CyPSA
Cyber Physical Situational Awareness

Kate Davis
Cyber-Physical Security Assessment (CyPSA)

ARPA-E   DE-AR0000342   $1.5M   Apr 2013 – Aug 2016

Topologies
- Cyber Network Topology
- Power System Topology
- Device Cyber/Physical Interconnections

Cyber Threats
- Cyber State Information
- Consequence Analysis

Power Flows
- Compute Connectivity, Attack Graph Analysis, Physical Impact Analysis, and Rankings

Situational Awareness
- Ranked Contingency List
Team

Kate Davis
Robin Berthier
David Nicol
Edmond Rogers
Pete Sauer
Olivier Soubigou
Gabe Weaver
Rakesh Bobba
Panini
Patapanchala
Matt Davis
Saman Zonouz
Luis Garcia
Tim Heidel
Erik Desrosiers
CyPSA Project Objectives

- To describe the function of individual device operations
- Focus analyst effort to have the greatest benefit
- Mapping relays to model and network has been challenging
- Recent advances in computing allow for development of cyber physical transient stability studies
- This calculation can be performed every 15 minutes as system conditions change
- Real time calculations provide for more reliable operation by addressing previously undefined contingencies
Accomplishments

- CyPSA testing with a municipal utility and Avista
  - Successfully modeled their transmission network
  - Validated cyber physical model
  - Improved and added to use cases

- Refactored toolset and released in August 2016

- Provided dynamic visualizations of cyber physical interaction

- Successfully performed cyber physical contingency analysis within 15 minutes
Challenges

- Consideration of all potential cyber access paths was very challenging

- This challenge was resolved by limiting the scope of potential cyber access paths by considering attack surface reduction provided by firewalls

Remaining challenges
- Providing automated means to index relay configuration
  - Currently this information resides in confederated databases
- Integration of Cyber Security State Estimation
  - Need to mature cyber/physical inventory modeling
- Visualization of larger networks
  - Need to develop ways to effectively display over lots of devices
Lessons Learned

- We identified how to quickly mature the aspects of CyPSA that can be most beneficial to utilities *now*
  - Mapping relay to breakers
  - Cyber/Physical inventory

- We identified how CyPSA can provide information that planners can use to positively impact Reliability
Models

- The team needed to create realistic data sets to use in the CyPSA engine

- Two synthetic models have been created with detailed information for an 8 and 300 bus model

- The models have detailed information
  - Firewall configuration
  - Relay to breaker tie information
  - IP address information for operational devices
300 Bus Model

Overall Project Accomplishments
Cyber-Physical Test Cases

- In proof of concept testing, an 8 bus model was used extensively.

- This included reproduction of 3 of the 8 substations in the 8 bus model in our lab at UIUC.

- This allowed for validation that the CyPSA engine performed its intended function.

- From there the team developed a cyber physical model of the IEEE 300 bus model:
  - 298 substations and over 5000 cyber devices.
Achieving the Mission

- Kaedago is “Small-wires-up instead of big-wires-down”
- Effort with Avista, SEL, and PowerWorld
- Online retrieval, management, and model mapping of device-level relay data
- Identification and prioritization of most critical devices
  - By IP exposure and attack surface
  - By system-wide impact of “torturing relays”
    - Critical clearing time
  - For cyber-physical situational awareness (CyPSA)
Status and Plans

- Tech-to-Market and Commercialization led by kaedago

### 2017 Goals

- Control Panel
  - Prioritization
  - Aggregate Exposure
  - Patching
  - Baseline
  - Change indication
  - Cyber incident planning

### Project Information

- **Project Name:** 8bus
- **Entry Point:** 10.31.1.201

#### Table:

<table>
<thead>
<tr>
<th>Relay</th>
<th>Address</th>
<th>Performance</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.7.200</td>
<td>1.37953033</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10.37.1.201</td>
<td>2.0330608</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10.37.1.101</td>
<td>2.0330608</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10.37.1.102</td>
<td>2.0330608</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>192.168.1.200</td>
<td>1.37953033</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10.31.1.201</td>
<td>1.37953033</td>
<td></td>
</tr>
</tbody>
</table>

### Cyber Connectivity

- Threat surface

### SEL and RTAC Relays

- PowerWorld Corporation

### CyPSA

- Power quality and system analysis tool for power systems.
Technology-to-Market

- T2M focus has been narrowed significantly due to feedback from utility partners

- Inventory of cyber physical assets has been identified as a minimum viable product

- Continued research efforts depend on being able to automate collection of the necessary tie information

- PowerWorld users and planners at utilities need a system to define their cyber physical inventory
Partners

› PowerWorld has been on the team since the beginning of the project
  – Cyber object integration in latest version of PowerWorld

› Schweitzer Engineering Labs (SEL) is also providing support of the CyPSA effort and working with the team as we engage utilities

› As we encounter larger utilities, it has been a challenge balancing compliance, infosec, and operational units
Provides support and installation for CyPSA

Commercial client kaedago for automation of relay cyber/physical tie information

Presented at WECC PowerWorld users group

Partners with SEL, PowerWorld, and Network Perception
Conclusions

‣ We are pursuing commercial opportunities that will enable the use of cyber-physical analysis tools in industry.

‣ Enable further applications including cyber incident detection components of the research.

‣ Release 8 and 300 bus models for researchers to use.

‣ Finding an effective means of visualization weighs heavily on the success of active components.
Questions?

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

Kate Davis
krogers6@illinois.edu
kate@kaedago.com

Edmond Rogers
ejrogers@Illinois.edu
edmond@kaedago.com