CyPSA

(Cyber Physical Situational Awareness)

A rejected Blackhat talk.

kaedago

CyPSA Project

Aug 3, 2016

ILLINOIS

Oregon State UNIVERSITY

RUTGERS UNIVERSITY

U.S. DEPARTMENT OF ENERGY arpa·e

PowerWorld Corporation

Pacific Northwest NATIONAL LABORATORY

SEL SCHWEITZER ENGINEERING LABORATORIES

np network perception

Project Team

ILLINOIS

Kate Davis

Robin Berthier

David Nicol

Edmond Rogers

Pete Sauer

Gabe Weaver

Mouna Bamba

Olivier Soubigou

Oregon State UNIVERSITY

Rakesh Bobba

Panini Patapanchala

Vishnu Priya Rayala

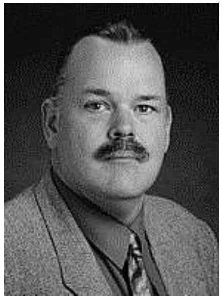
RUTGERS UNIVERSITY

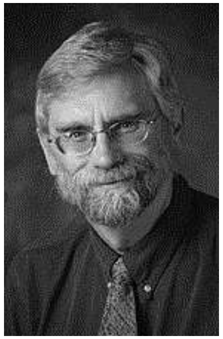
Saman Zonouz

Luis Garcia

PowerWorld Corporation

Matt Davis





ARPA-E: Tim Heidel, Sameh Elsharkawy, Erik Derosiers

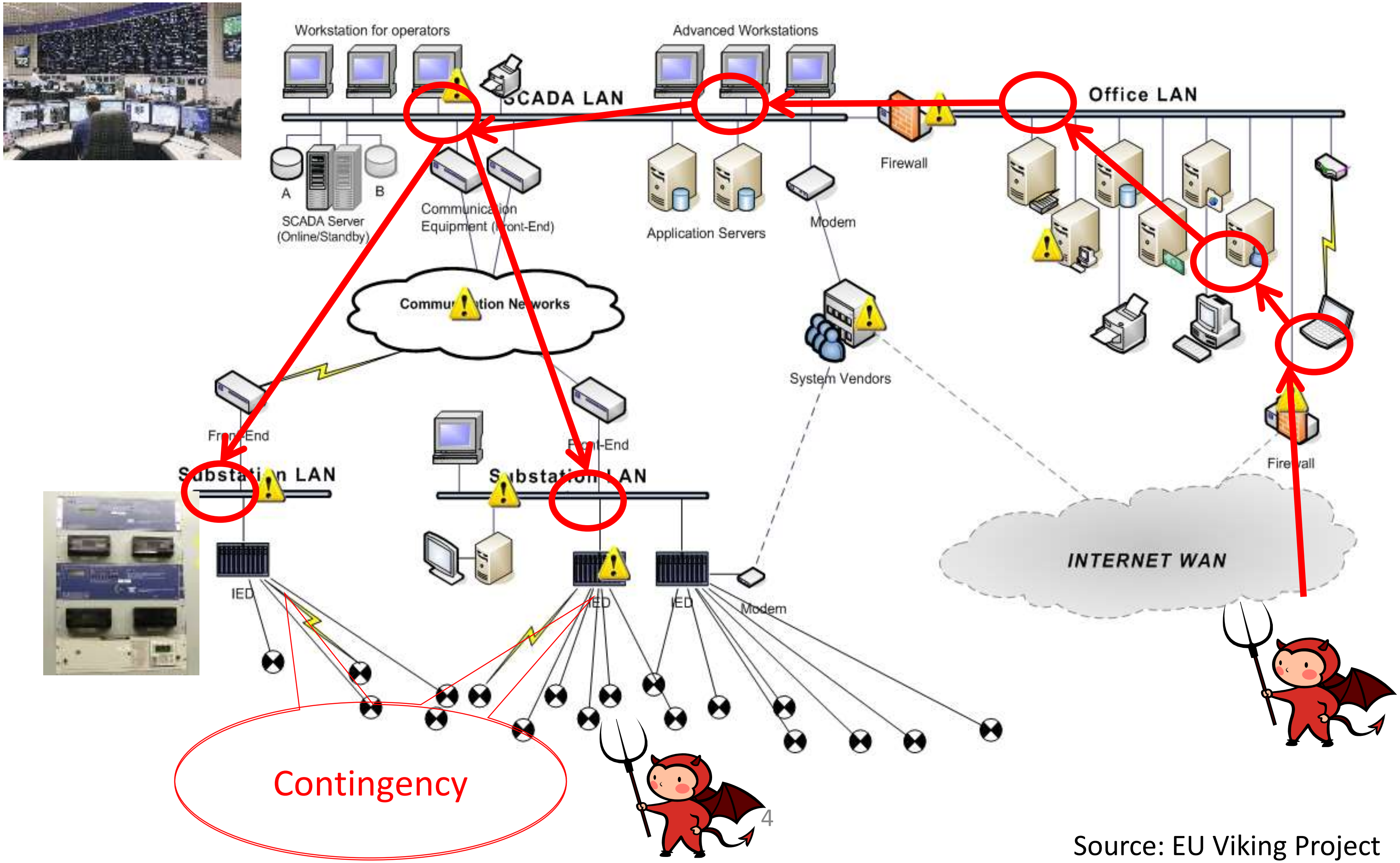
Challenges

- How to ensure operational reliability given our increasing dependence on cyber systems?

- How to understand the impact of cyber vulnerabilities on grid operations?

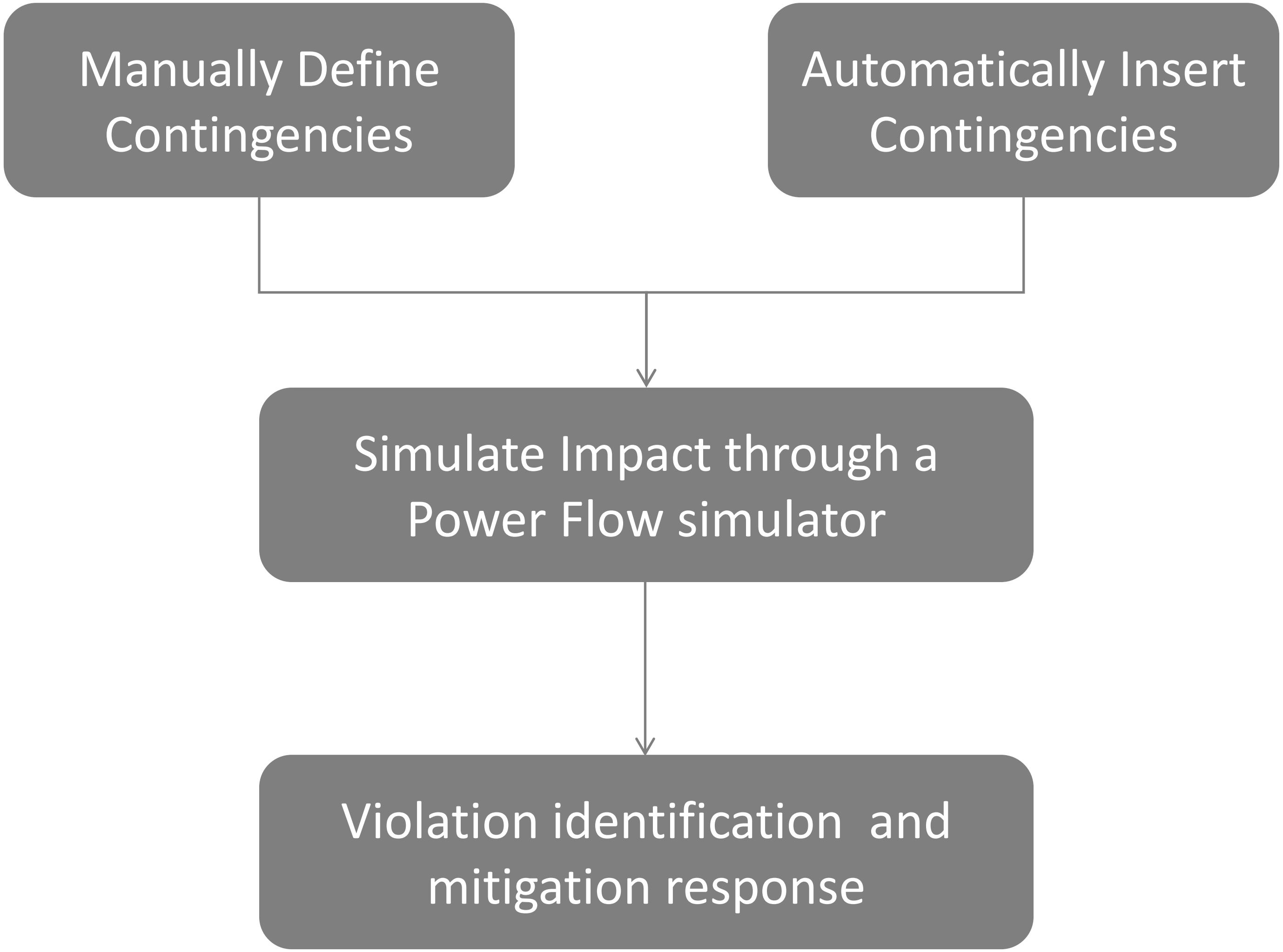
- How to prioritize cyber security efforts in control networks and substations?

What is the Problem?



Source: EU Viking Project

Traditional Contingency Analysis



Manually Define Contingencies

Automatically Insert Contingencies

Simulate Impact through a Power Flow simulator

Violation identification and mitigation response

Traditional Contingency Analysis

- Meant to be prepared for one outage (“N - 1” criteria)
  - no violations when any one element (line, generator or major transformer) goes out of service
  - “N - 1” criteria is reliability standard

- Is preparedness for one outage enough?
  - probability of multiple independent failures is considered small enough to accept the risk

- Cyber-assets are not considered
  - redundant provisioning
  - probability of multiple independent failures is considered small enough to accept the risk

Limitations with Current Practice

- With threat of cyber-attacks
  - multiple failures no longer unlikely
  - redundant provisioning alone not sufficient

- Prevention/protection mechanisms are not foolproof

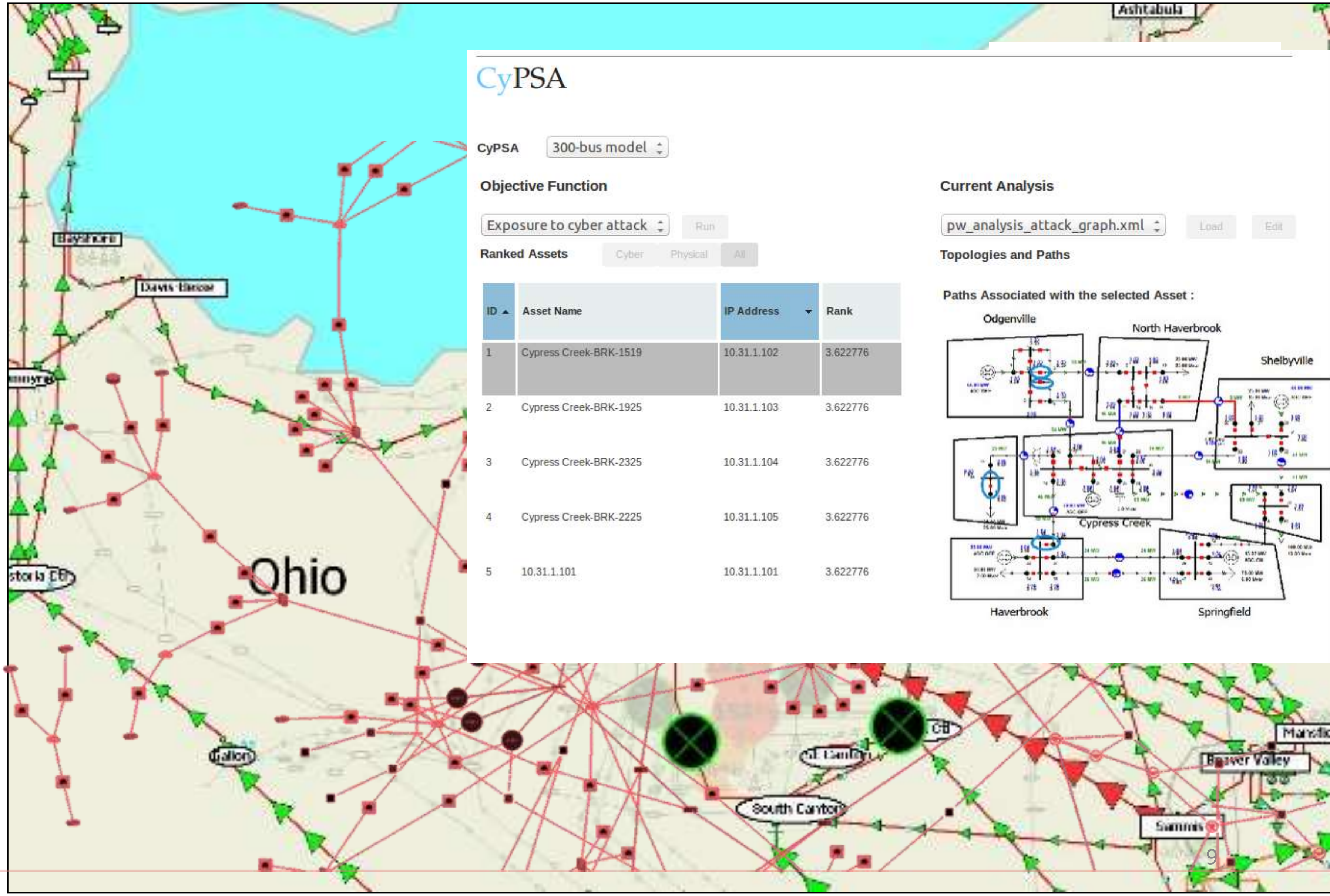
- Power system needs to be reliable even in the face of cyber-attacks
  - Need to deal with multiple outages ("N – x")
  - Need to deal with failures of "cyber assets"

Challenges of multiple outages

- Size of the contingency list can grow very large*
    - For 1000 line system
        - N-1 means solving 1000 line outages
        - N-2 means solving 499500 line outages (1000 choose 2)!
        - WECC N-2 for transmission lines ~135M contingencies
            - ~15 days with super computer!

- Operating at “N – x” reliability criterion can be expensive
    - limits flow capacity

*Charles Davis, Thomas Overbye: Linear Analysis of Multiple Outage Interaction. HICSS 2009: 1-8



CyPSA

CyPSA: 300-bus model

Objective Function

Exposure to cyber attack — Run

Ranked Assets — Cyber | Physical | All

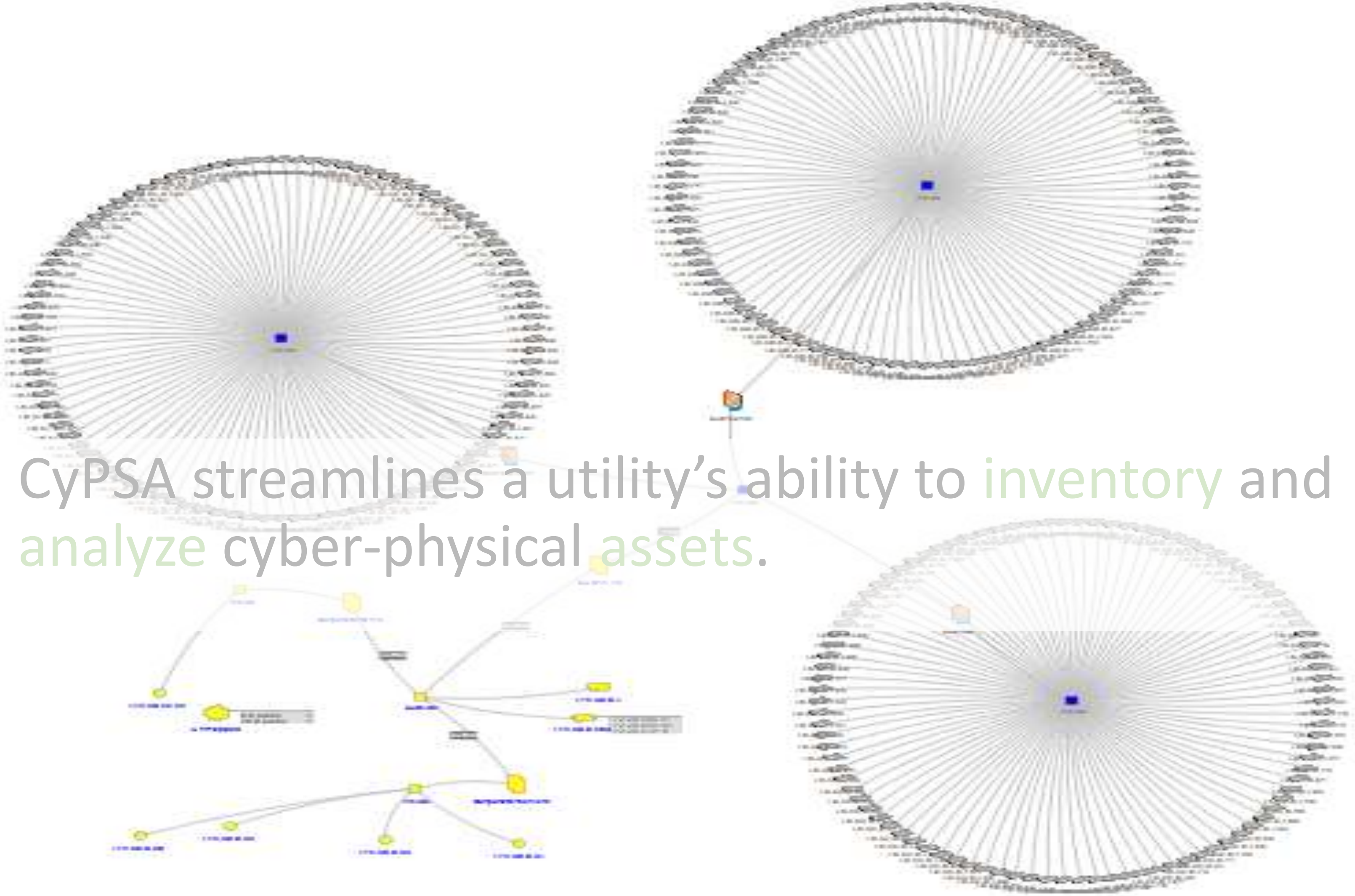
ID ▲	Asset Name	IP Address ▼	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776
5	10.31.1.101	10.31.1.101	3.622776

Current Analysis

pw_analysis_attack_graph.xml — Load — Edit

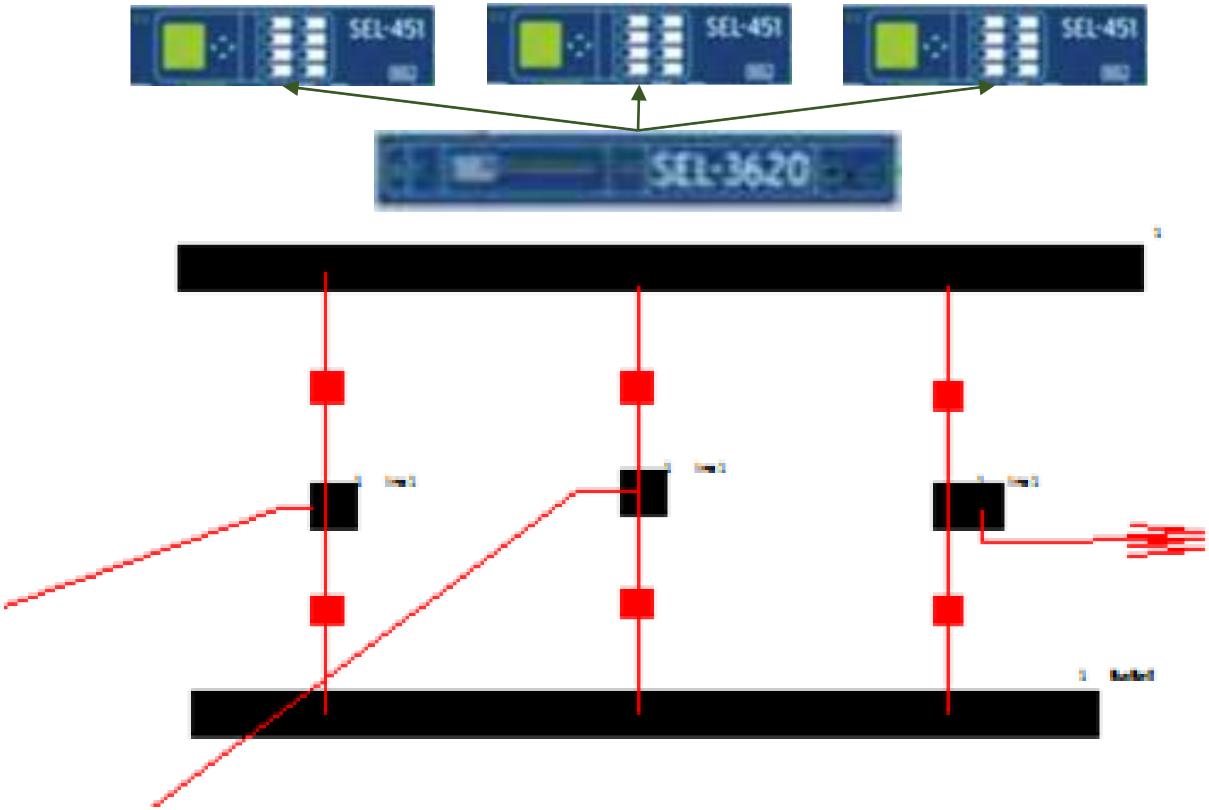
Topologies and Paths

Paths Associated with the selected Asset :



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

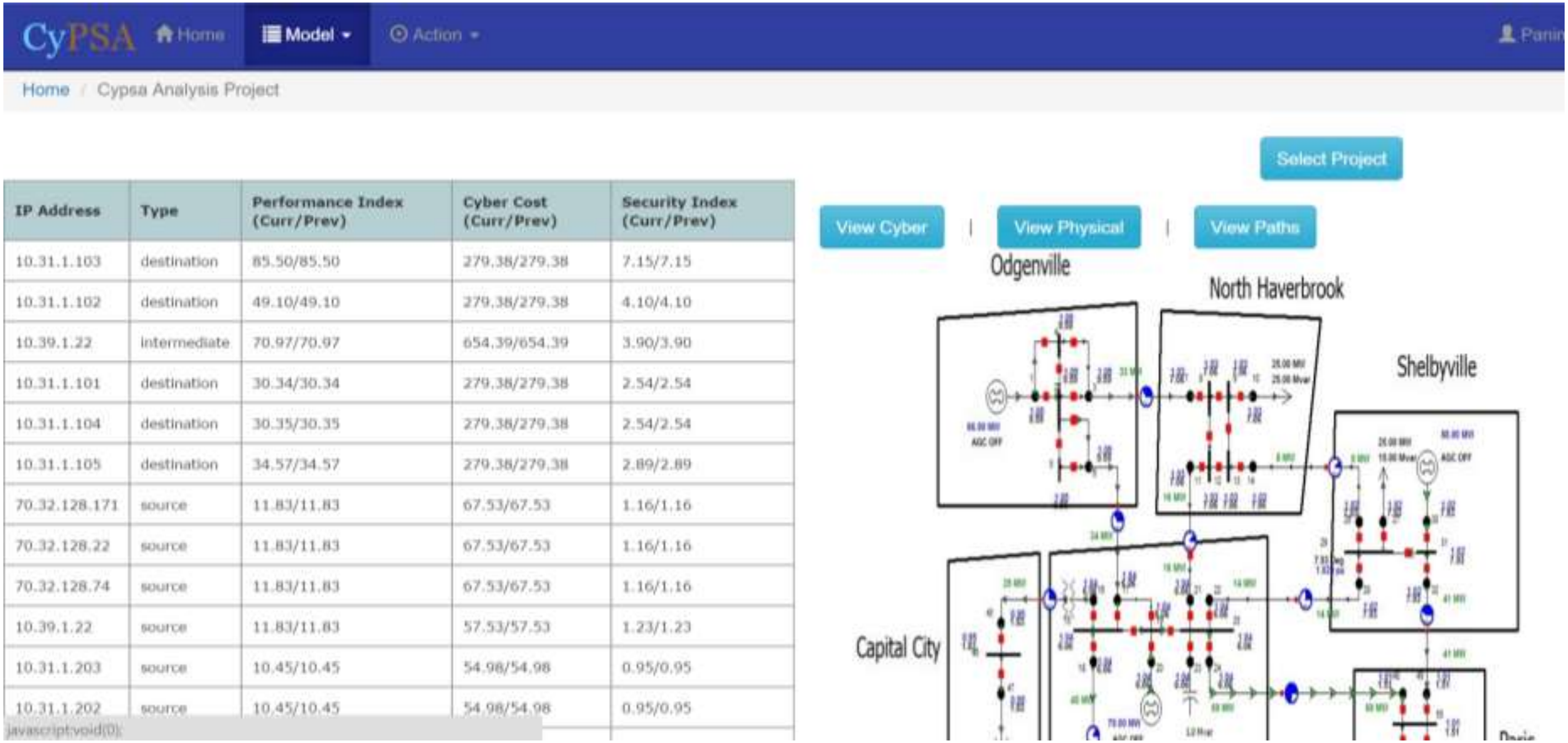
Collect and manage inventory data



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 at 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

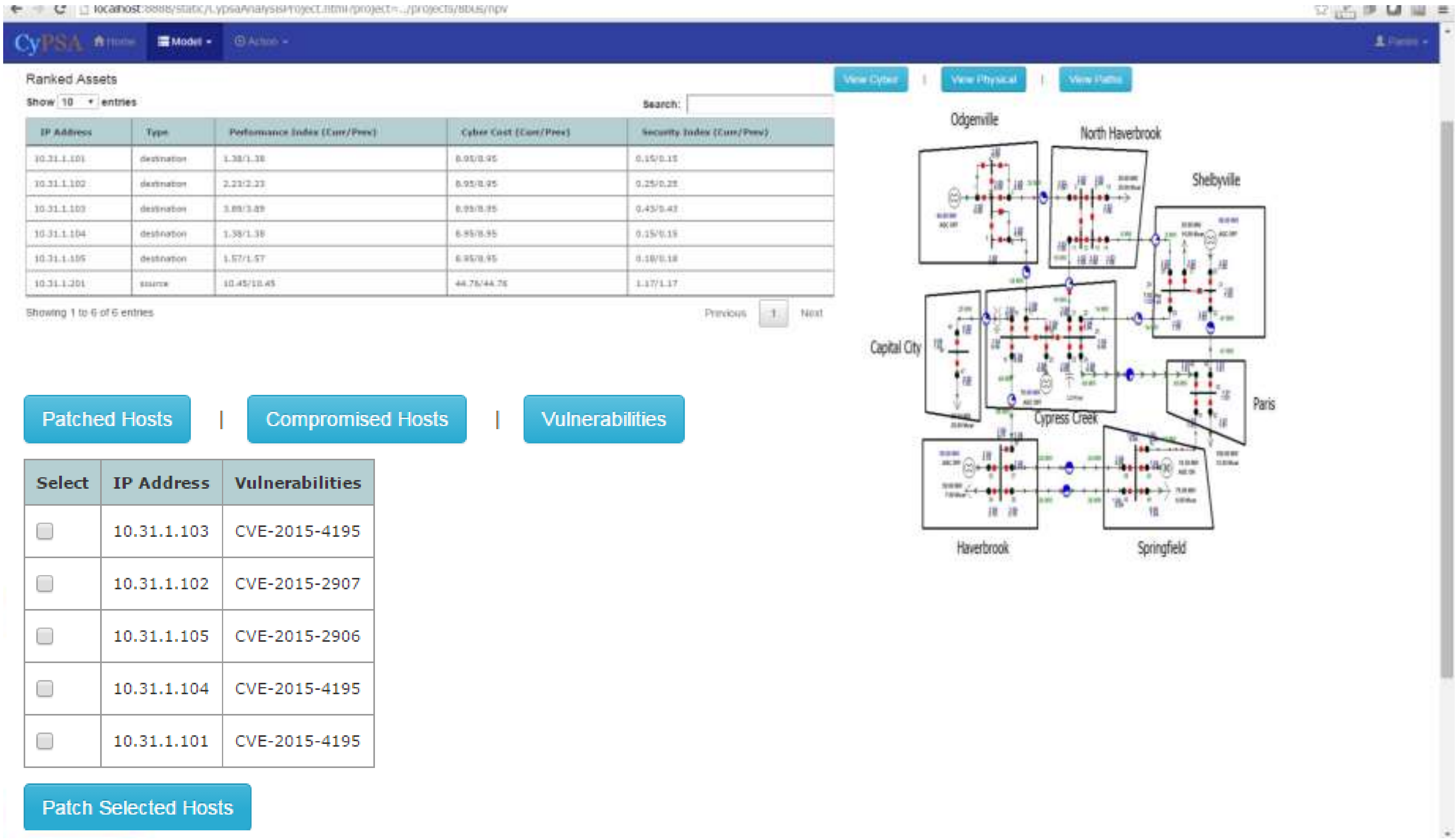


IP Address	Type	Performance Index (Curr/Prev)	Cyber Cost (Curr/Prev)	Security Index (Curr/Prev)
10.31.1.103	destination	85.50/85.50	279.38/279.38	7.15/7.15
10.31.1.102	destination	49.10/49.10	279.38/279.38	4.10/4.10
10.39.1.22	intermediate	70.97/70.97	654.39/654.39	3.90/3.90
10.31.1.101	destination	30.34/30.34	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

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



Ranked Assets

Show 10 entries

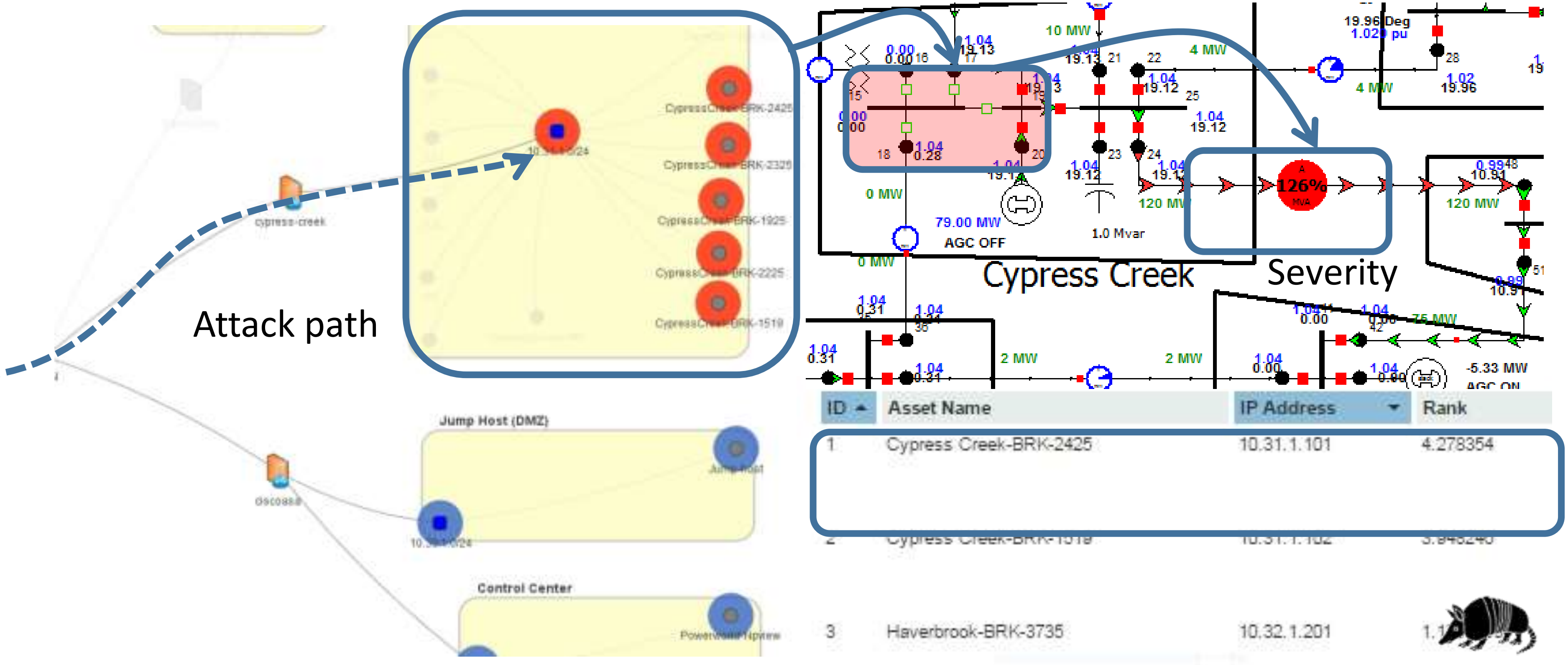
Search:

IP Address	Type	Performance Index (Curr/Prev)	Cyber Cost (Curr/Prev)	Security Index (Curr/Prev)
10.31.1.101	destination	1.38/1.38	0.95/0.95	0.15/0.15
10.31.1.102	destination	2.23/2.23	0.95/0.95	0.25/0.25
10.31.1.103	destination	3.89/3.89	0.95/0.95	0.43/0.43
10.31.1.104	destination	1.38/1.38	0.95/0.95	0.15/0.15
10.31.1.105	destination	1.57/1.57	0.95/0.95	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

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

Rank assets and paths based on physical topology, impact, cyber connectivity, and vulnerabilities



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	3.948240
3	Haverbrook-BRK-3735	10.32.1.201	1.1

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

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**

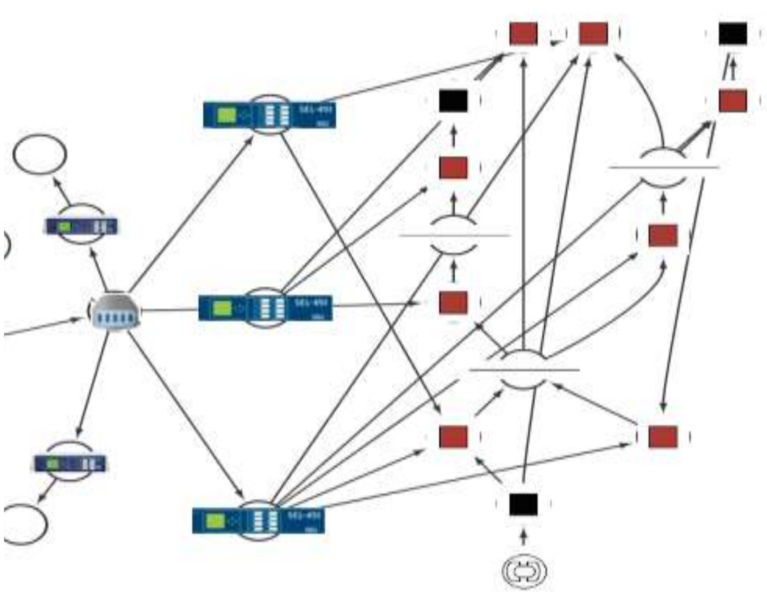
from **URL or Path to Annotation**

Join on **OS**

GO

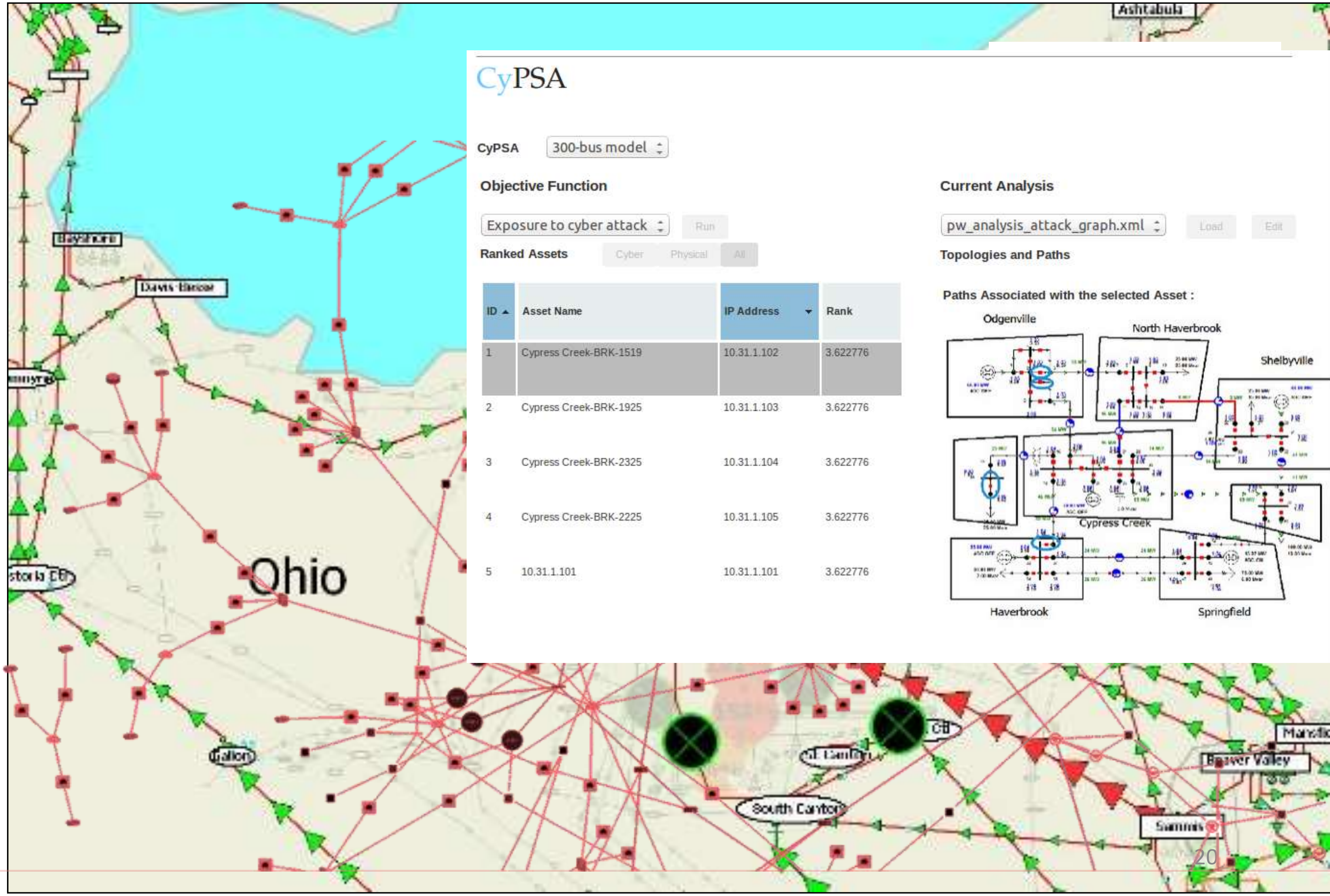
ⓘ ⓧ

Cypress Creek, Substation Network



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.



CyPSA

CyPSA: 300-bus model

Objective Function

Exposure to cyber attack — Run

Ranked Assets — Cyber | Physical | All

ID	Asset Name	IP Address	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776
5	10.31.1.101	10.31.1.101	3.622776

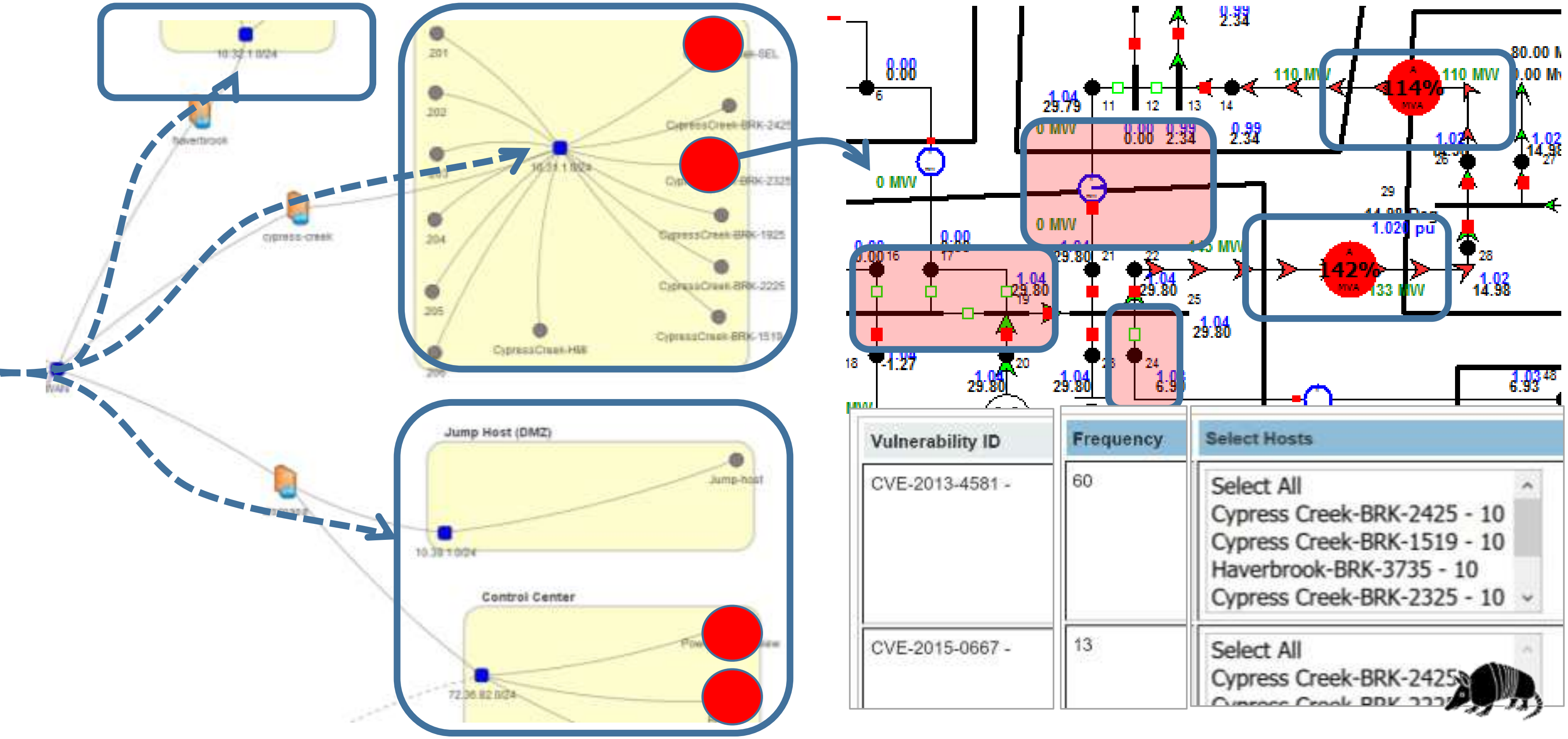
Current Analysis

pw_analysis_attack_graph.xml — Load | Edit

Topologies and Paths

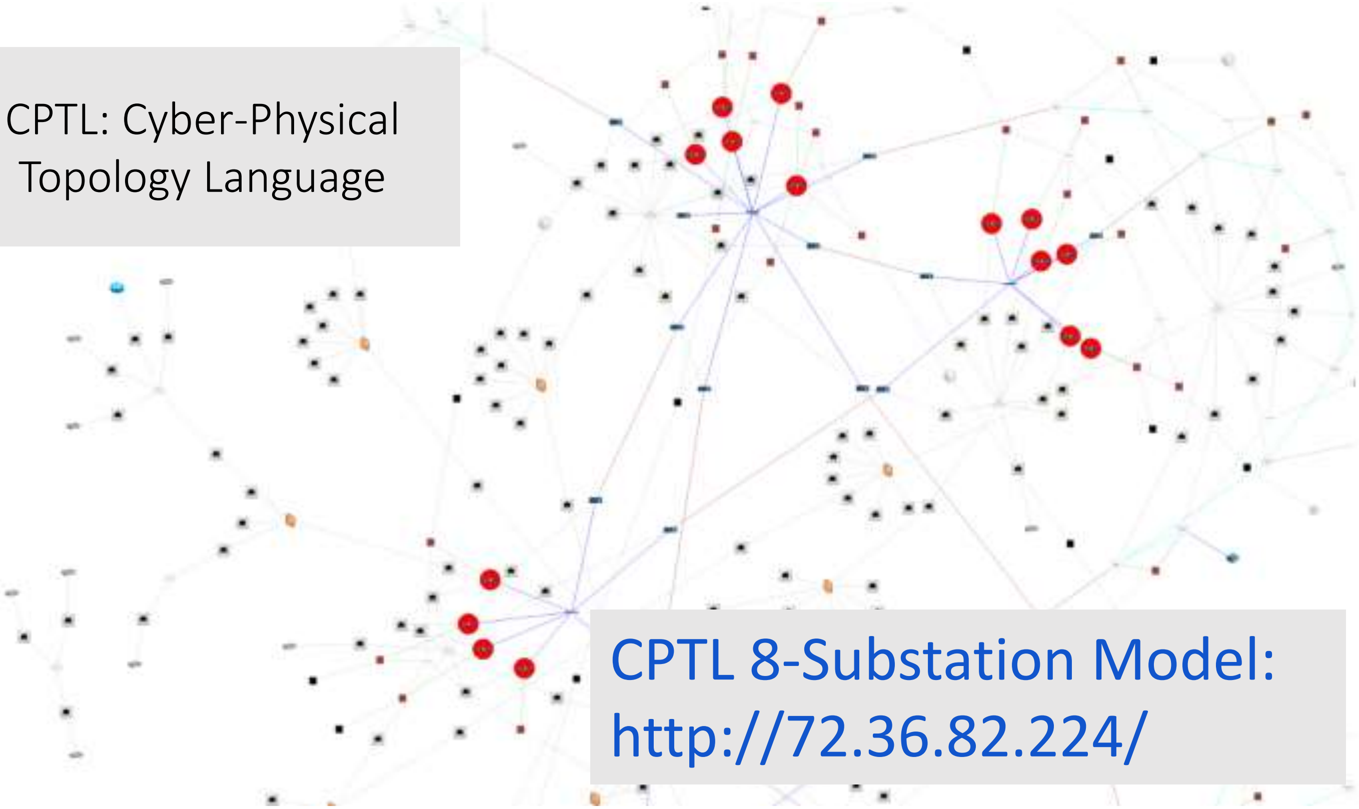
Paths Associated with the selected Asset :

Aggregate information and plan actions



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

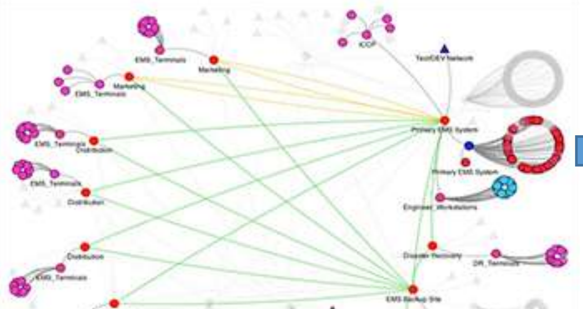
Analyze cyber-physical dependencies

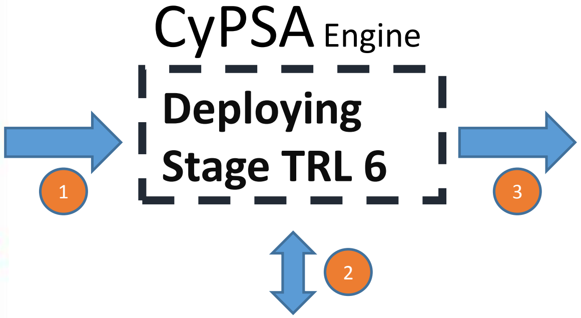


CPTL: Cyber-Physical Topology Language

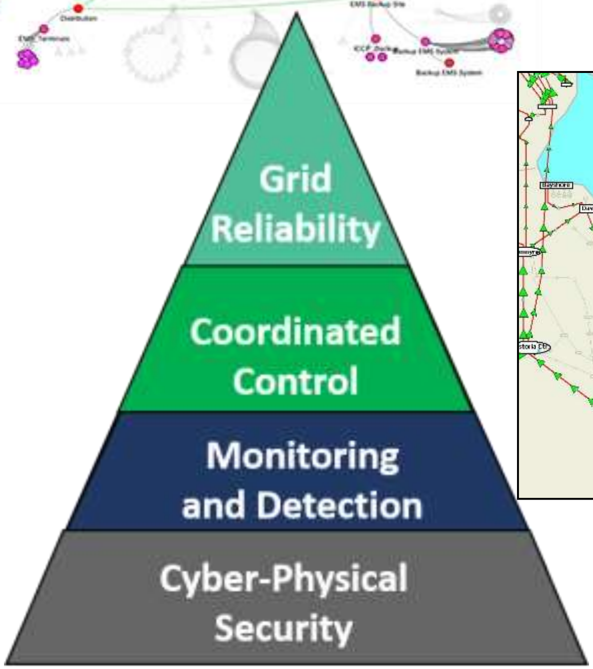
CPTL 8-Substation Model: http://72.36.82.224/

Cyber-Physical Security Assessment (CyPSA)




CyPSA Engine

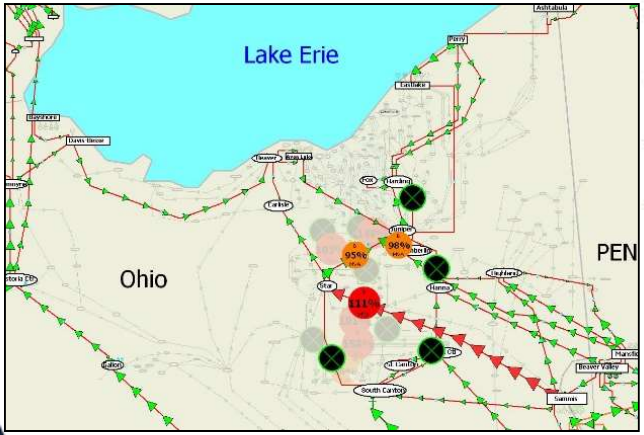
Deploying
Stage TRL 6

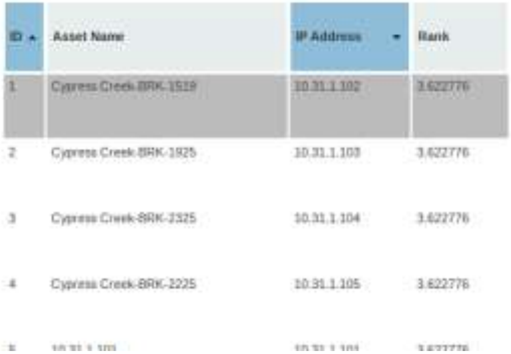

Grid Reliability

Coordinated Control

Monitoring and Detection

Cyber-Physical Security





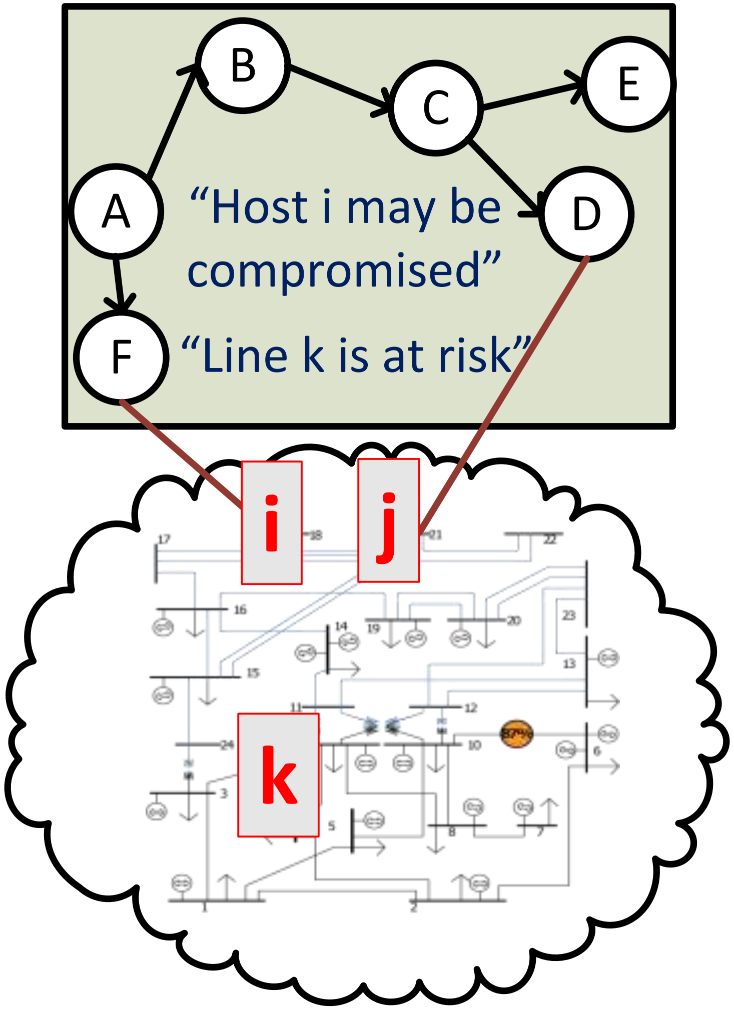
ID ▲	Asset Name	IP Address ▼	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776
5	10.31.1.101	10.31.1.101	3.622776

CyPSA Open Source Release : Armadillo

- Use high-fidelity modeling and simulation to assess the ***interdependency*** between ***cyber*** and ***physical*** infrastructure

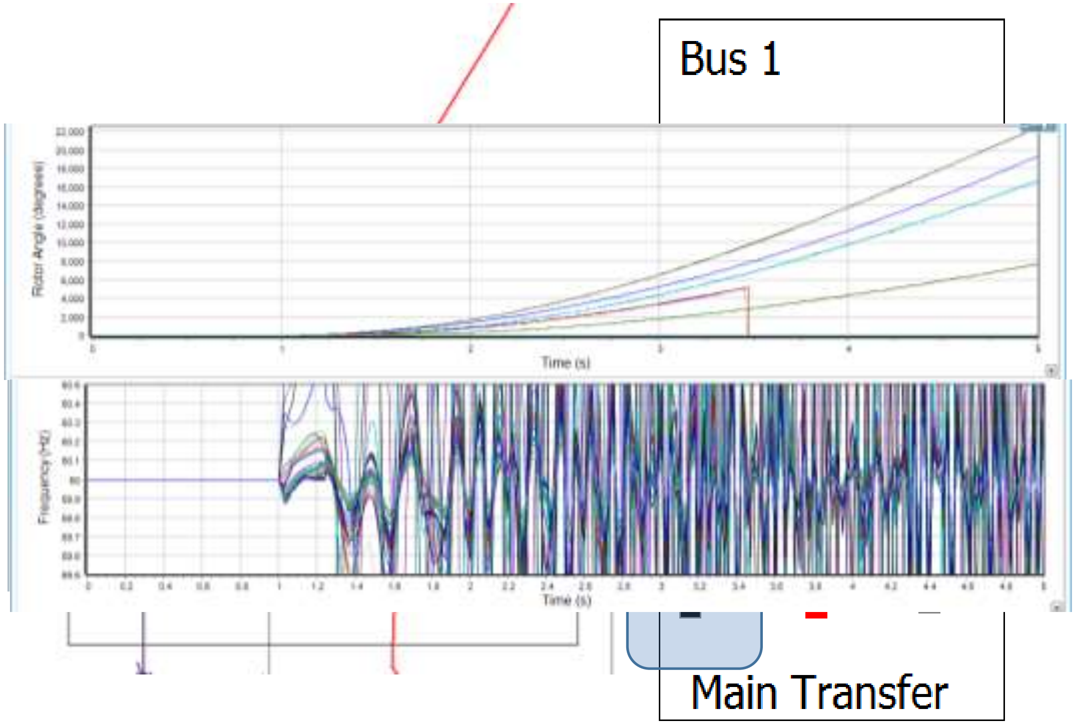
- Co-utilize information from ***cyber*** and ***power*** network to determine the ***state*** of the ***cyber-physical*** system and provide a scalable approach to detecting reliability threats due to cyber threats

Physical Connections and Impact



“Host i may be compromised”

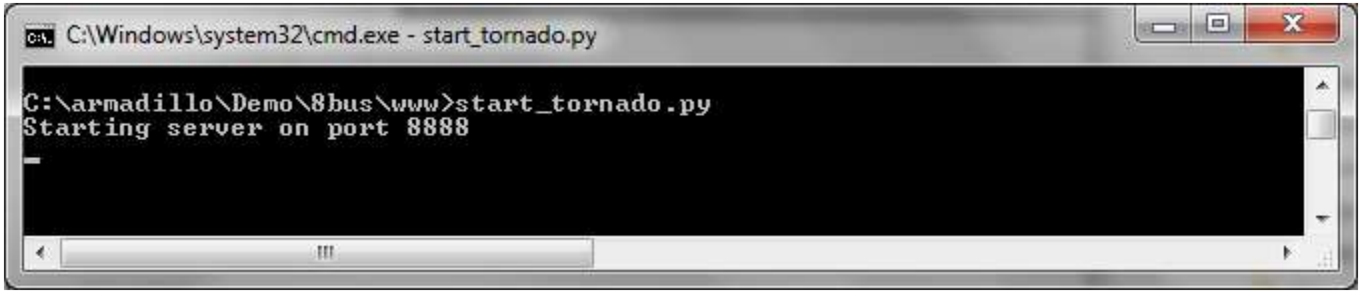
“Line k is at risk”



Demo?

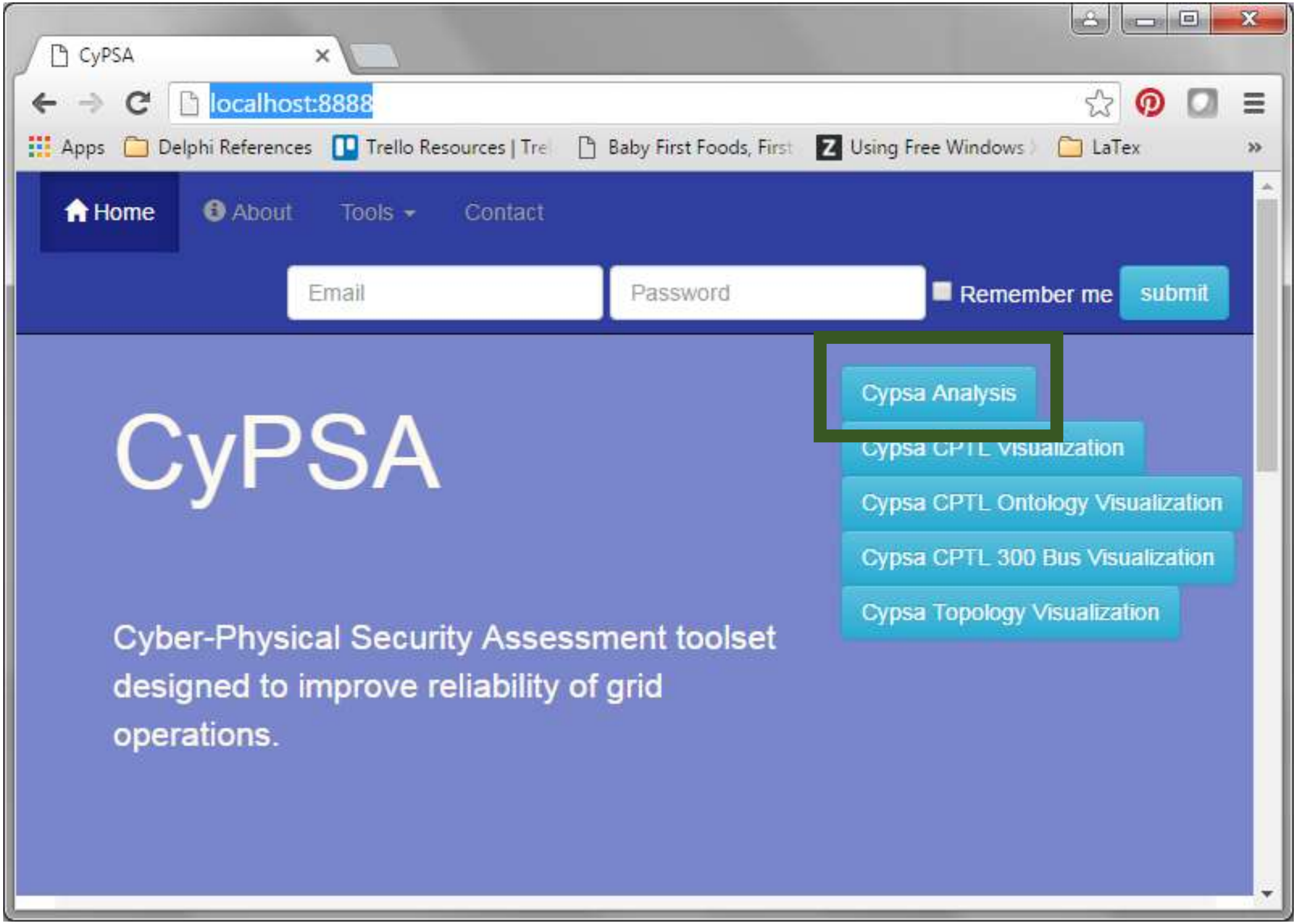
Running Armadillo

- Start backend



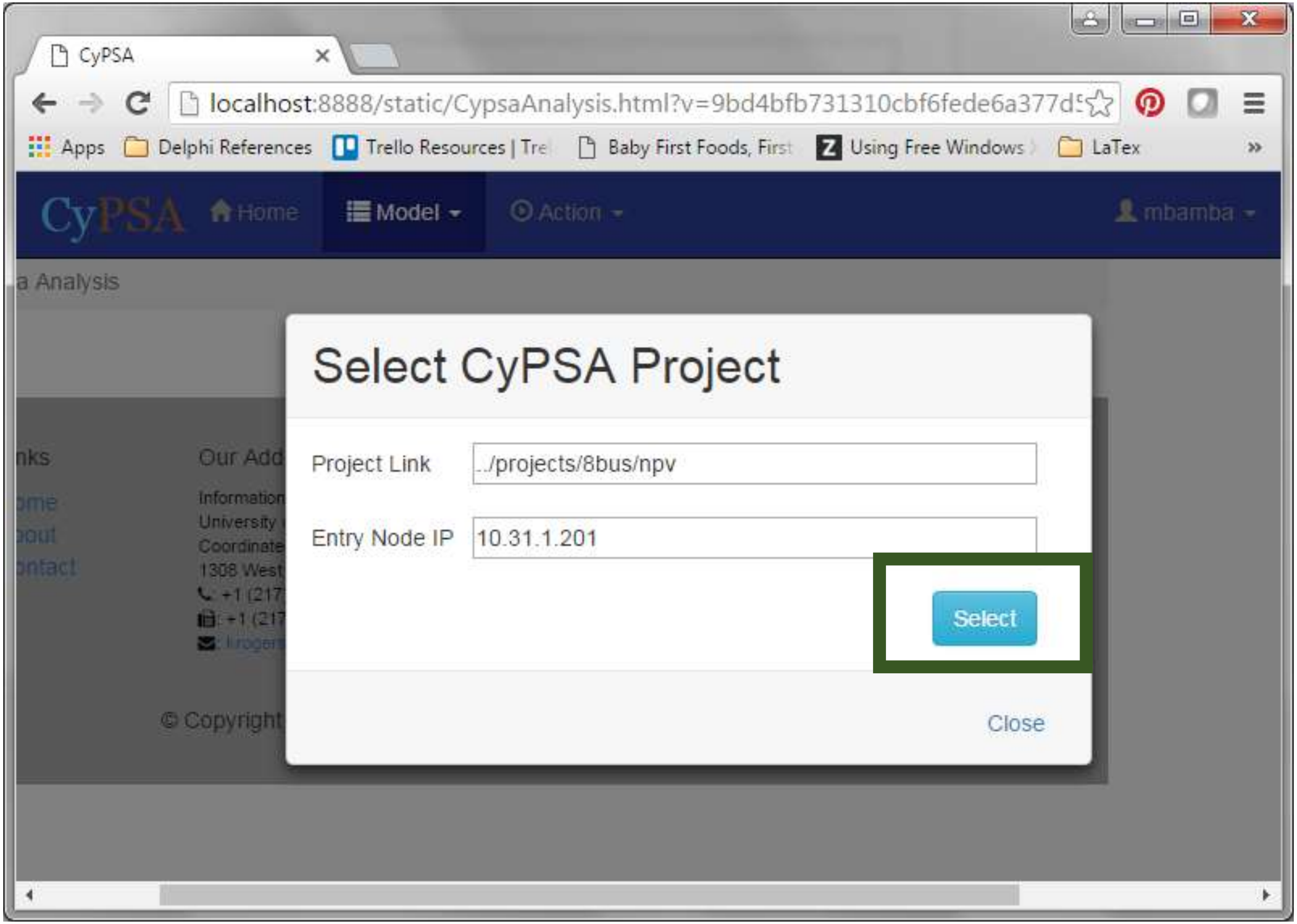
```
C:\armadillo\Demo\8bus\www>start_tornado.py
Starting server on port 8888
_
```

- Launch control panel in browser



CyPSA

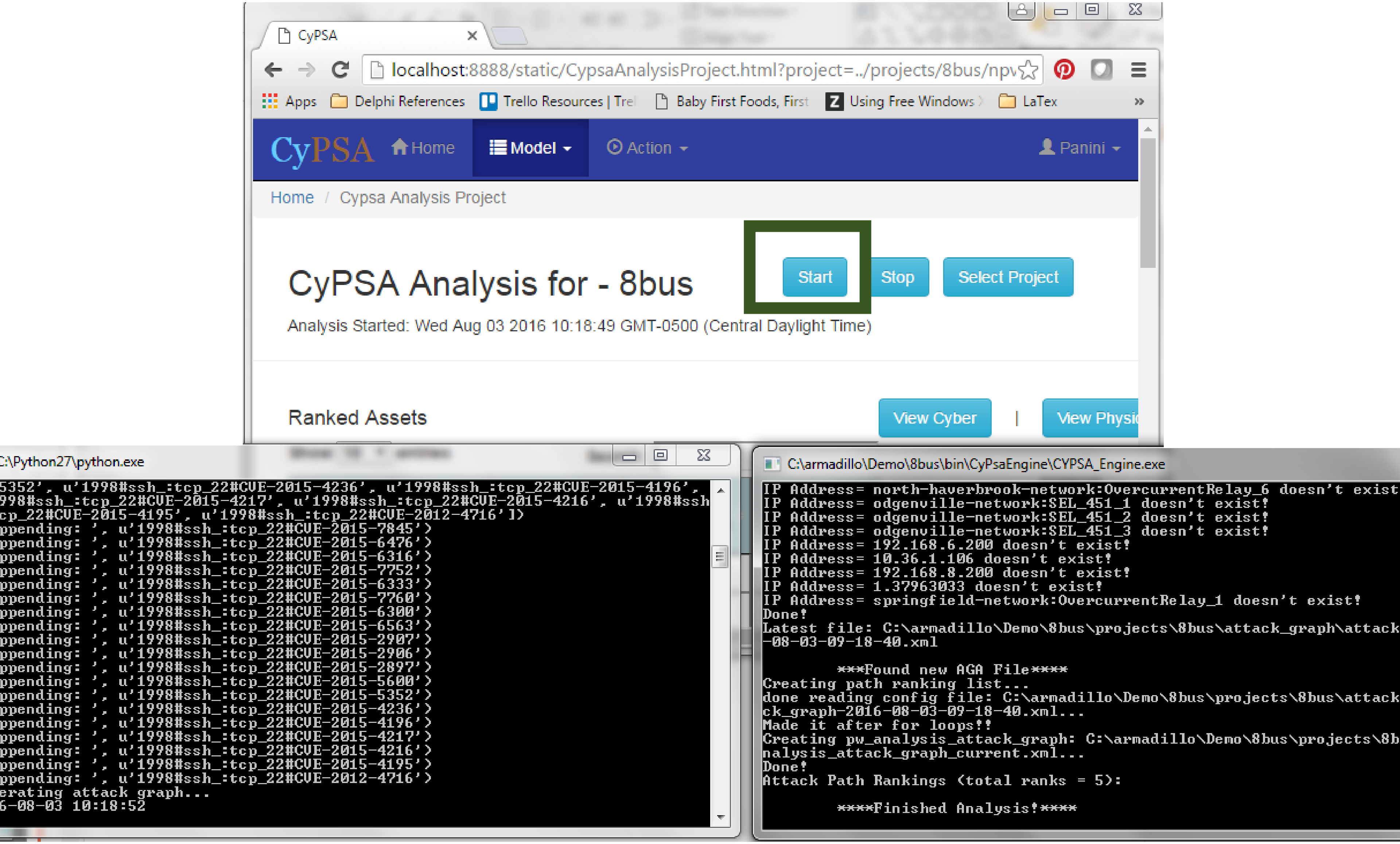
Cyber-Physical Security Assessment toolset designed to improve reliability of grid operations.



Select CyPSA Project

Project Link: ../projects/8bus/npv

Entry Node IP: 10.31.1.201



CyPSA Analysis for - 8bus

Analysis Started: Wed Aug 03 2016 10:18:49 GMT-0500 (Central Daylight Time)

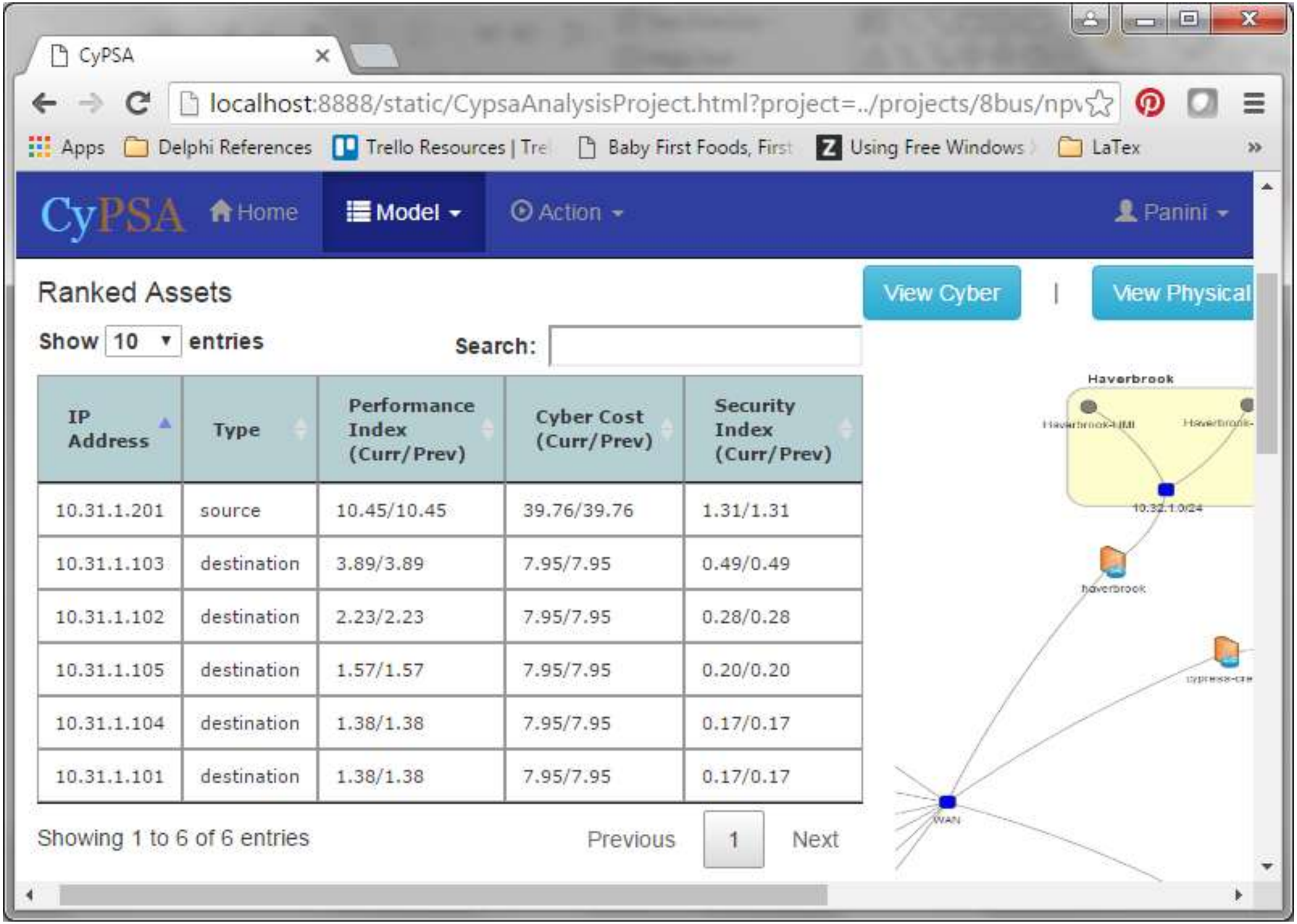
Ranked Assets

```
5352', u'1998#ssh_:tcp_22#CVE-2015-4236', u'1998#ssh_:tcp_22#CVE-2015-4196',
998#ssh_:tcp_22#CVE-2015-4217', u'1998#ssh_:tcp_22#CVE-2015-4216', u'1998#ssh
cp_22#CVE-2015-4195', u'1998#ssh_:tcp_22#CVE-2012-4716'])
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-7845')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-6476')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-6316')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-7752')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-6333')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-7760')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-6300')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-6563')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-2907')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-2906')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-2897')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-5600')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-5352')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-4236')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-4196')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-4217')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-4216')
ppending: ', u'1998#ssh_:tcp_22#CVE-2015-4195')
ppending: ', u'1998#ssh_:tcp_22#CVE-2012-4716')
erating attack graph...
6-08-03 10:18:52
```

```
IP Address= north-haverbrook-network:OvercurrentRelay_6 doesn't exist
IP Address= odgenville-network:SEL_451_1 doesn't exist!
IP Address= odgenville-network:SEL_451_2 doesn't exist!
IP Address= odgenville-network:SEL_451_3 doesn't exist!
IP Address= 192.168.6.200 doesn't exist!
IP Address= 10.36.1.106 doesn't exist!
IP Address= 192.168.8.200 doesn't exist!
IP Address= 1.37963033 doesn't exist!
IP Address= springfield-network:OvercurrentRelay_1 doesn't exist!
Done!
Latest file: C:\armadillo\Demo\8bus\projects\8bus\attack_graph\attack
-08-03-09-18-40.xml

        ***Found new AGA File****
Creating path ranking list...
done reading config file: C:\armadillo\Demo\8bus\projects\8bus\attack
ck_graph-2016-08-03-09-18-40.xml...
Made it after for loops!!
Creating pw_analysis_attack_graph: C:\armadillo\Demo\8bus\projects\8b
nalysis_attack_graph_current.xml...
Done!
Attack Path Rankings (total ranks = 5):

        ****Finished Analysis!****
```



Ranked Assets

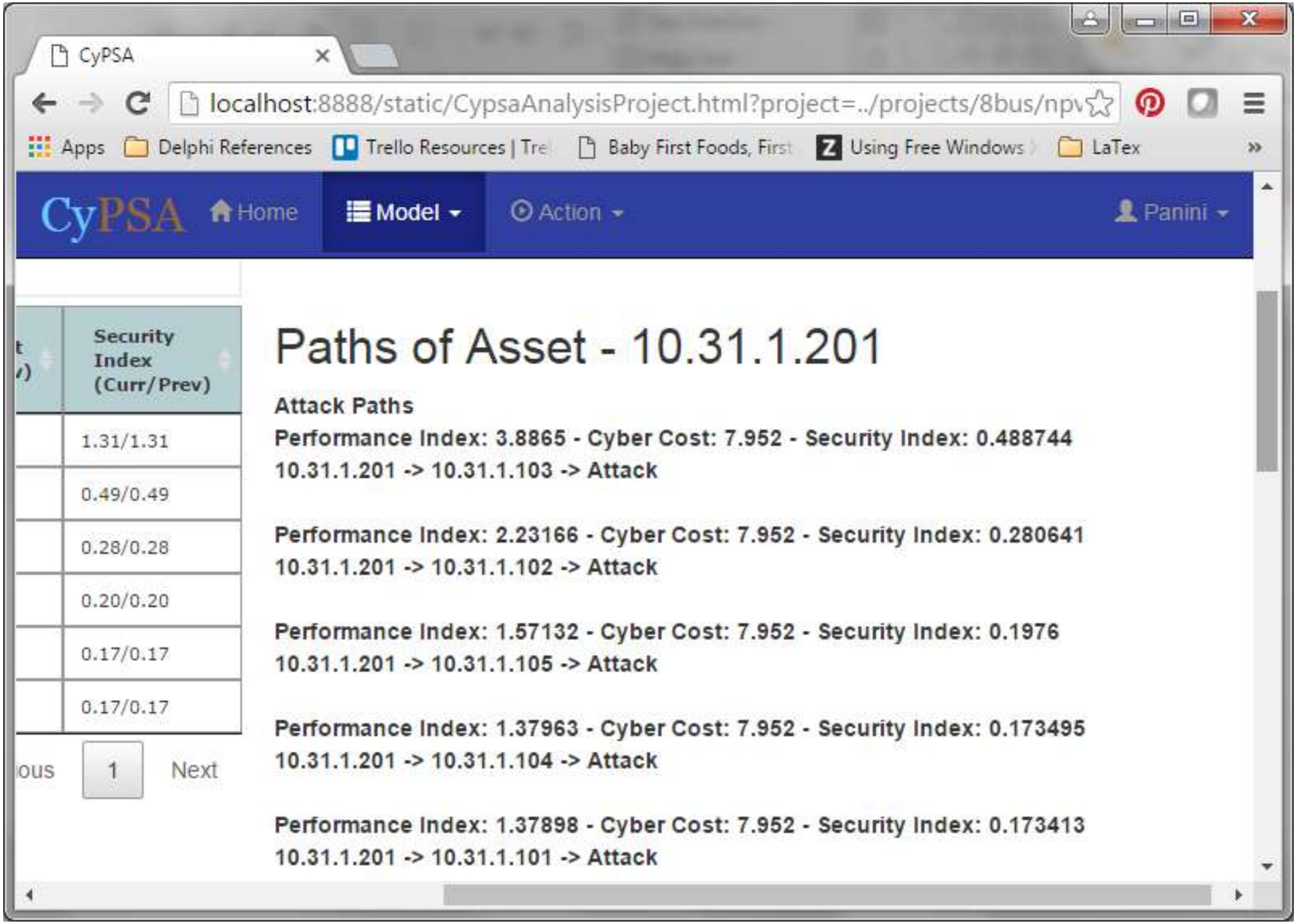
Show 10 ▾ entries

Search:

IP Address	Type	Performance Index (Curr/Prev)	Cyber Cost (Curr/Prev)	Security Index (Curr/Prev)
10.31.1.201	source	10.45/10.45	39.76/39.76	1.31/1.31
10.31.1.103	destination	3.89/3.89	7.95/7.95	0.49/0.49
10.31.1.102	destination	2.23/2.23	7.95/7.95	0.28/0.28
10.31.1.105	destination	1.57/1.57	7.95/7.95	0.20/0.20
10.31.1.104	destination	1.38/1.38	7.95/7.95	0.17/0.17
10.31.1.101	destination	1.38/1.38	7.95/7.95	0.17/0.17

Showing 1 to 6 of 6 entries

Previous 1 Next



Security Index (Curr/Prev)
1.31/1.31
0.49/0.49
0.28/0.28
0.20/0.20
0.17/0.17
0.17/0.17

Paths of Asset - 10.31.1.201

Attack Paths

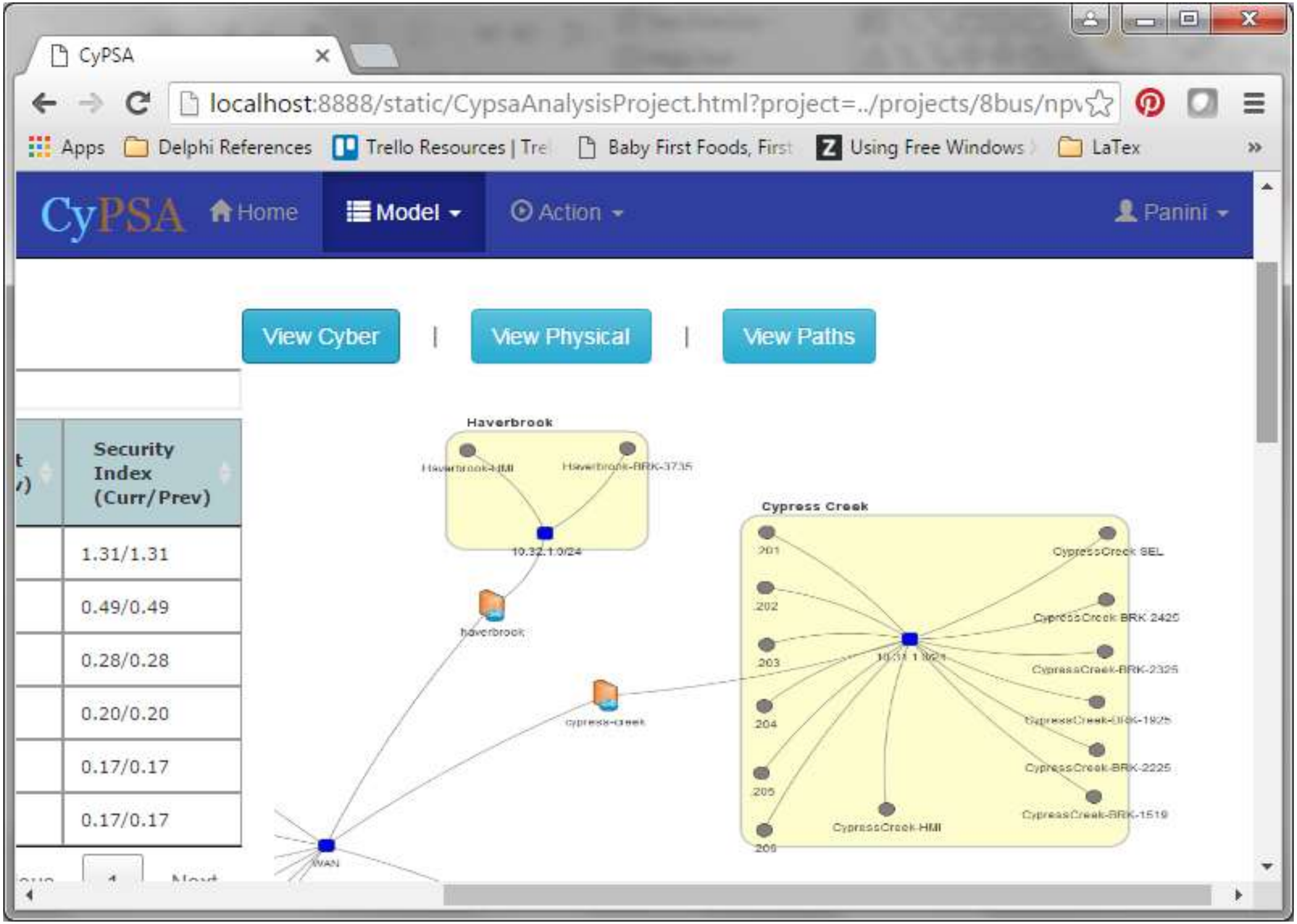
Performance Index: 3.8865 - Cyber Cost: 7.952 - Security Index: 0.488744
10.31.1.201 -> 10.31.1.103 -> Attack

Performance Index: 2.23166 - Cyber Cost: 7.952 - Security Index: 0.280641
10.31.1.201 -> 10.31.1.102 -> Attack

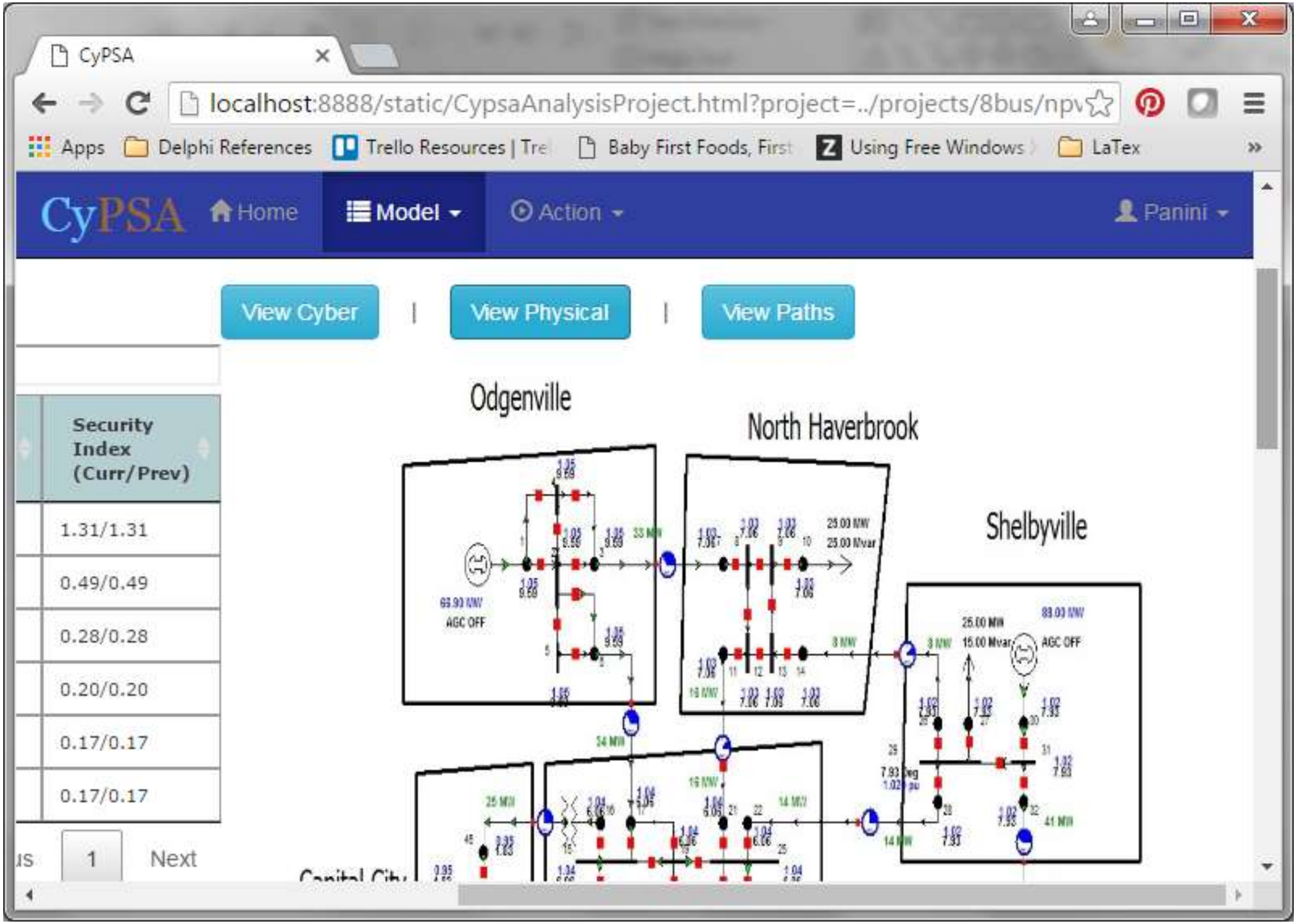
Performance Index: 1.57132 - Cyber Cost: 7.952 - Security Index: 0.1976
10.31.1.201 -> 10.31.1.105 -> Attack

Performance Index: 1.37963 - Cyber Cost: 7.952 - Security Index: 0.173495
10.31.1.201 -> 10.31.1.104 -> Attack

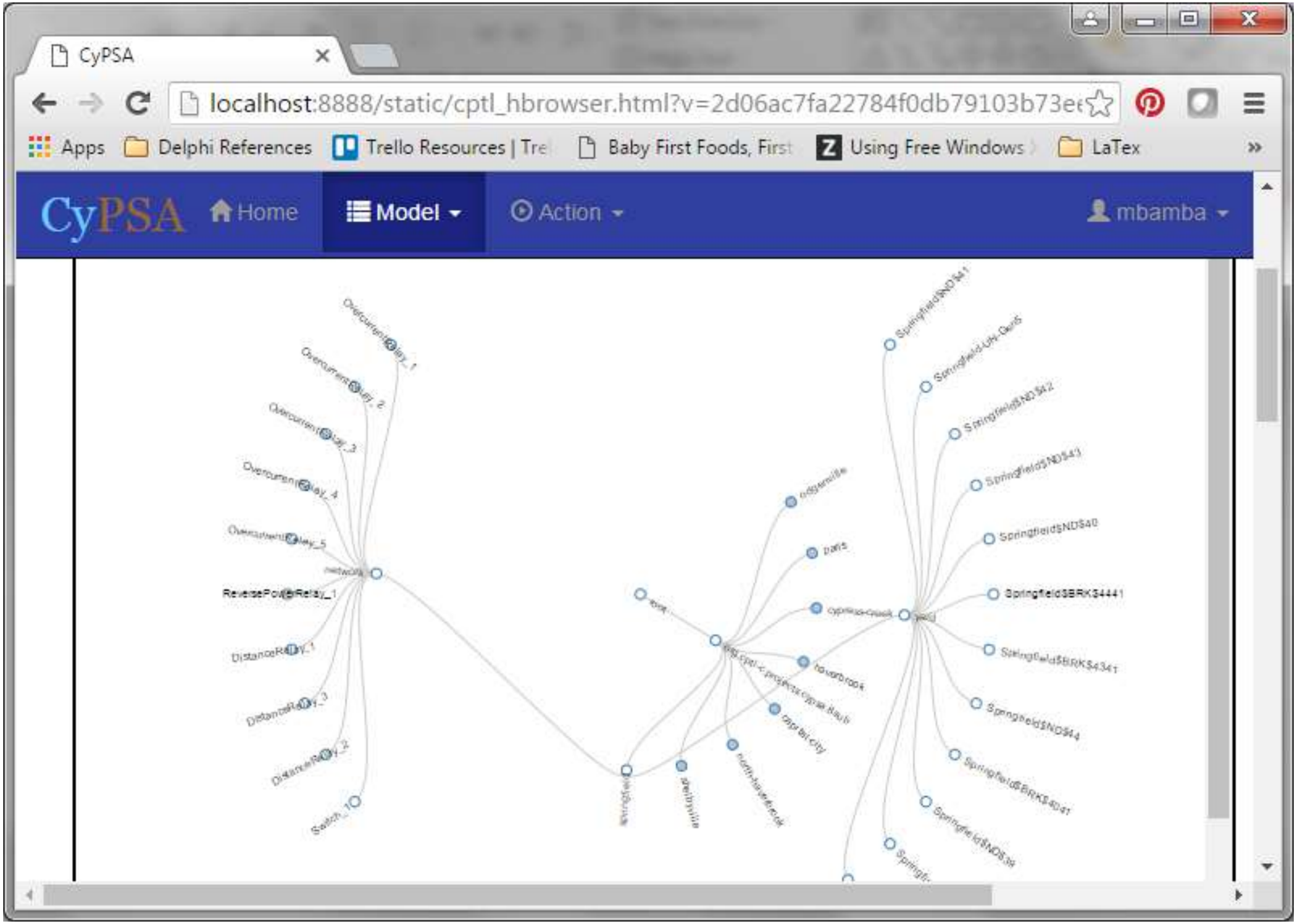
Performance Index: 1.37898 - Cyber Cost: 7.952 - Security Index: 0.173413
10.31.1.201 -> 10.31.1.101 -> Attack



t /)	Security Index (Curr/Prev)
	1.31/1.31
	0.49/0.49
	0.28/0.28
	0.20/0.20
	0.17/0.17
	0.17/0.17



Security Index (Curr/Prev)
1.31/1.31
0.49/0.49
0.28/0.28
0.20/0.20
0.17/0.17
0.17/0.17


CyPSA
localhost:8888/static/cptl_hbrowser.html?v=2d06ac7fa22784f0db79103b73e
Apps
Delphi References
Trello Resources | Tre
Baby First Foods, First
Using Free Windows
LaTex
CyPSA
Home
Model
Action
mbamba
OvercurrentRelay_1
OvercurrentRelay_2
OvercurrentRelay_3
OvercurrentRelay_4
OvercurrentRelay_5
network
ReversePowerRelay_1
DistanceRelay_1
DistanceRelay_3
DistanceRelay_2
Switch_1
root
ogdenville
paris
cypress-creek
grid
haverbrook
capital city
north-haverbrook
shelbyville
Springfield
Springfield$ND$41
Springfield-UN-Gen5
Springfield$ND$42
Springfield$ND$43
Springfield$ND$40
Springfield$BRK$4441
Springfield$BRK$4341
Springfield$ND$44
Springfield$BRK$4041
Springfield$ND$39
Springfi

More than just power

- The CyPSA engine can be used on things other than the power grid
- The open source release have JSON templates for entering your own impact data
- This allows for the engine to be run stand alone to make a list of top Cyber/Physical contingencies

How do I do that shit?

In order to run offline mode manually, do the following steps:

1. Make sure the CPGenOutput.csv file is located in the project folder. You should also configure the location in the config.dat file under the tag "CP_GEN_OUTPUT_FILE".

2. When using runCypsa.bat, just add a 3rd command line option "offline".
For example, to run the 8bus model, just call "runCypsa.bat 8bus 10.31.1.201 offline"

STOP
$2
-A-HOOP

CYPSA

Cyber/Physical Situational Awareness

Thank You!

CyPSA Project – U. of Illinois

Kate Davis kate@kaedago.com

Edmond Rogers edmond@kaedago.com

www.github.com/bigezy/armadillo

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

www.kaedago.com