CyPSA: Cyber-Physical Security Assessment

Project Information

- Team members
  - *UIUC*: David Nicol, Pete Sauer, Kate Davis, Edmond Rogers, Robin Berthier, Olivier Soubigou, Gabe Weaver.
  - *OSU*: Panini Patapanchala, Vishnu Rayala, Rakesh Bobba
  - *Rutgers*: Luis Garcia, Saman Zonouz
  - *PowerWorld*: Matt Davis
- Sponsor: ARPA-E
- Duration: April 2013 – Aug 2016
- Commercialization: Kaedago Inc.

- Based on two papers under TCIPG
  - Zonouz, S., Davis, C. M., Davis, K. R., Berthier, R., Bobba, R. B., & Sanders, W. H. (2014). **SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures**. IEEE Transactions on Smart Grid, 5(1), 3-13.

    Science of Security Significant Research in Cyber Security Citation
  - Zonouz, S., Rogers, K. M., Berthier, R., Bobba, R. B., Sanders, W. H., & Overbye, T. J. (2012). **SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures**. IEEE Transactions on Smart Grid, 3(4), 1790-1799.

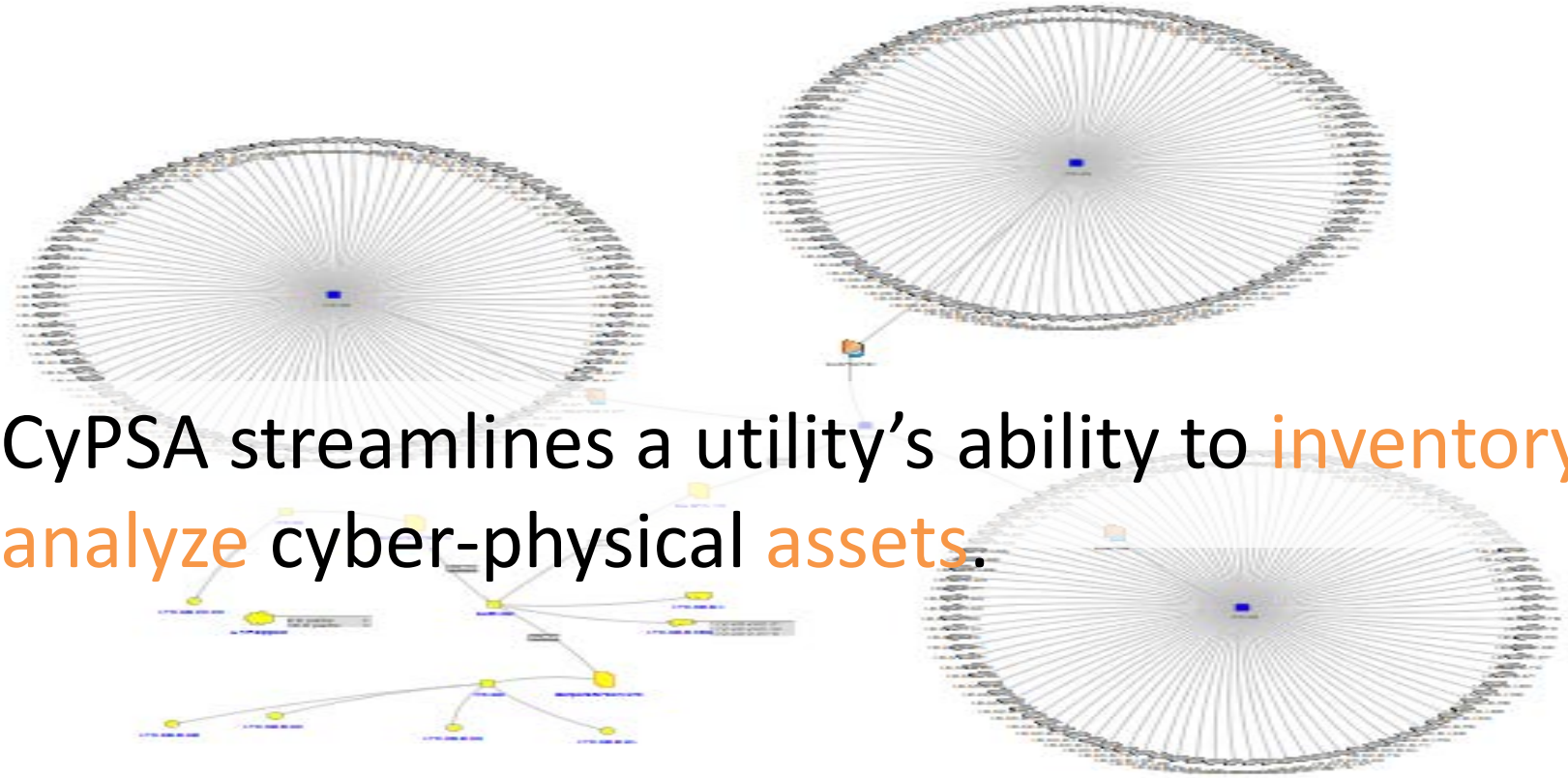
CyPSA Motivation

- Power system operators and planners are constantly studying the system to gauge the effect of outages and changes on the system. Presently, ***outages caused by cyber failures or attacks are not considered***

- The purpose of this work is to build a framework that includes the physical and cyber systems so that the impact of cyber outages on the power system can be taken into account

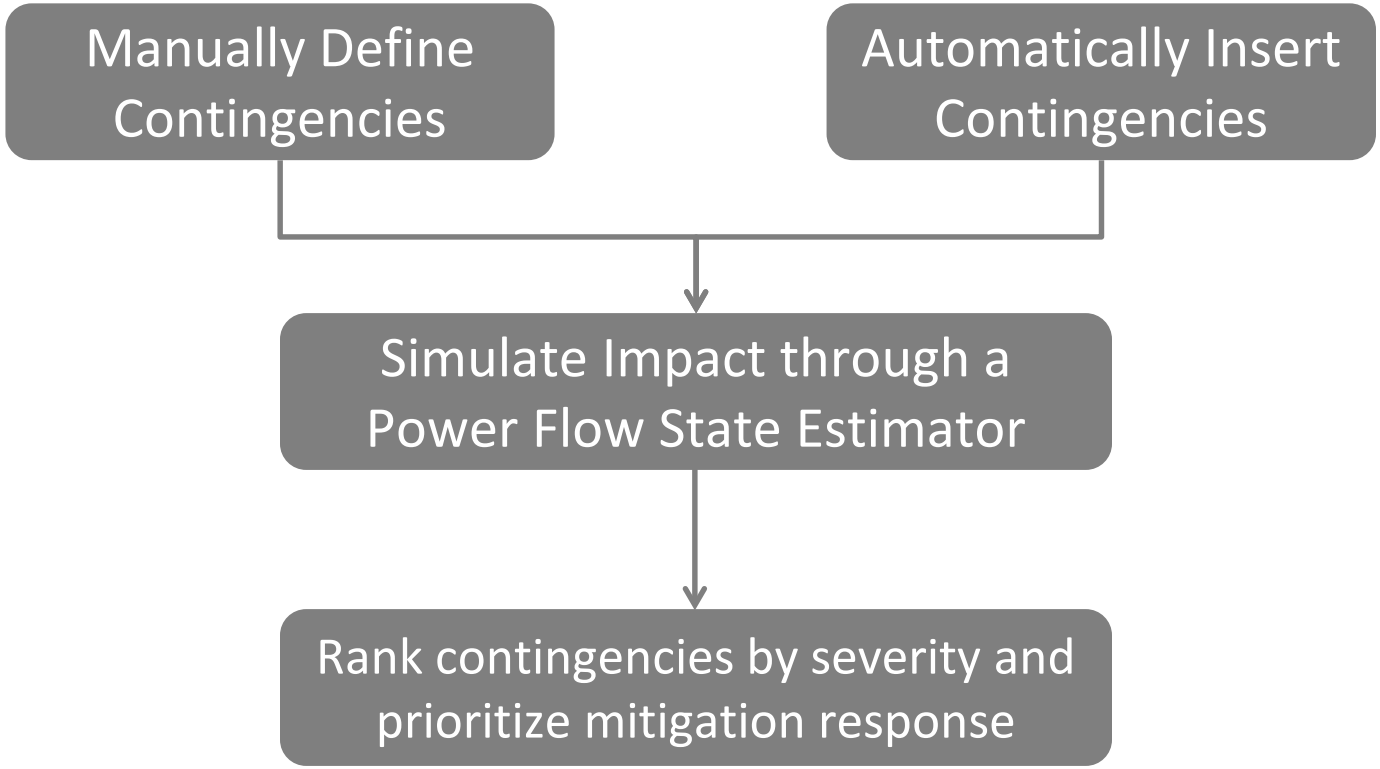
Challenges

- How to ensure operational reliability given our increasing dependence on cyber systems?
- How to understand the impact of cyber vulnerabilities on grid operations?
- How to prioritize cyber security efforts in control networks and substations?

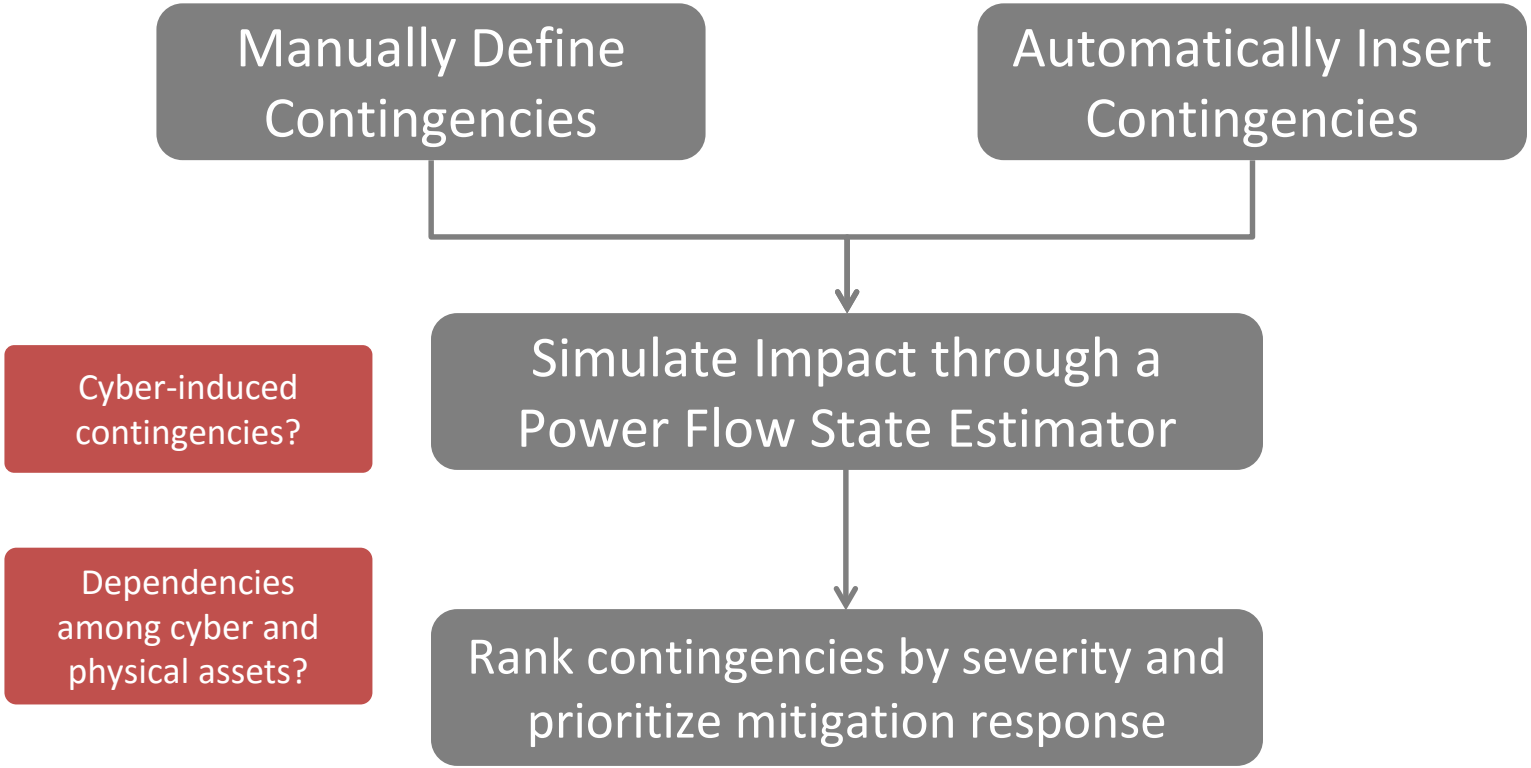


CyPSA streamlines a utility's ability to inventory and analyze cyber-physical assets.

Target Application: Contingency Analysis



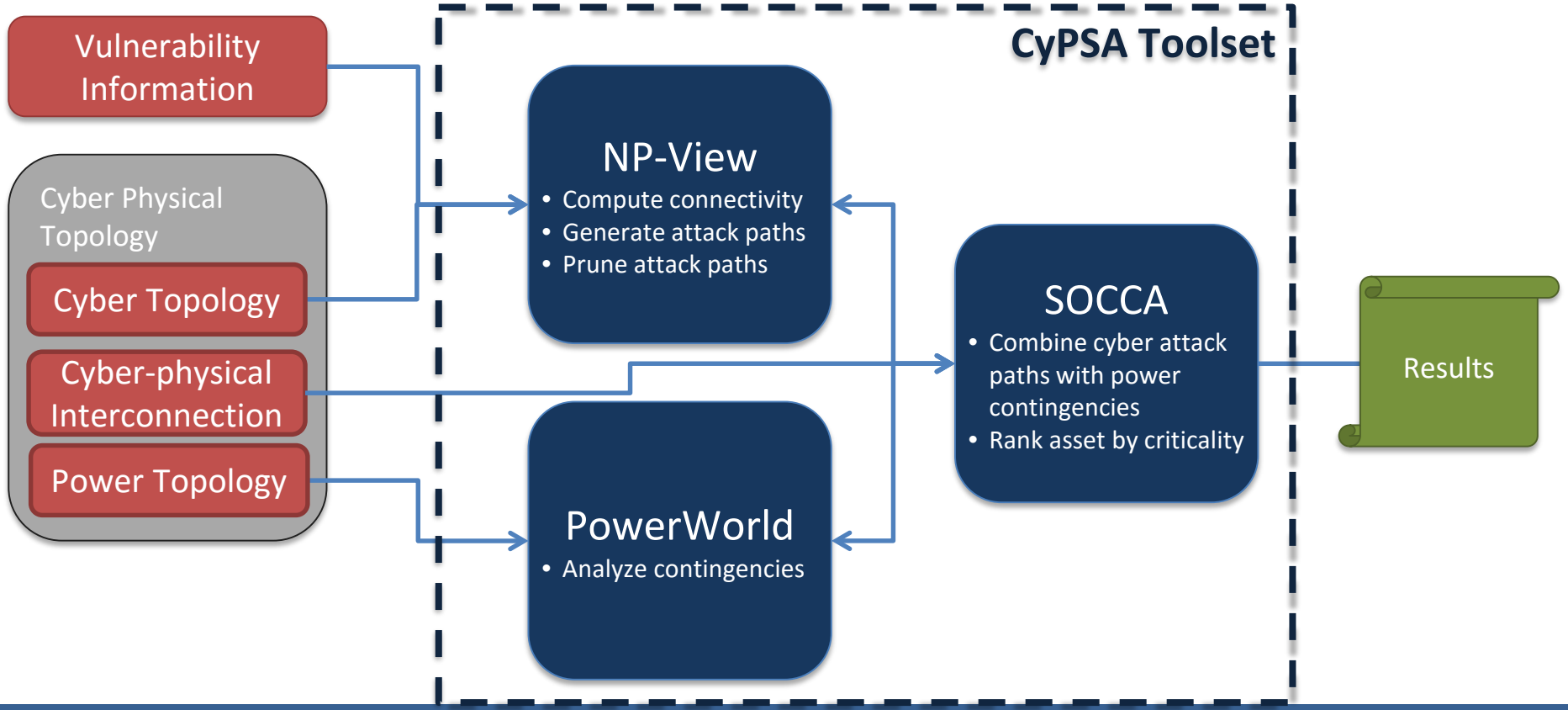
Target Application: Contingency Analysis



Approach

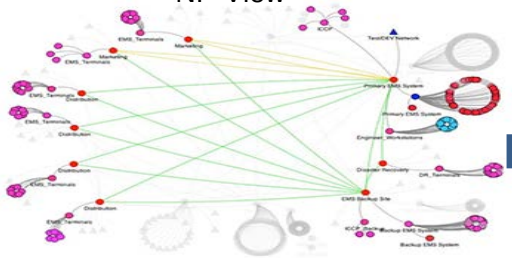
- Combining cyber and power topologies to create a realistic model of the infrastructure
  - cyber network topology + firewall rule-based attack graph generation
  - power system topology and power flow models
- Dividing the problem into manageable pieces
  - cyber-side attack graph analysis (ease of penetration)
  - physical line outages/contingencies (impact of penetration)
- Developing algorithms to compute potential attack paths and to assess risks accurately

CyPSA: Basic Pipeline



CyPSA Basic Pipeline Overview

NP-View

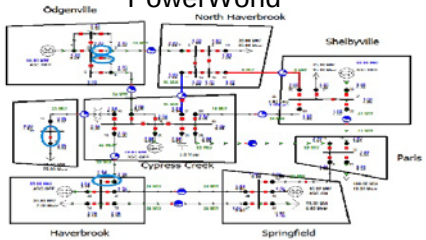


1

SOCCA on Zabbix

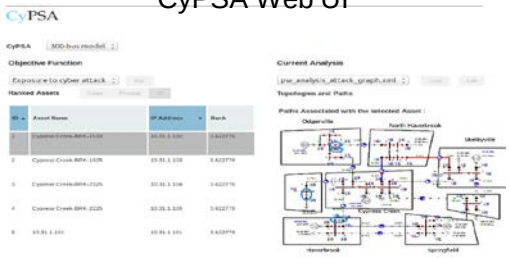
2

PowerWorld



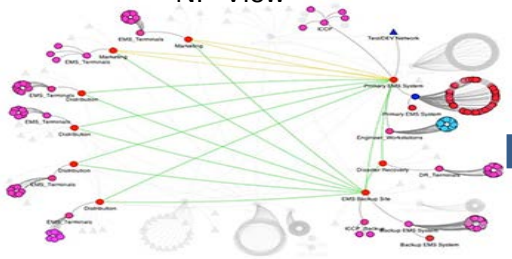
3

CyPSA Web UI



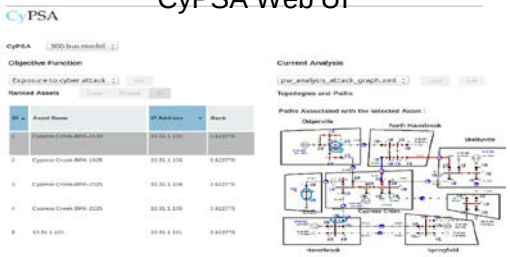
CyPSA Overview

NP-View



SOCCA on Zabbix

CyPSA Web UI

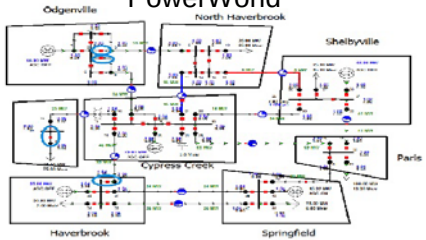


1

2

3

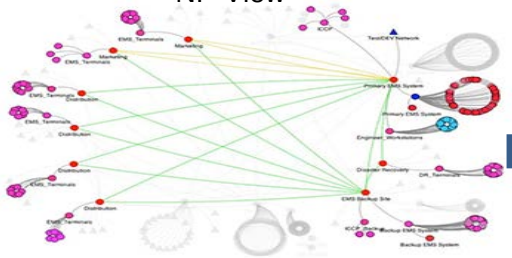
PowerWorld



1. NP-View analyzes cyber-network and provides cyber vulnerability analysis attack paths XML file to SOCCA

CyPSA Overview

NP-View

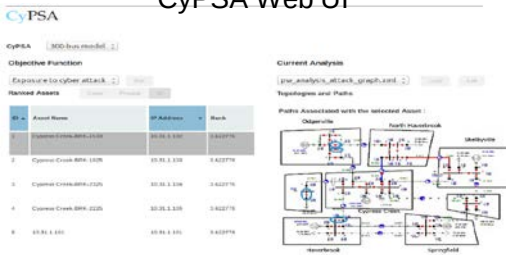


1

SOCCA on Zabbix

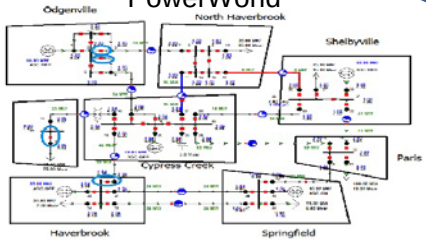
3

CyPSA Web UI



2

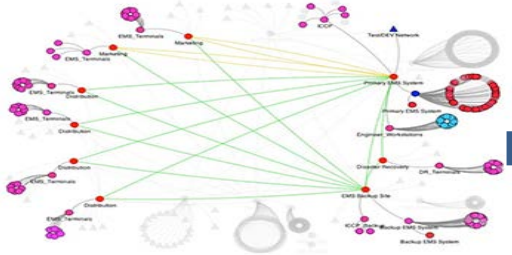
PowerWorld



2. SOCCA uses PowerWorld to calculate performance indices for all critical assets and then generates a cyber-physical attack path list ranked by security index

CyPSA Overview

NP-View

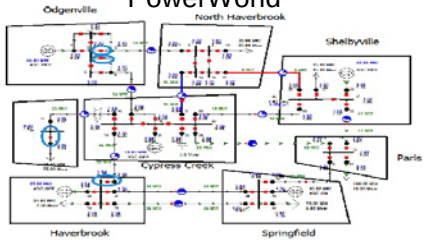


1

SOCCA on Zabbix

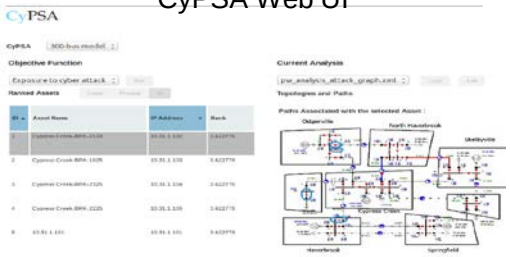
2

PowerWorld



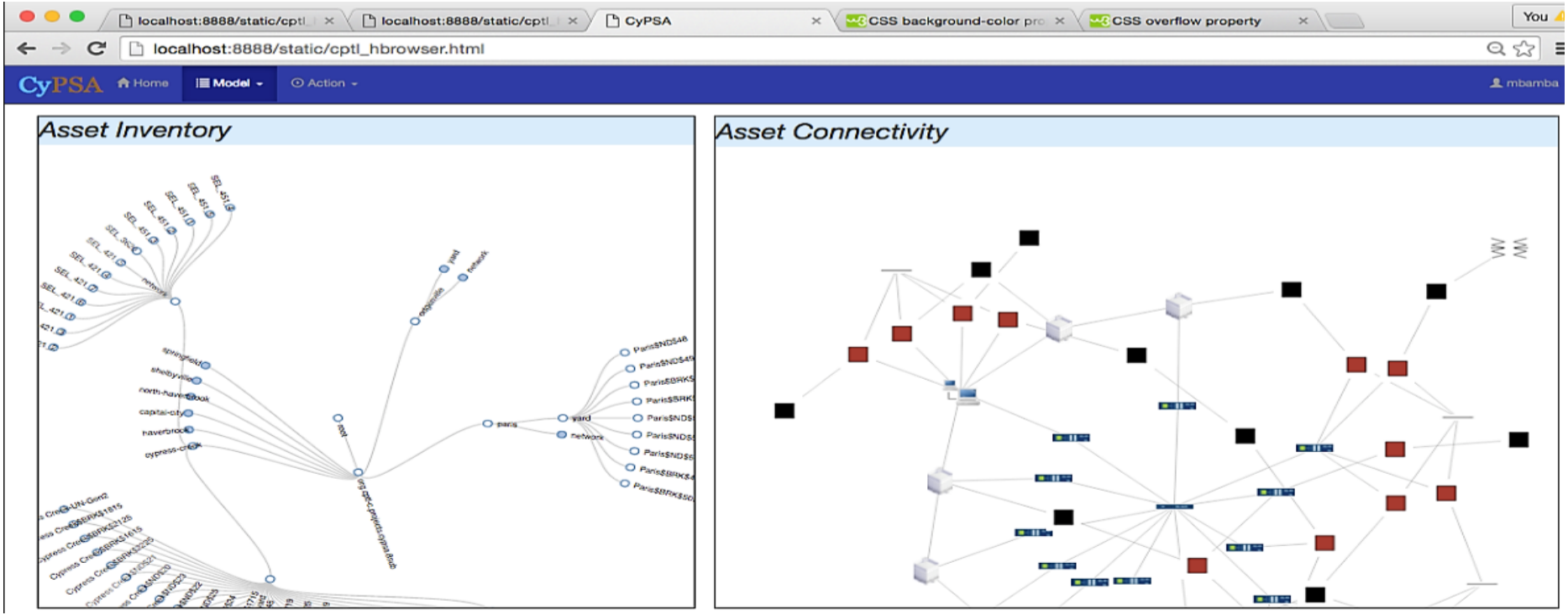
3

CyPSA Web UI



3. SOCCA sends the new cyber-physical attack graph to be displayed by the Web UI

CyPSA Data Interactions

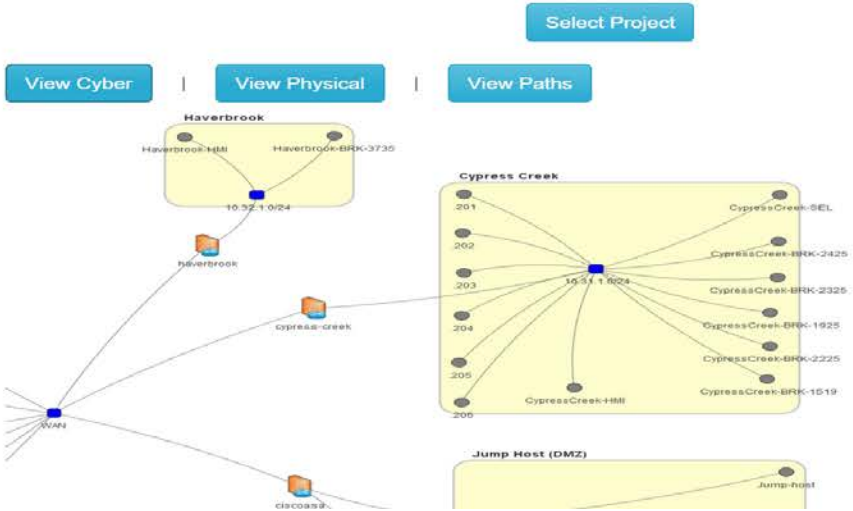


CyPSA Control Panel

CyPSA Home Model Action Panini

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



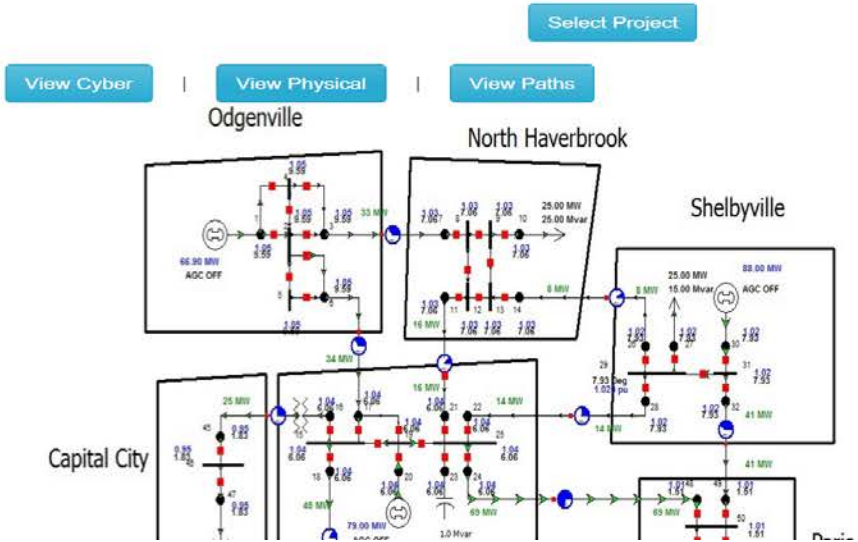
CyPSA Control Panel

CyPSA Home Model Action Panir

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);



Key Advantages

- Accurate **model** of connections and dependencies of **cyber** and **physical** systems
- ***What-if* scenario analysis** and **prioritization** of system-hardening and security patching efforts
- Address the challenge of **including cyber failures**/attacks in **contingency analysis**

Benefits and Use Cases

- For **utility operators** and **utility planners**:
  - Gain situational awareness on cyber systems
- For **security analysts**:
  - Save time and effort in prioritizing security protection deployment
- For **auditors**:
  - Improve understanding of the required scope of compliance efforts