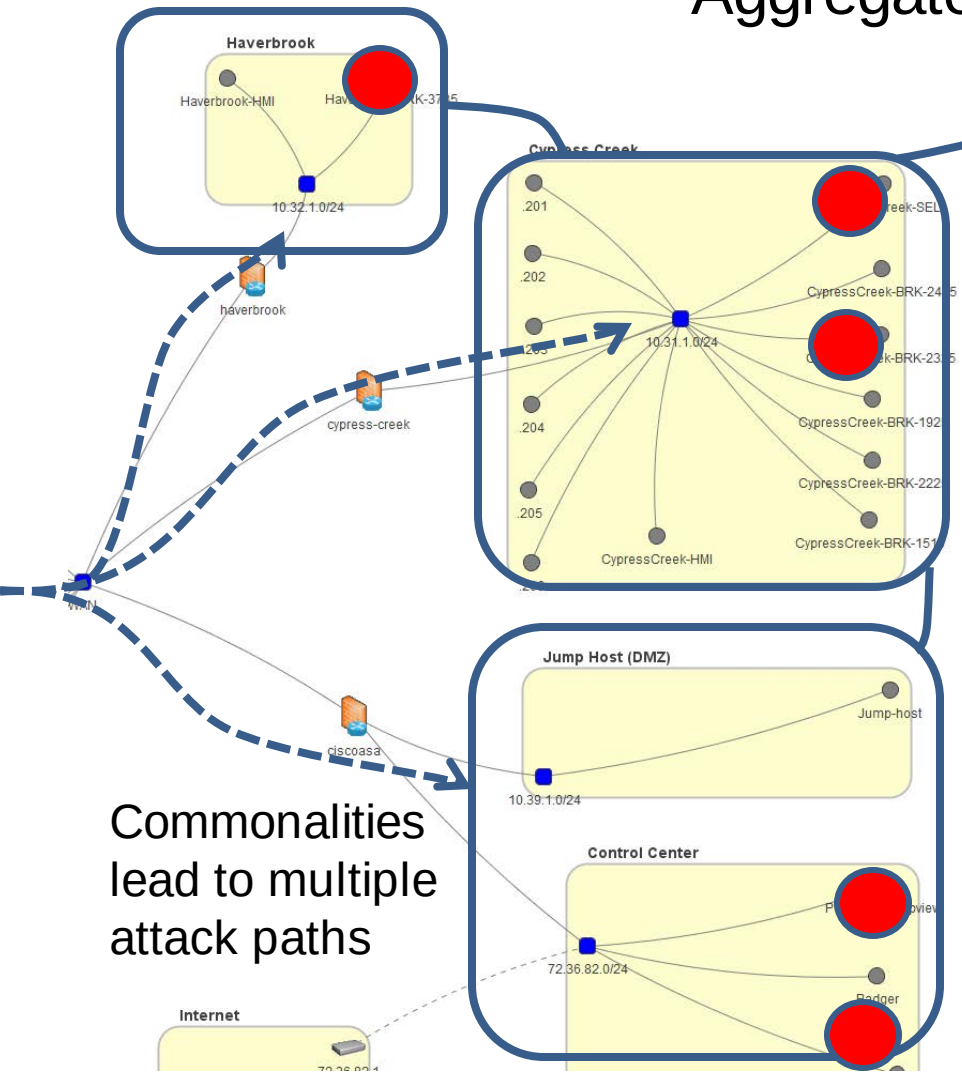
Select	IP Address	Vulnerabilities
☐	10.31.1.103	CVE-2015-4195
☐	10.31.1.102	CVE-2015-2907
☐	10.31.1.105	CVE-2015-2906
☐	10.31.1.104	CVE-2015-4195
☐	10.31.1.101	CVE-2015-4195

Patch Selected Hosts

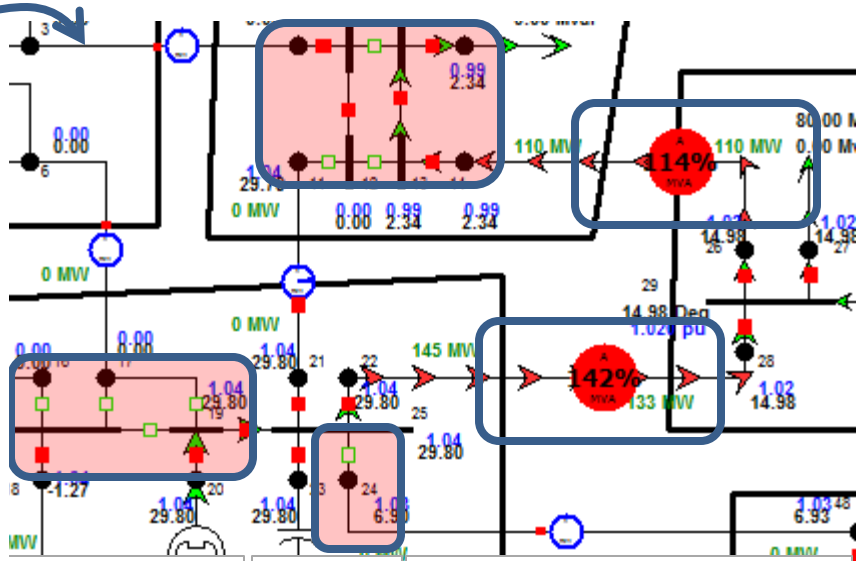
Use Case: Aggregate Exposure

Description	Analyze all attack paths for a given grouping of assets, e.g. all paths through assets of a given type or with a given vulnerability that lead to another asset of a given type (i.e., breakers). Rank based on both *impact* and *cyber exposure*
Role	**Manager**
Inputs	• A model • A source of vulnerability information • A set of assets to be ranked
Outputs	• A list of attack paths annotated with and ordered by a ranking

Aggregate Exposure



Commonalities lead to multiple attack paths



Vulnerability ID	Frequency	Select Hosts
CVE-2013-4581 -	60	Select All Cypress Creek-BRK-2425 - 10 Cypress Creek-BRK-1519 - 10 Haverbrook-BRK-3735 - 10 Cypress Creek-BRK-2325 - 10
CVE-2015-0667 -	13	Select All Cypress Creek-BRK-2425 - 12 Cypress Creek-BRK-2225 - 1

Use Case: Cyber Incident Planning

Description	Devices are marked as compromised and asset rankings are re-computed.
Role	**IT Administrator** **Manager** **Power Engineer**
Inputs	• A model • A source of vulnerability information • A set of assets to be ranked
Outputs	A list of assets whose rankings have been updated based upon which assets were compromised.

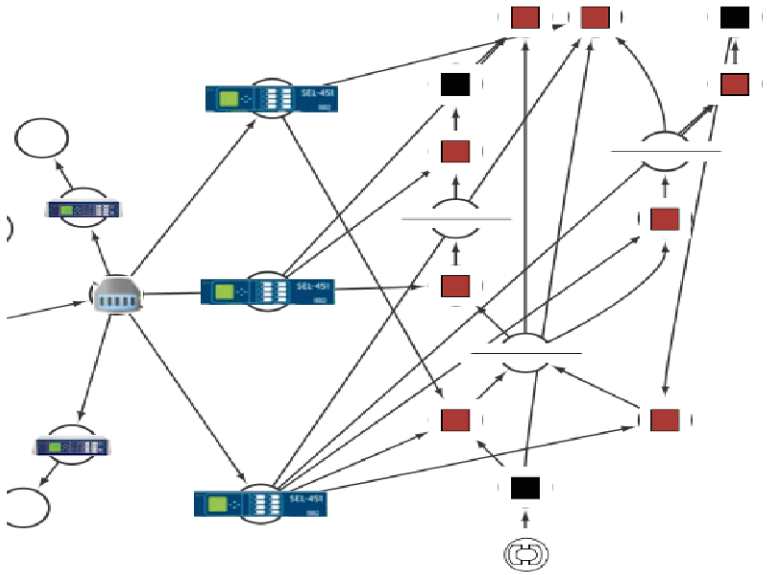
Annotation, Vulnerability Information: Manager

Annotate Model

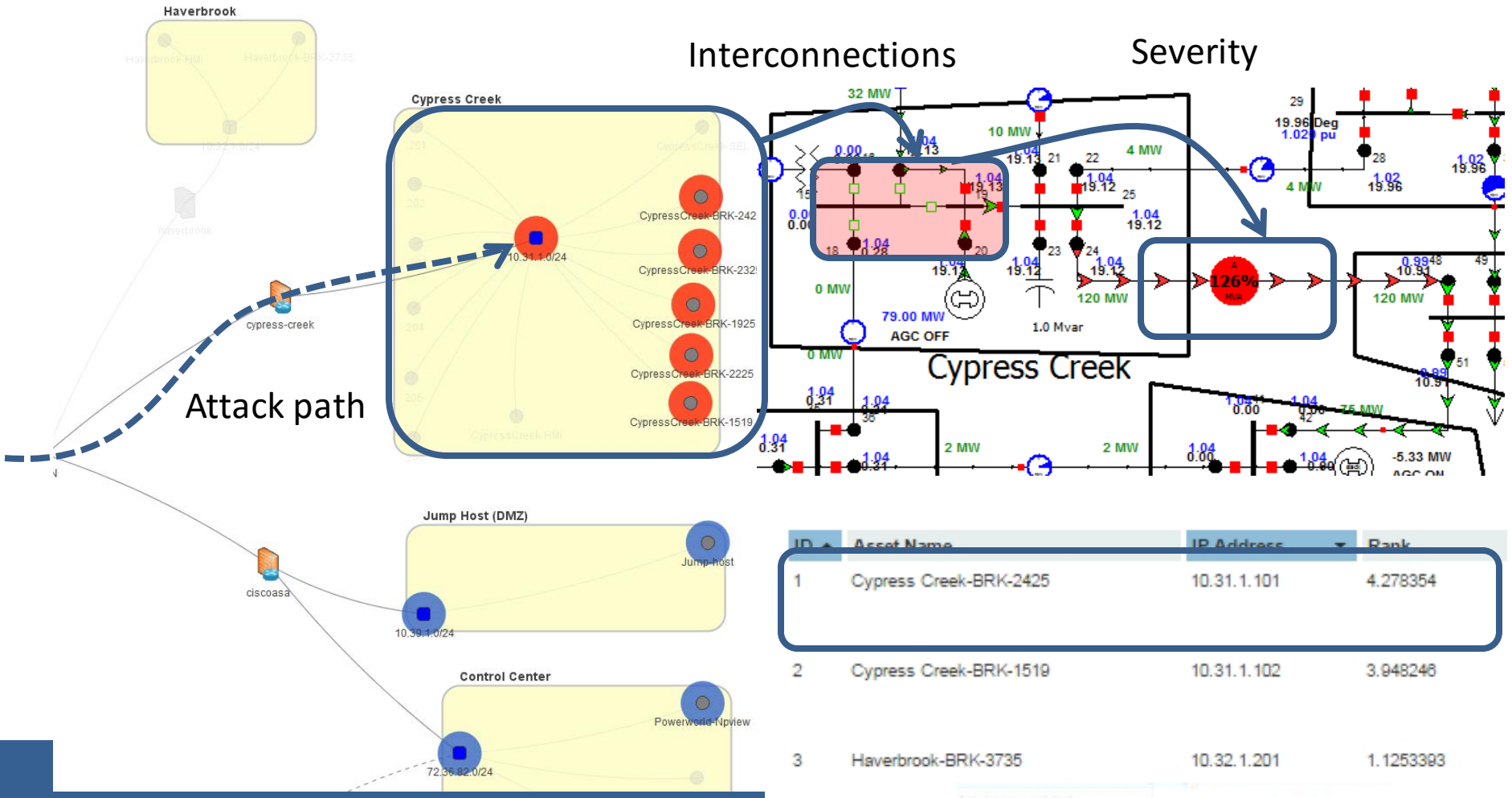
Name	OS	CVE Vulns	Freq
SEL 3620 1			
SEL 421 1			
SEL 421 2			
...			
SEL 451 1			
...			

Load annotations data
on CVE Vulns
from URL or Path to Annotation
Join on OS
GO

Cypress Creek, Substation Network



Beyond ‘N-1’
transient stability analysis using a cyber incident



ID	Asset Name	IP Address	Rank
1	Cypress Creek-BRK-2425	10.31.1.101	4.278354
2	Cypress Creek-BRK-1519	10.31.1.102	3.948246
3	Haverbrook-BRK-3735	10.32.1.201	1.1253393

DEMO

- Start-up partnering with Powerworld and SEL
- Provides support and installation for CyPSA
- Commercial client kaedago for relay cyber/physical tie information

Take Action

Kate Davis
krogers6@illinois.edu
kate@kaedago.com
Edmond Rogers
ejrogers@Illinois.edu
edmond@kaedago.com

1. Learn more
2. Provide feedback
3. Try it