Online Intrusion Tolerance and Response in Power Systems

Kate Davis

Texas A&M University

(katedavis@tamu.edu)

PSERC Webinar
January 23, 2018

Presentation Outline

- **Cyber-Physical Perspective**
- **Formulating Attack-Resilient Response**
  - **Requirements**
  - **Cyber-Side and Physical Controls**
  - **Operational Challenges**
  - **Future Work**
- **Discussion**

Acknowledgement

- **NSF Cyber-Physical Systems (CPS) Awards 1446229 and 1446471**

- **Team:**
  - Shamina Hossain-McKenzie (Sandia, formerly UIUC)
  - Maryam Kazerooni (Apian Way, formerly UIUC)
  - Sriharsha Etigowni (Rutgers)
  - Saman Zonouz (Rutgers)
  - Kate Davis (TAMU, formerly UIUC)

Cyber-Physical Perspective: Resilience

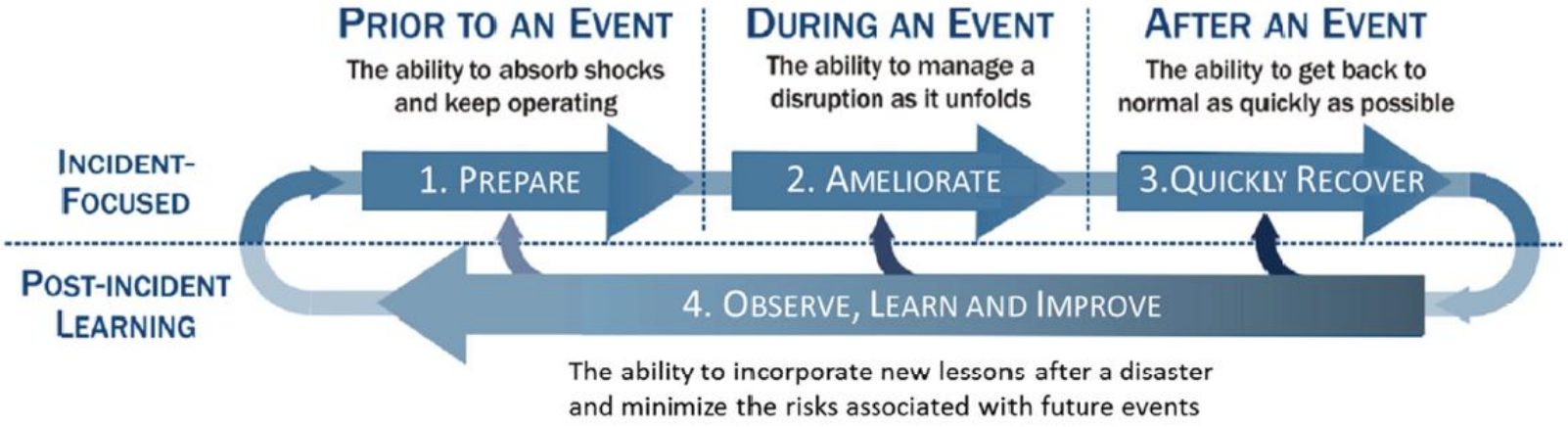


Fig. 1.2 (A), p. 36

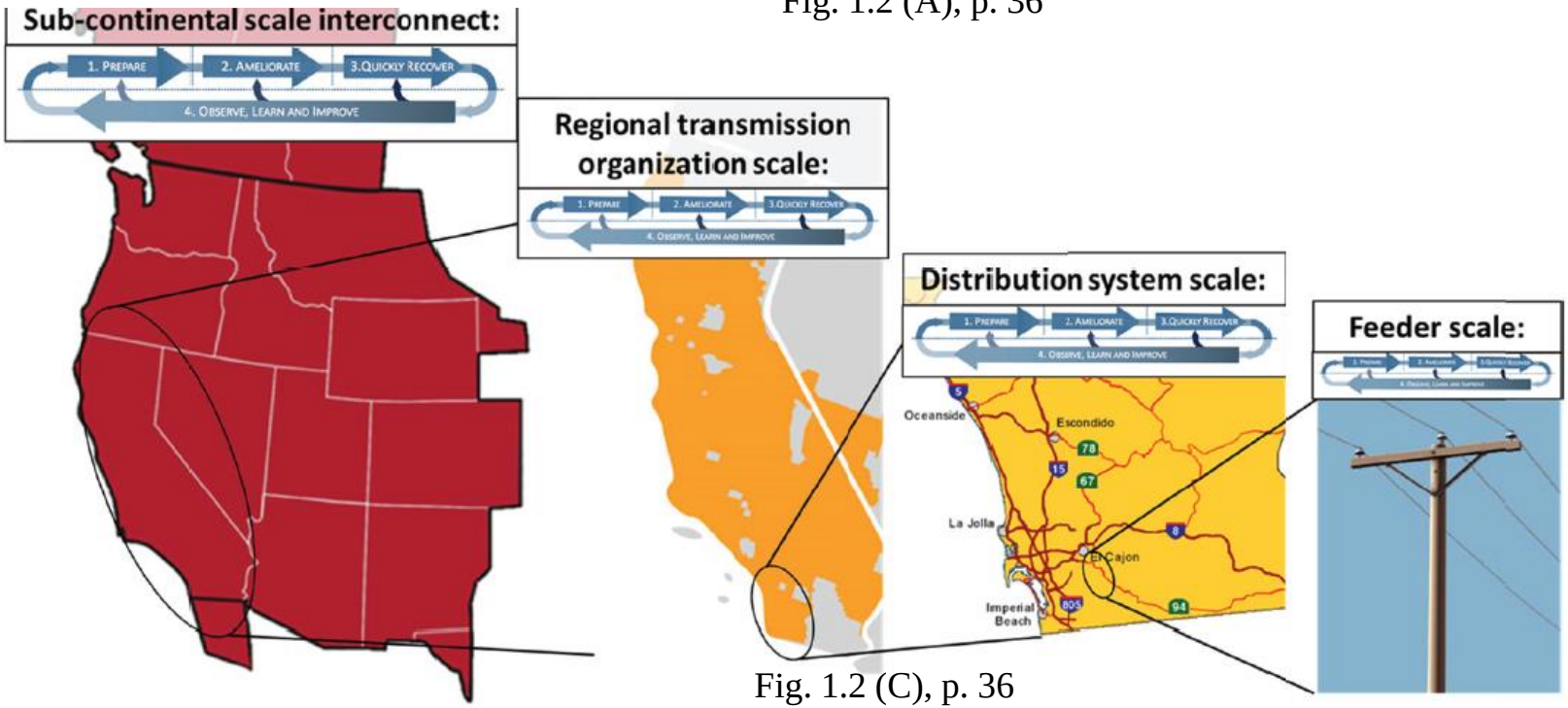


Fig. 1.2 (C), p. 36

The National Academies "Enhancing the Resilience of the Nation's Electricity System," July 2017.

Threats to Resilience

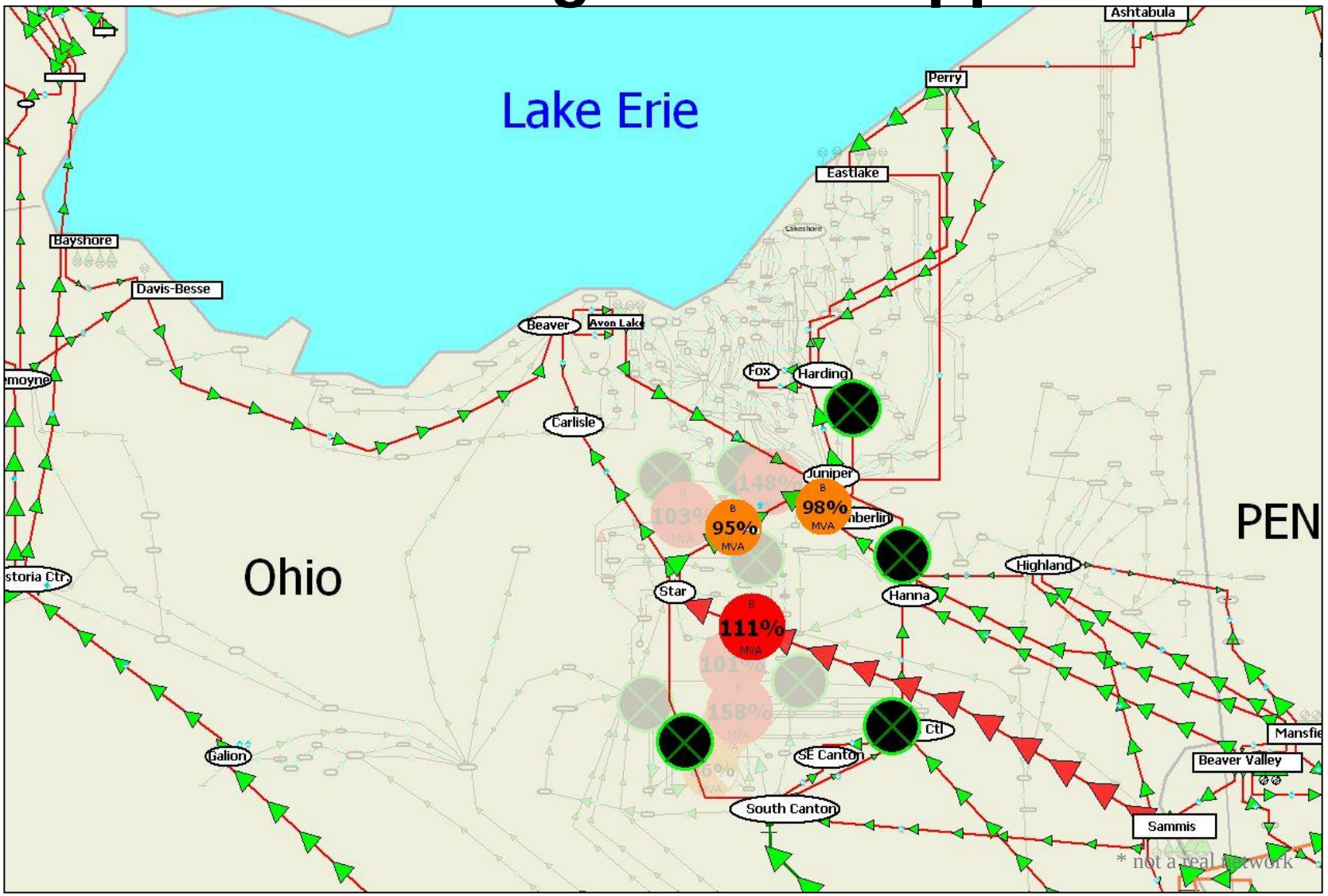
BOX S.1

Causes of Most Electricity System Outages (shown in alphabetical order and reviewed in Chapter 3)

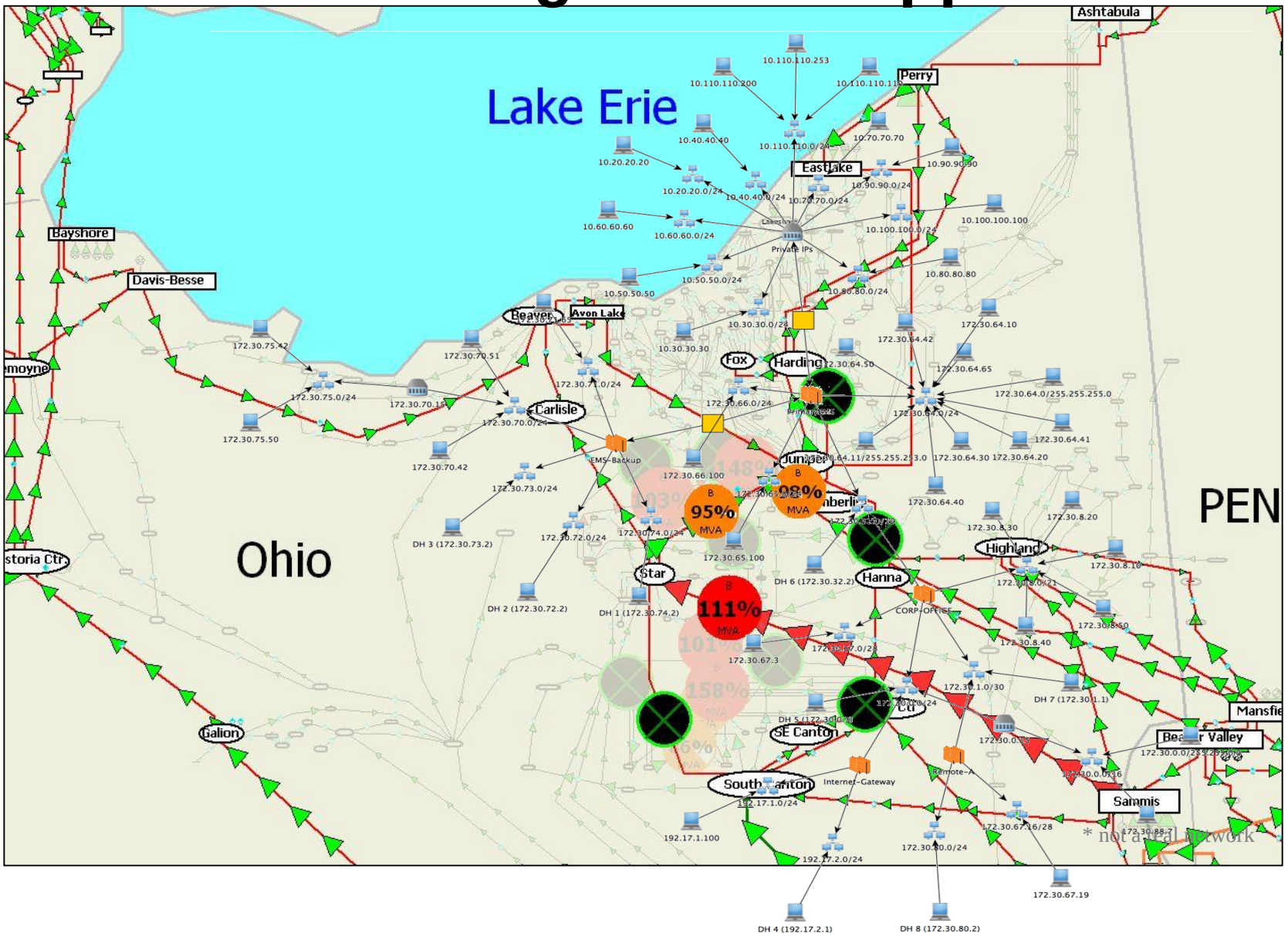
- Cyber attacks
- Drought and water shortage
- Earthquakes
- Floods and storm surge
- Hurricanes
- Ice storms
- Major operations errors
- Physical attacks
- Regional storms and tornadoes
- Space weather and other electromagnetic threats
- Tsunamis
- Volcanic events
- Wildfires

The National Academies "Enhancing the Resilience of the Nation's Electricity System," July 2017.

Operating Though Failure: A Graceful Degradation Approach

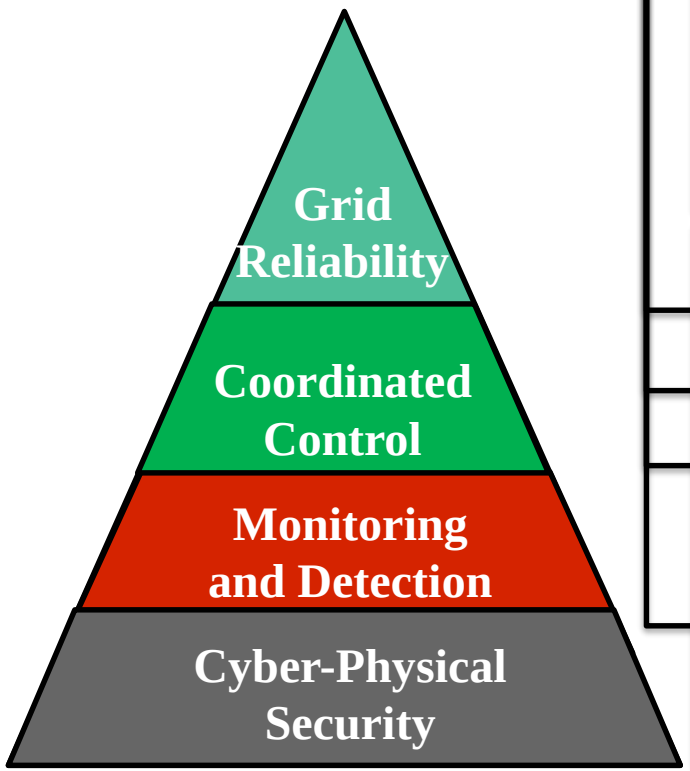


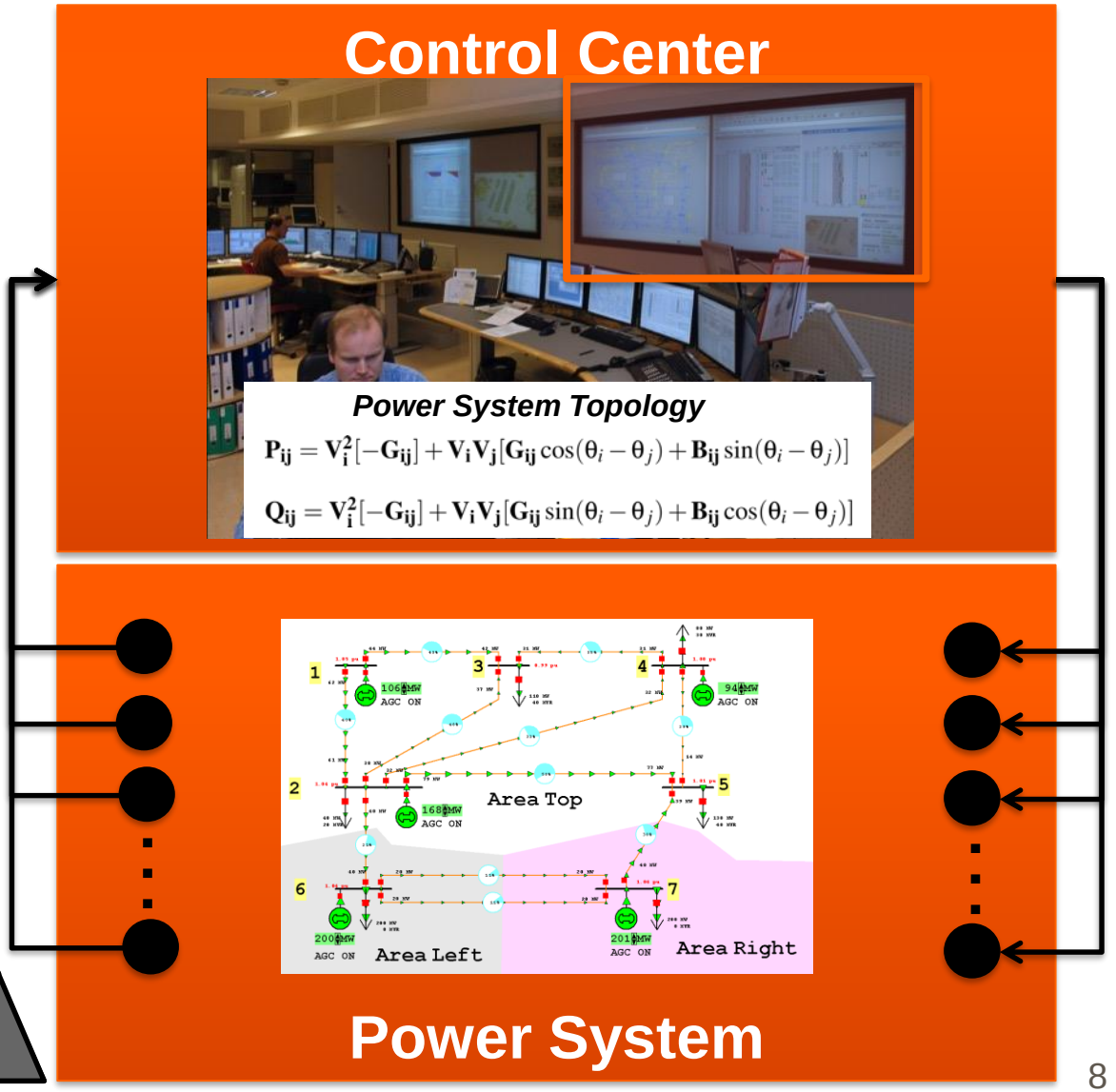
Operating Though Failure: A Graceful Degradation Approach



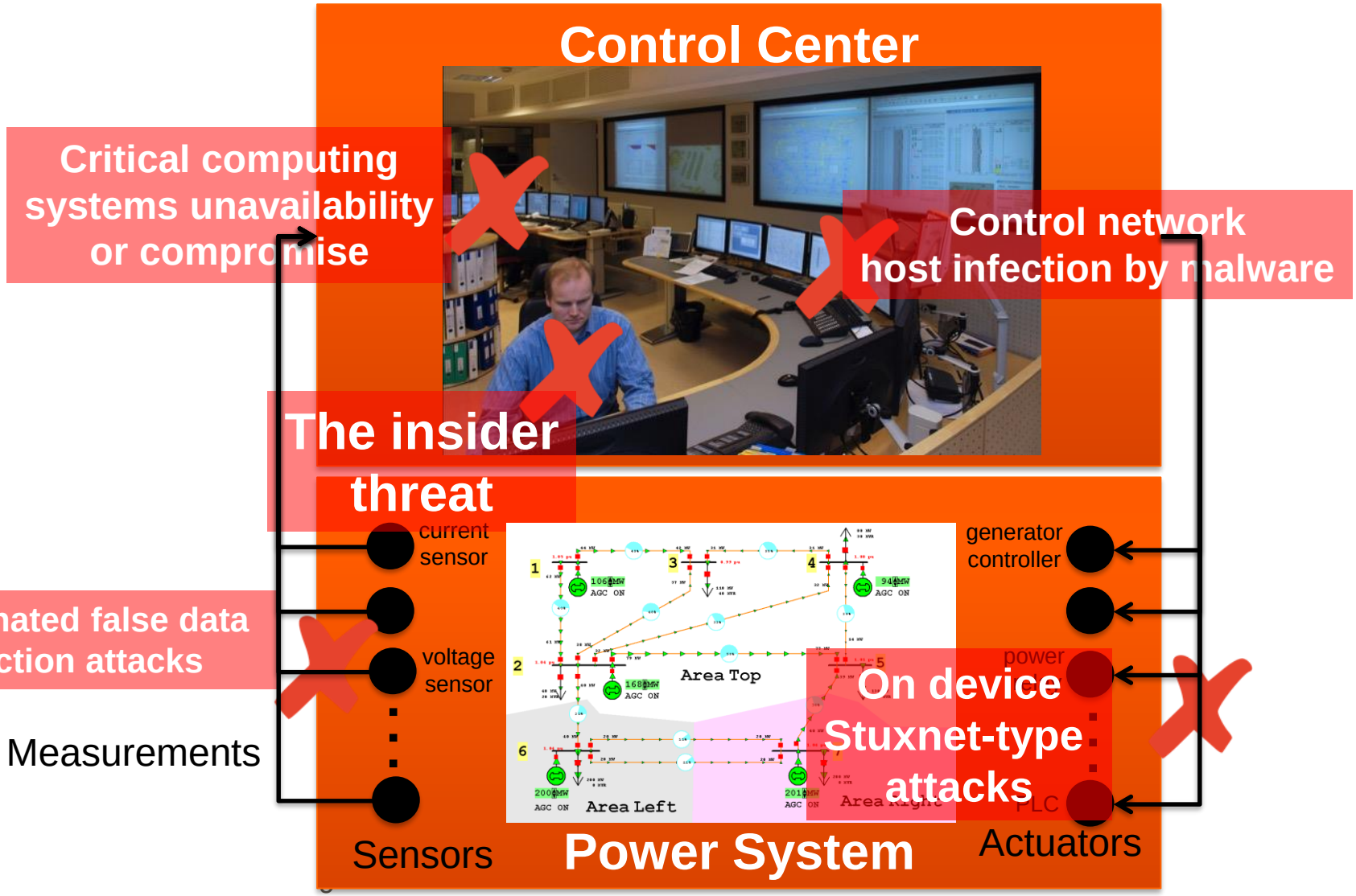
Resilience Needs Data Flow Assurance

1. Monitoring
2. Analysis
3. Control



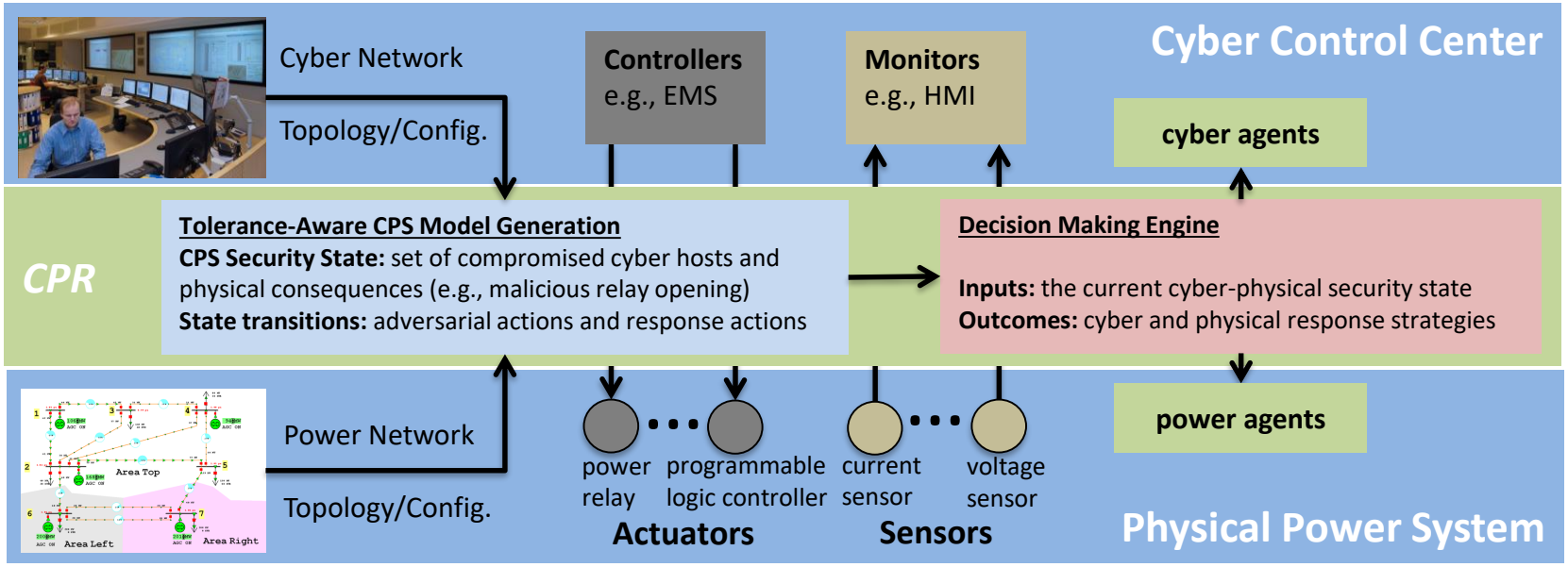


Some Critical Attack Surfaces



Cyber-Physical Intrusion Tolerance & Response

- Estimate cyber-physical security state
- Determine & actuate optimal response based on both cyber and power networks



NSF CPS Award Numbers: 1446229 and 1446471

Response Strategies

- Must take into account the power system when deciding upon a cyber-based action
  - Example: prioritize the recovery of a device affecting control of a critical generator
    - Failure leads to severe physical impact

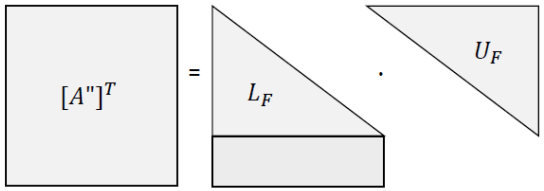
- Must be cyber-security-aware when making power operating decisions
  - Example: isolate or disable a compromised controller from the rest of the system
    - Then, apply corrective controls to compensate

Strategy: Identify Controller Response Sets

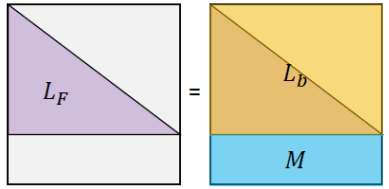
Can be computed quickly

- ***Critical controllers*** (u_{C_i}): devices that are irreplaceable and mandatory for system controllability
- ***Essential controllers*** (u_{E_i}): minimal set of devices required to maintain system controllability
- ***Redundant controllers*** (u_{R_i}): devices that can be removed without affecting system controllability

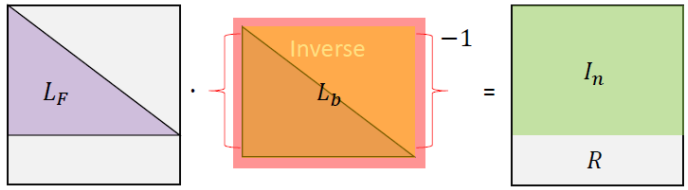
$[A"]^T = \mathrm{L}_F \cdot U_F$



$L_F = \begin{bmatrix} L_b \\ M \end{bmatrix}$



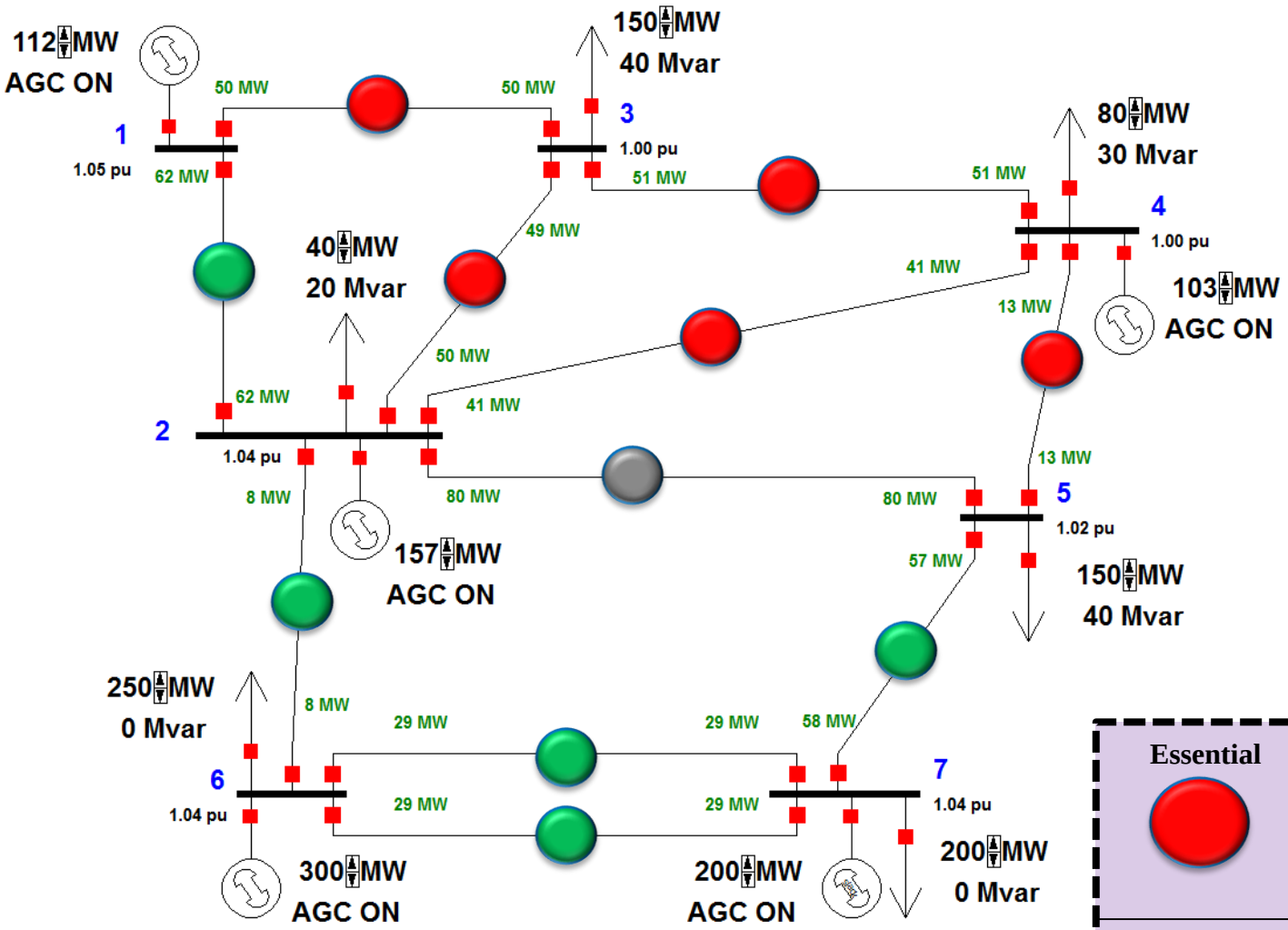
$\mathrm{L_{CER}} = \mathrm{L}_F \cdot L_b^{-1} = \begin{bmatrix} I_n \\ R \end{bmatrix}$

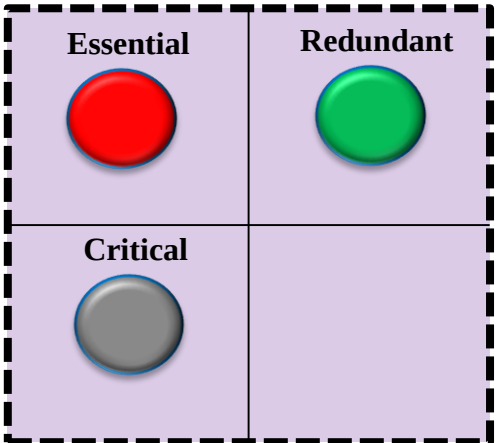


	EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6	
Essential/Critical	1.0000	0	0	0	0	0	
	0	1.0000	0	0	0	0	I_n
	0	0	1.0000	0	0	0	
	0	0	0	1.0000	0	0	
	0	0	0	0	1.0000	0	
	0	0	0	0	0	1.0000	
Redundant	-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000	
	-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000	R
	0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466	
	-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000	

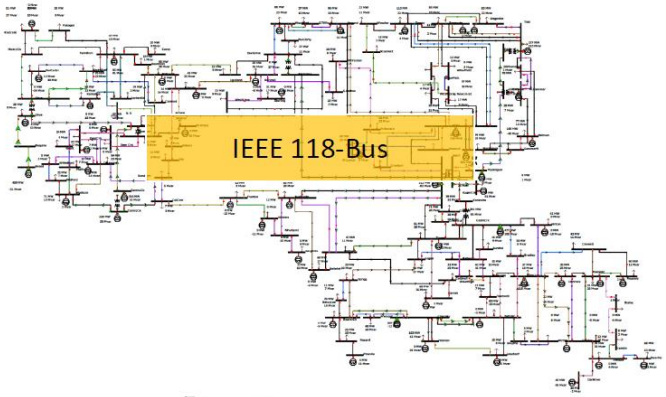
(*) Hossain-McKenzie et al., “Distributed Controller Role and Interaction Discovery,” *ISAP 2017*.

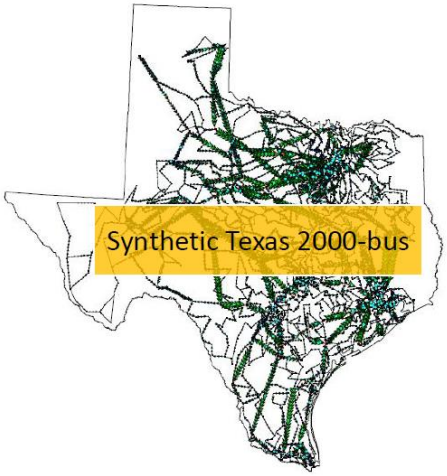
Example Controller Response Sets

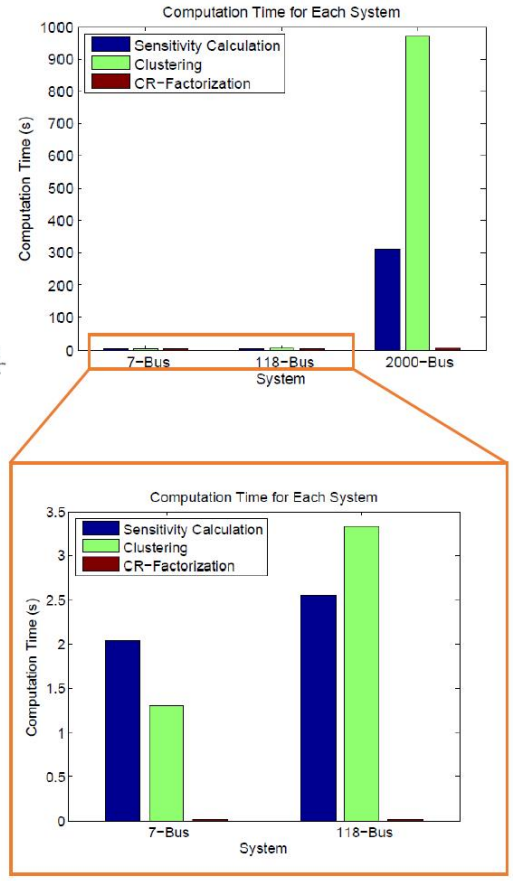




IEEE 118-Bus and Texas 2000-Bus Computation Times







Maximizing Controllability Span

- Essential controllers are a minimal set

Obtain sensitivity matrix A''

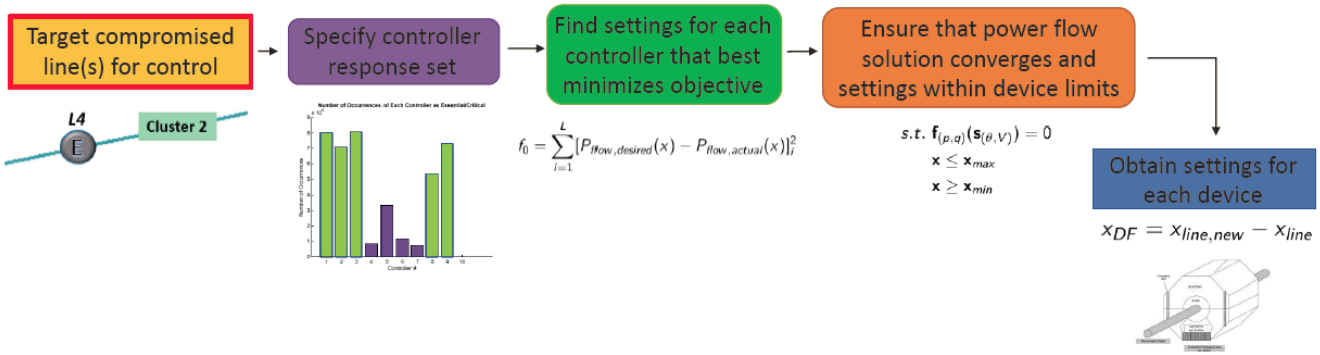
- Must reflect control parameter and controlled quantity

Process rows of A'' with clustering

- Calculate coupling index and data-dependent cluster number
- Determine Line Flow and Control Support Groups

Process columns of A'' with LU decomposition

- Apply on modified, target A'' set
- Determine Critical, Essential, and Redundant Controller Sets



(*) Hossain-McKenzie et al., “Distributed Controller Role and Interaction Discovery,” *ISAP 2017*.

Strategy: Eliminating Critical Controllers

- Optimize controller placement to avoid critical controllers over a wide range of conditions

Table 4: Transformed Basis with Added Redundant Controller to Line 5

EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6
1.0000	0	0	0	0	0
0	1.0000	0	0	0	0
0	0	1.0000	0	0	0
0	0	0	1.0000	0	0
0	0	0	0	1.0000	0
0	0	0	0	0	1.0000
-0.0014	-0.0000	-0.0000	0.0899	-0.0000	-0.0000
-0.0000	0.0000	1.0000	-0.0000	-0.0000	0.0000
-0.0144	0.0000	-0.0000	0.9227	-0.0000	-0.0000
0.0000	1.5107	0.0000	-0.0018	-1.0644	0.7466
-0.1250	-0.0000	0.0000	-0.1865	0.0000	-0.0000

(*) Chen, Abur, “Placement of PMUs to Enable Bad Data Detection in State Estimation,” 2006.

Strategy: Optimize Essential/Redundant

- Focus here is on actions AFTER compromise
- Optimal response with the recurrent controllers performed best over a variety of compromise scenarios

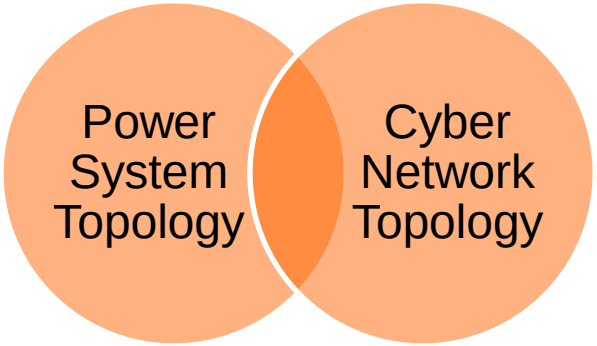
TABLE IV: Responding to Controller Compromises with Recurrent CE Response Set and Calculated Settings

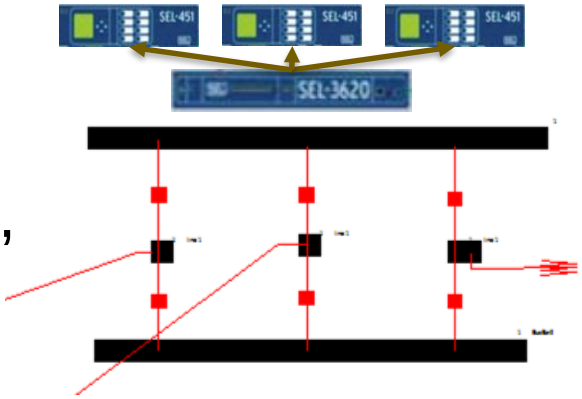
$C\#_{Compr.}$	x_{DF} (pu)	MVA $L\#,Orig.$	MVA $L\#,Compr.$	$C\#_{Resp.}$	Settings (pu)	MVA $L\#,Resp.$
2	-0.072	44.2%	55.7%	1,3,8,9	-0.015,-0.054, 0.072,-0.018	48.9%
4	-0.054	44.5%	56.8%	1,2,3,8,9	0.015,-0.072, -0.054,0.072,-0.018	46.8%
5	-0.036	67.6%	78.6%	1,2,3,8,9	0.015,-0.072, -0.054,-0.072,-0.018	71.9%
7	-0.009	23.5%	24.3%	1,2,3,8,9	0.0088,-0.0077, -0.0127,0.002,0.0017	22.9%
9	-0.018	32.8%	35.5%	N/A	N/A	–
10	-0.072	14%	17.6%	1,2,3,8,9	0.015,-0.072, -0.054,-0.072,0.018	15.7%
2,10	-0.072,-0.072	44.2%, 14%	55.5%, 17.3%	1,3,8,9	-0.015,-0.054, 0.072,0.018	49%, 16.3%
4,5,9	-0.054,-0.036, -0.018	44.5%, 67.6%, 32.8%	53.8%, 74.4%, 31.5%	1,2,3,8	0.015,-0.072, -0.054,-0.072	46.8%, 70.4%, 31.6%

(*) S. Hossain-McKenzie, et.al., “Proactive Control Strategies Against Distributed Controller Compromise in Power Systems,” in review.

Cyber and Physical State Awareness

- **To defend your system from these threats, you need a map**
- A cyber-physical map describes the linkages between the cyber and physical systems
- The map tells what relays, RTUs, IEDs, etc. control what physical devices
- Found in the substation design and the protection settings



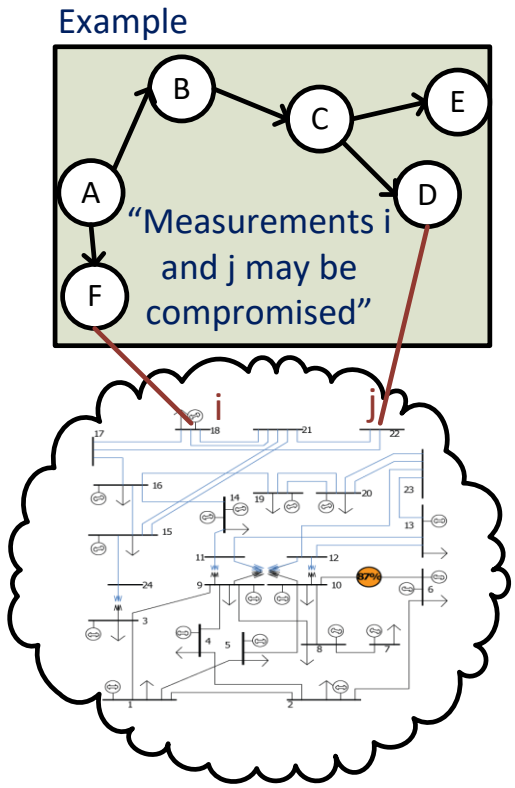


Cyber-Physical View: Substation

Cyber and Physical State Awareness

- Model and simulate the ***interdependencies*** between ***cyber*** and ***physical*** infrastructure

- Co-utilize information from ***cyber*** and ***power*** network to determine the ***state*** of the ***cyber-physical*** system



(*) S. A. Zonouz, et.al., "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power-Grid Critical Infrastructures," IEEE Transactions on Smart Grid, Dec. 2012.

Both Cyber and Physical Mechanisms Should be Employed to Fix Compromise

- The consequence of a malicious attack on the power side is occasionally fixable through physical-only controls
- Example: a malicious relay opening could be reverted by closing it again
- However, the attacker may simply repeat the attack (open the relay again) if the controller(s) remains compromised

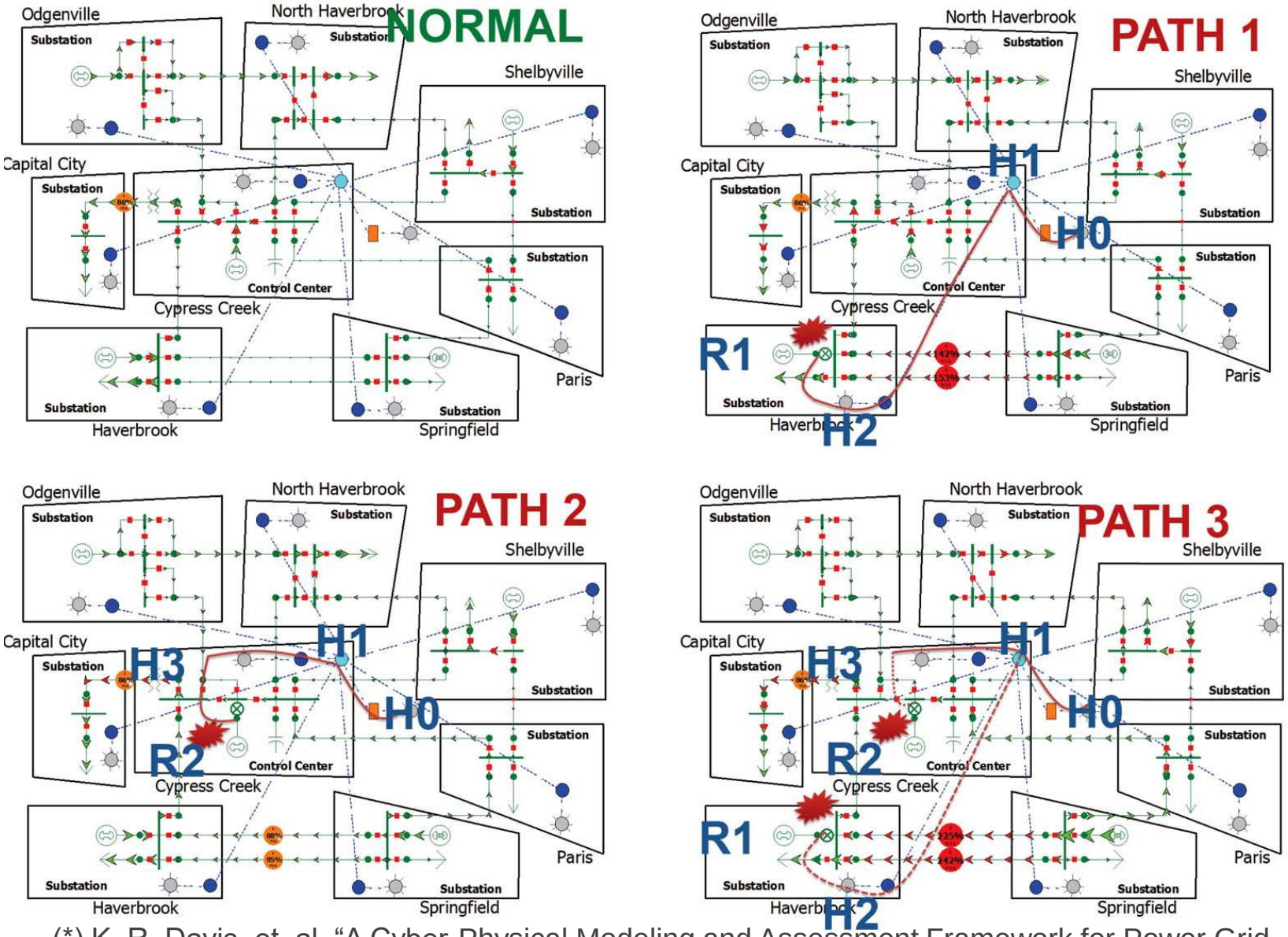
Response and Recovery Strategy

- To formulate this, you need to know

1. What is important to the system

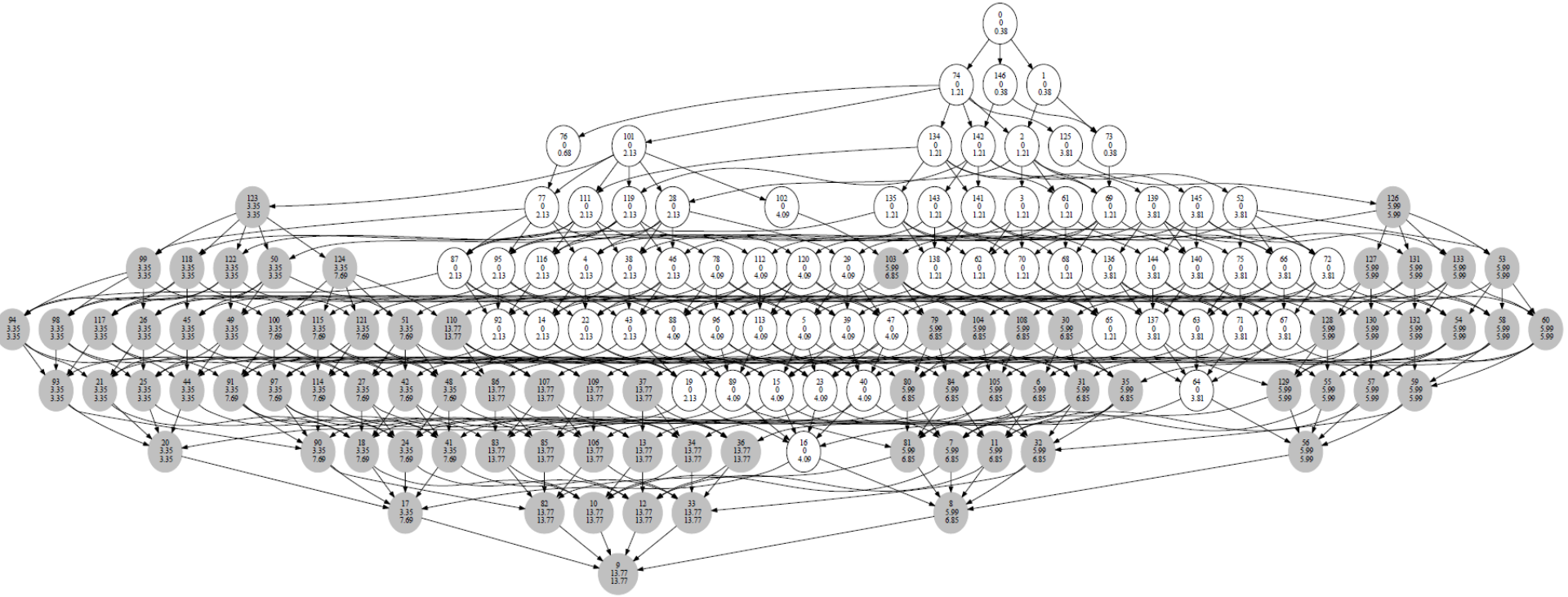
2. How to control/protect/defend what is important

In Current State, Find Worst Attack Paths



(*) K. R. Davis, et. al, “A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures,” *IEEE Transactions on in Smart Grid*, 2015.

Generating a Model



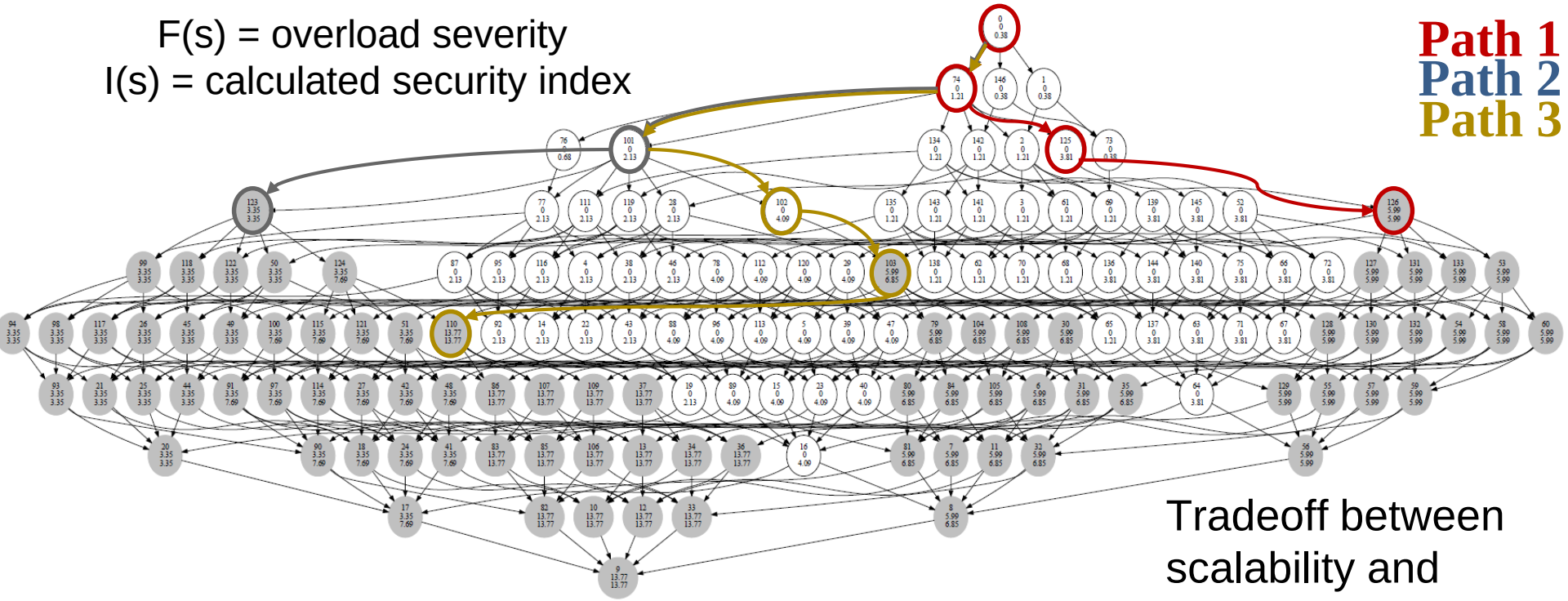
Markov Decision Process (MDP) Model:

- Each circle is a **state** (grey circles show physical impact)
- **Transitions** are based on control connections and vulnerabilities
- Each state holds a **security index value**: ease of attack + impact

Ranked Attack Path Example

State #
F(s)
I(s)

F(s) = overload severity
I(s) = calculated security index



Path 1
Path 2
Path 3

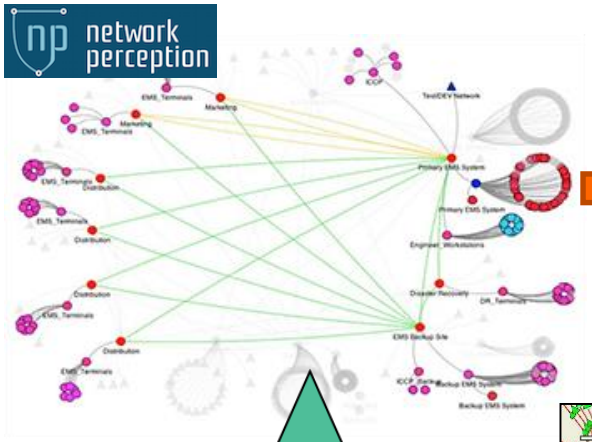
Tradeoff between scalability and accuracy

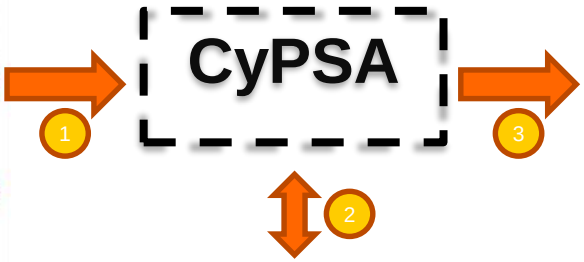
Line outage:

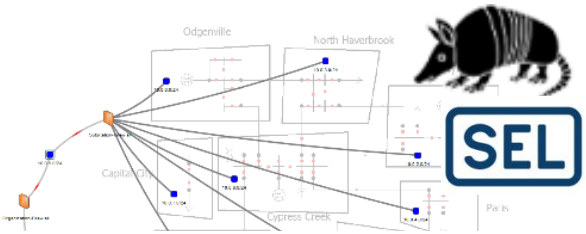
- Paths 1 and 2 are the most severe single path attacks
- Path 3 is more complex and leads to a double line outage

(*) S. Zonouz et. al, "SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures," *IEEE Trans. Smart Grid,* 2014.

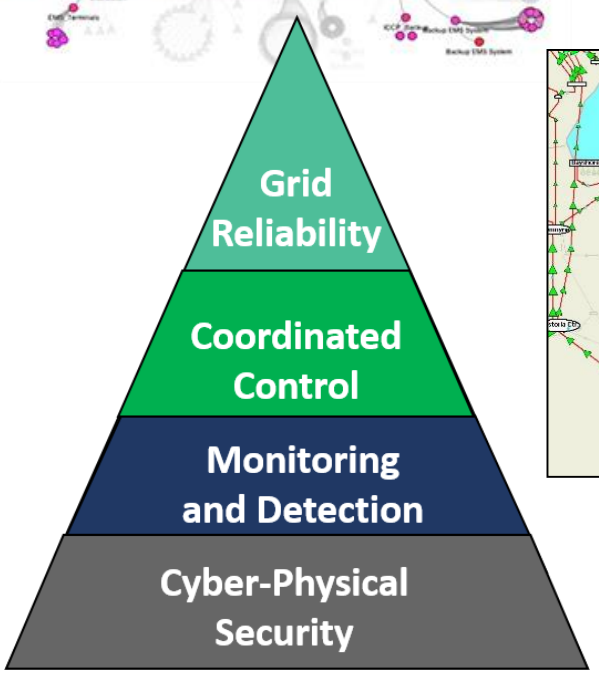
CyPSA Framework and Toolset

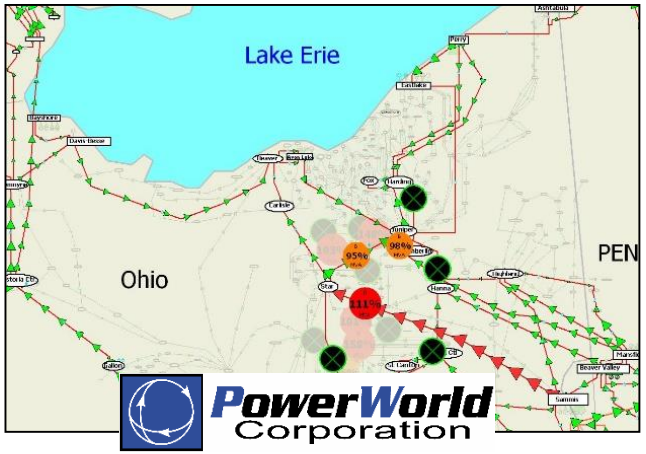






ID	Asset Name	IP Address	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776





Results identify "high-risk" cyber-attack induced outages

U.S. DEPARTMENT OF ENERGY
arpa·e

(*) K. R. Davis, et. al., "Cyber-Physical Security Assessment for Electric Power Systems," *IEEE-HKN: The Bridge*, 2016.

Attack Graph Analysis Model

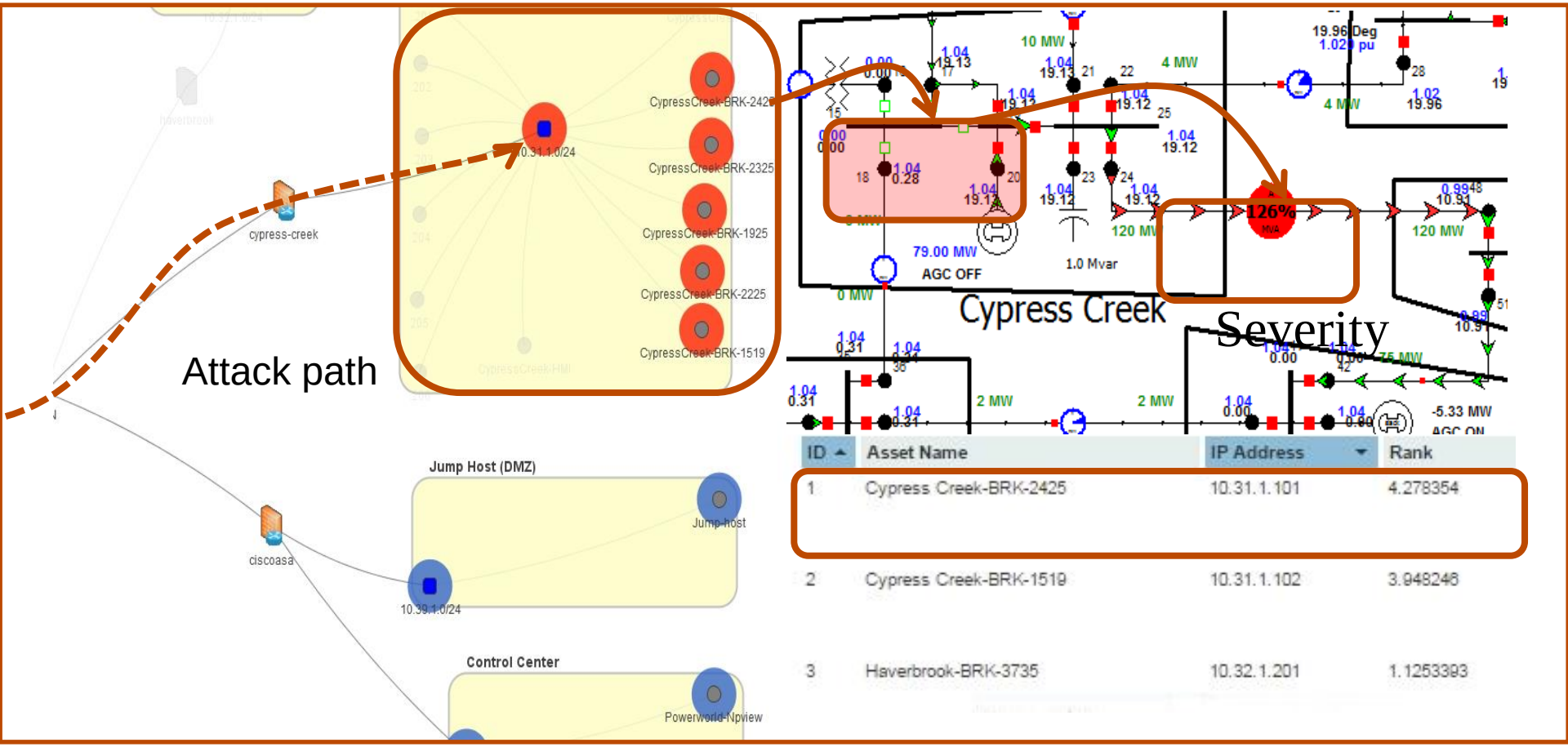
- A pathfinding approach to compute shortest paths based on depth-first-search is used in CyPSA instead of MDP
- An graph is built based on connectivity that considers only allowed ports and protocols and only attacks with physical impact
- Exploitability score assigned from National Vulnerability database

CyPSA Analyses: 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	
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

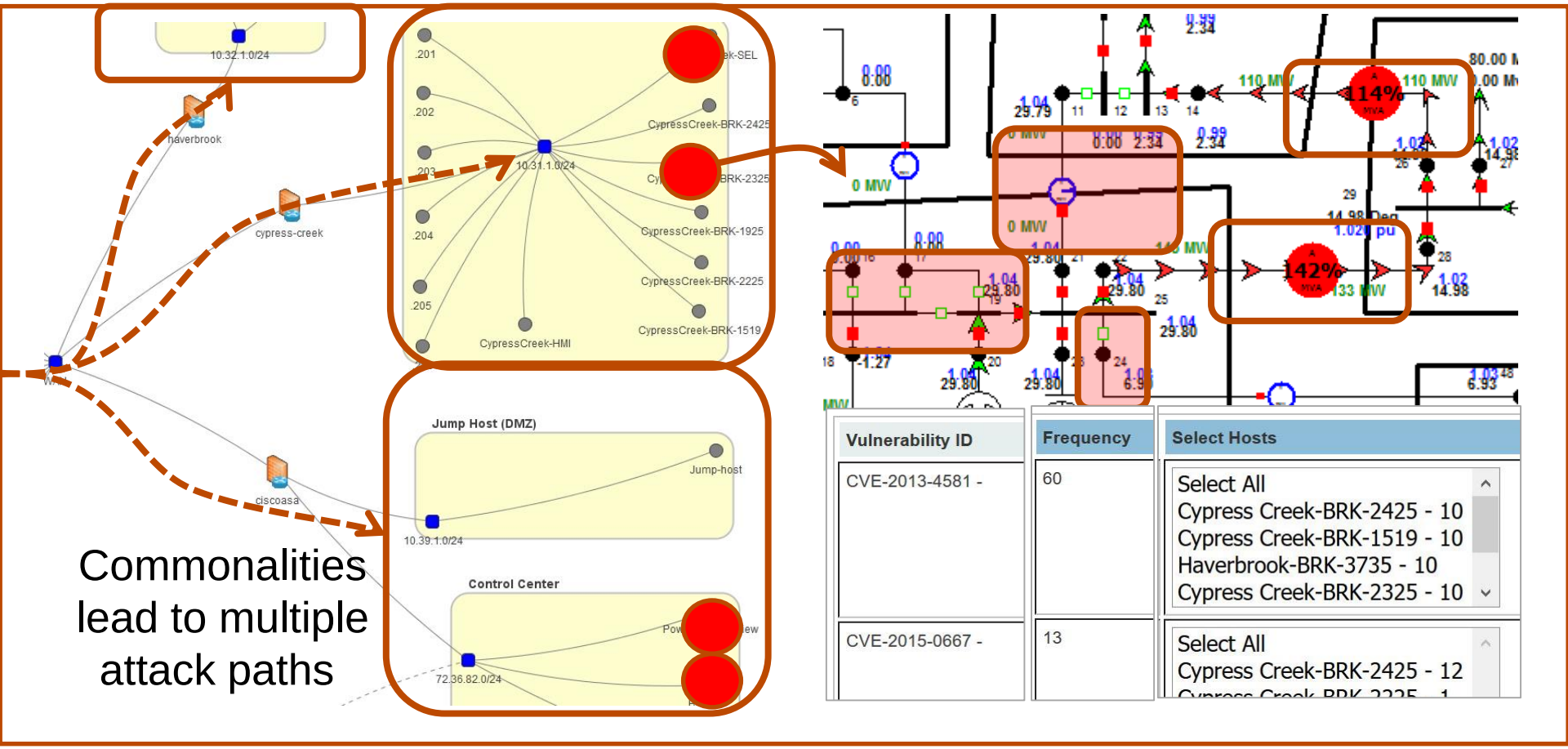
CyPSA: Asset Ranking

How to Prioritize Defenses



Assets and paths are ranked using (1) physical topology and impact and (2) cyber connectivity and vulnerabilities.

CyPSA: Aggregate Exposure of Device Groups

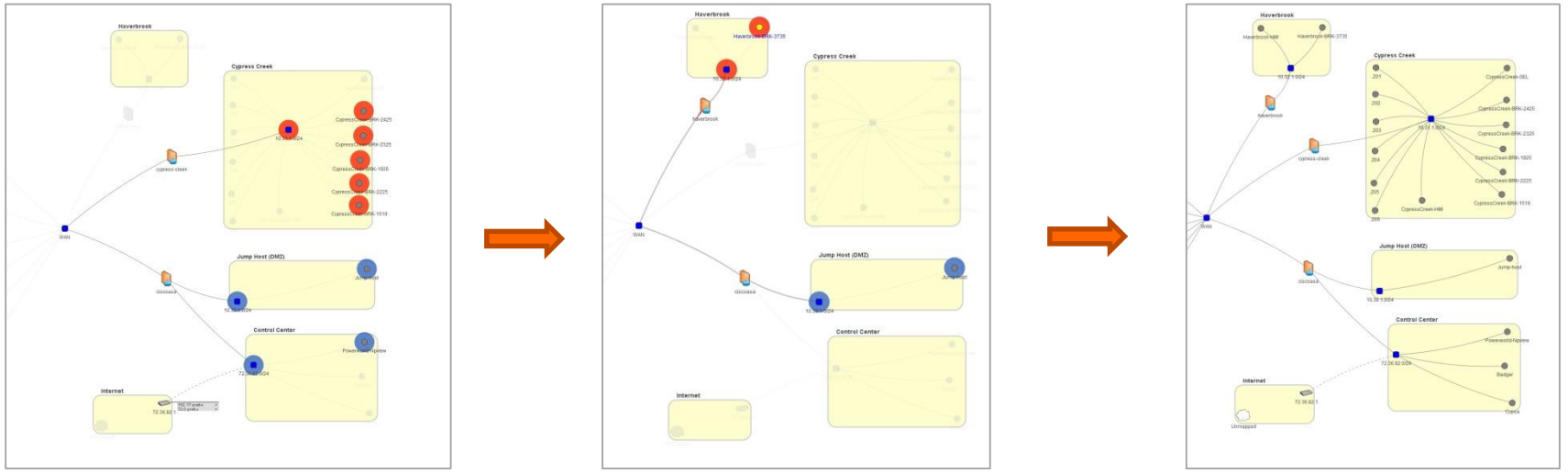


CyPSA Analyses: Patch Planning

Description	Select hosts or vulnerabilities to patch and re-compute attack path rankings.

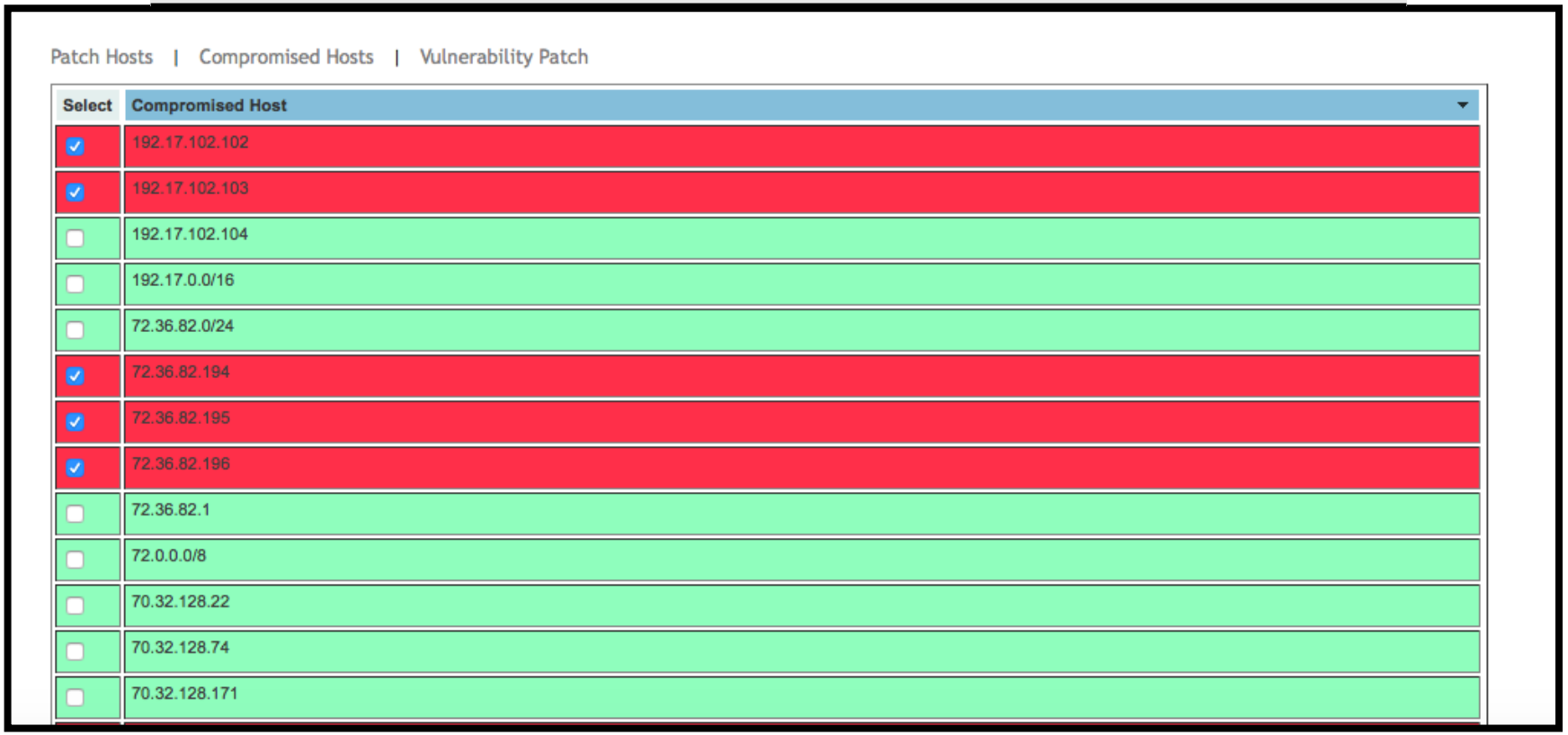
Patch Hosts | Compromised Hosts | Vulnerability Patch

Select	Patch Host	CVE-ID's
☑	10.32.1.201	CVE-2013-4581, CVE-2015-0984, CVE-2014-8517
☐	10.31.1.105	CVE-2013-4581, CVE-2015-2157, CVE-2015-0667
☑	10.31.1.101	CVE-2013-4581, CVE-2015-0667
☑	10.31.1.104	CVE-2013-4581, CVE-2014-7299
☐	10.31.1.102	CVE-2013-4581, CVE-2014-3348
☑	10.31.1.103	CVE-2013-4581, CVE-2014-2198, CVE-2014-3563



CyPSA: Cyber Incident Planning

Description	Devices are marked as compromised and asset rankings are re-computed.



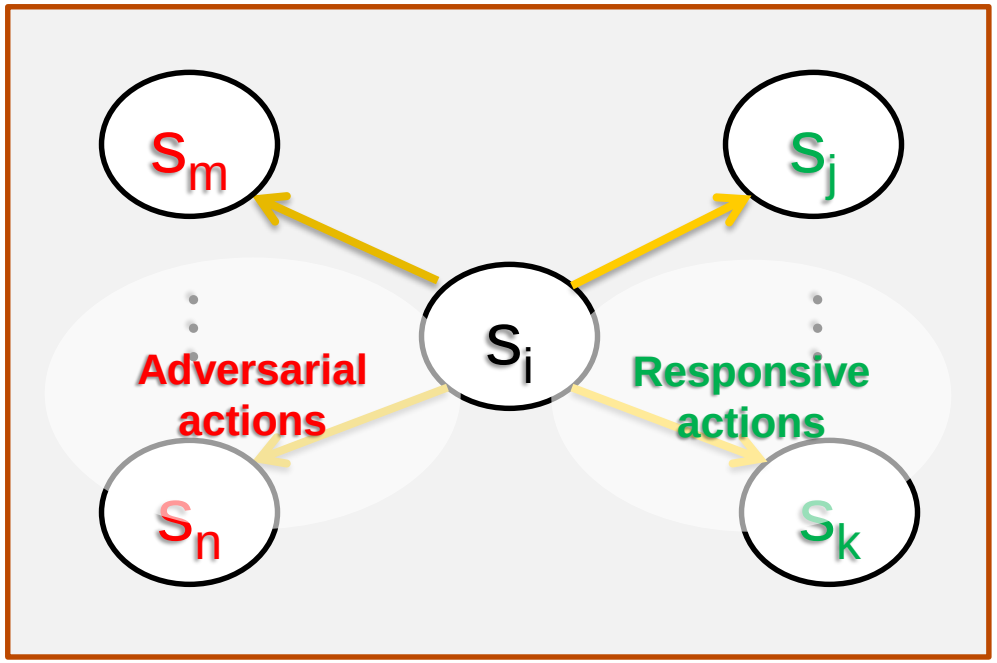
CyPSA Analyses

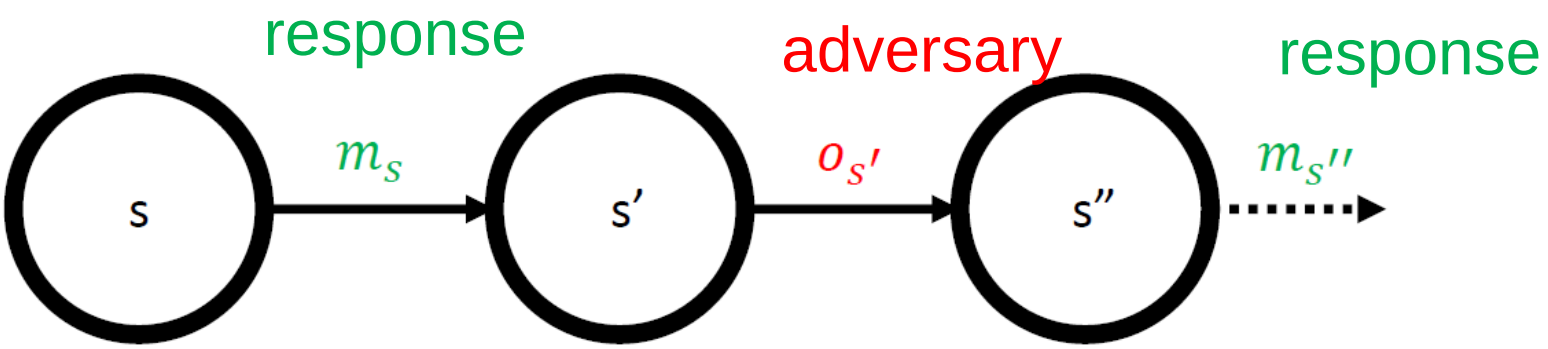
Analysis Name	Description
Asset Ranking	Get all attack paths for a given set of assets. Prioritize assets and paths based on cyber and physical metrics.
Aggregate Exposure	Rank attack paths in terms of common vulnerabilities and their physical impact.
Patching	Select hosts or vulnerabilities to patch and re-compute attack path rankings.
Cyber Incident Planning	Compute attack path rankings given a set of compromised devices.

- CyPSA can be optimized to tell us where to fix the system to reduce damage.
- However, fixing known holes is only a small part of a complete response strategy.

Adversary vs. Response Engine

Response engine takes the action which ***minimizes the maximum damage*** by the attacker later





(*) S. A. Zonouz, et. al., "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," *IEEE /IFIP International Conference on Dependable Systems and Networks*, 2009.

Control Theoretic Security Modeling

- Framework for decision making based on modeling reciprocal interactions between adversary and defender
- Competitive Markov Decision Process (CMDP) *(S, A, R, Pr, γ)*
  - *S*: security state space (set of compromised hosts)
  - *A*: set of actions (response and adversary)
  - *R(s):* measurable reward function
  - *Pr(s,a,s'):* transition probability function
  - γ: discount factor (difference between present and future rewards)

(*) Hossain et al., "Towards Cyber-Physical Intrusion Tolerance," *SmartGridComm, 2015* (Top-3 Student).

Modeling Intrusion Response

- In this model (*S*, *A*, *R*, *Pr*, *γ)*, how do we determine what to use for *A*?

A: set of actions (response and adversary)

- Response action set is affected by:
  - 1. Degree of redundancy
  - 2. Built-in topological flexibility

Cyber-based Response Actions

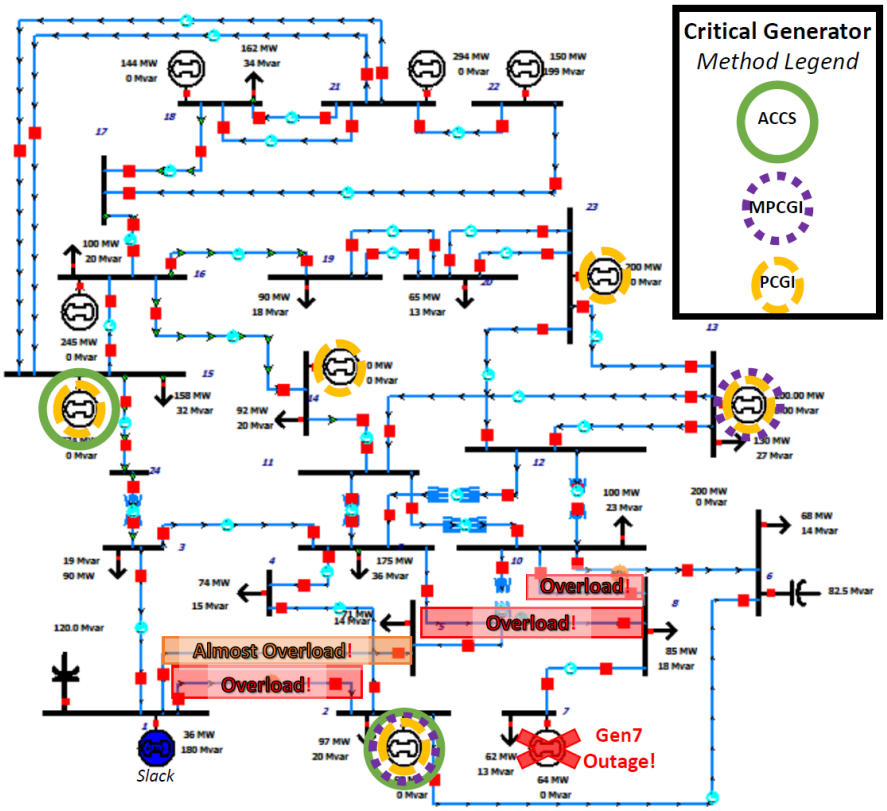
- Discrete sequential logic
- Computing platforms

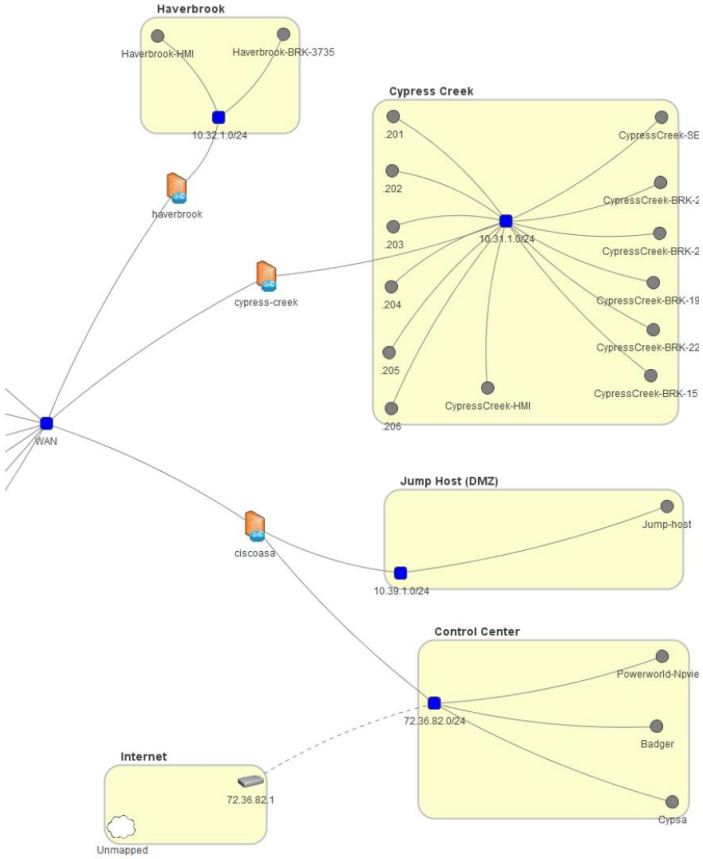
- Examples:
  - A firewall is reconfigured to prevent upcoming attack
  - Block access attempts to a particular resource or file
  - Restore previous known good state

Response Strategies

- Suppose an attack results in physical damage
  - Reliably and securely apply different components
- It may not be possible to remove the attack and restore the cyber system
  - Endure while protecting critical functions

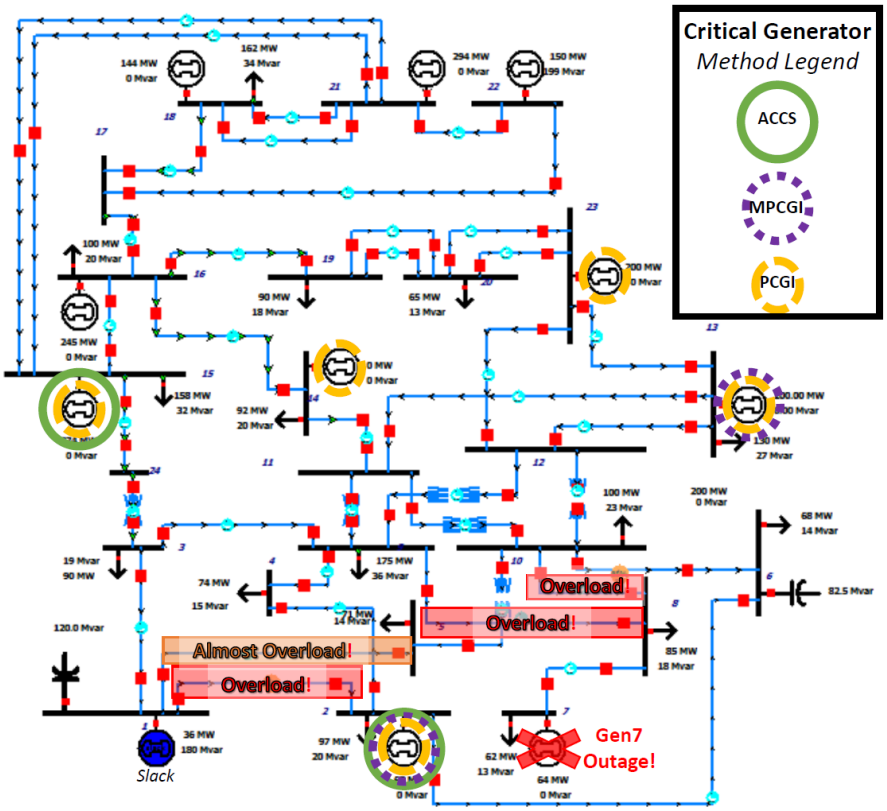
Attack Analysis in IEEE 24-Bus System

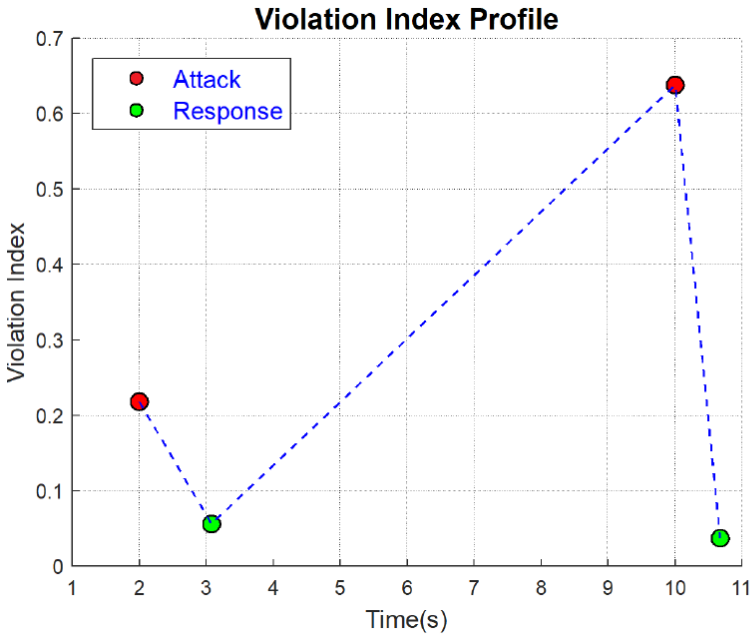




(*) S. Hossain-McKenzie, et.al., “Analytic Corrective Control Selection for Online Remedial Action Scheme Design in a Cyber Adversarial Environment,” *IET Cyber-Physical Systems,* 2017.

Attack Analysis in IEEE 24-Bus System



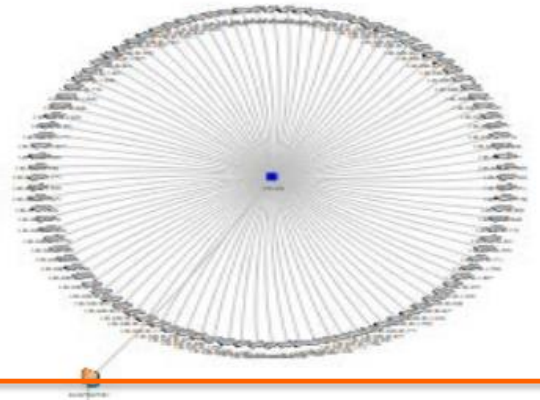


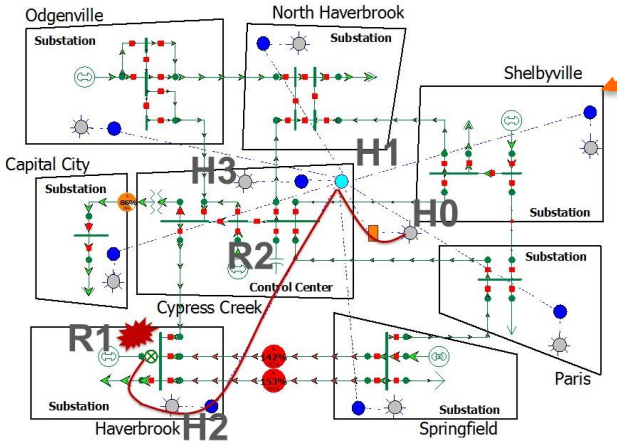
ns

Compromised IP Address	IP Address Location	Num. Paths	Path Cost	C_{EQ} (5)
10.31.1.201	Cypress Creek	5	7.952	1.5904
10.32.1.250	Haverbrook	1	6.832	6.832
10.39.1.22	DMZ	6	8.5888	1.4315
72.36.82.194	Control center	6	17.1776	2.8629

Distributed Actuation Requirements

Device Level Reach +
CyPSA + Verification
+ Online Remedial Action
Scheme (RAS) Design





Ask How To Get Involved!

We've held two utility workshops on this topic since August.

4 years and $1.5M later, we found that device (i.e., relay) interconnection data is an enabling first step.

Discussion

- Closing the loop: cyber decision space, nonlinear controllability analysis, and stability assessment

- Goal is to optimize cyber-physical controls together at scale for online intrusion tolerance and response (i.e., resilience)

- Accurate cyber-physical maps and models are a key enabling step

Final Thoughts

"Building a strategy to increase system resilience

requires an understanding of a wide range of preparatory, preventative, and remedial actions,

as well as how these impact planning, operation, and restoration

over the entire life cycle of different kinds of grid failures."

The National Academies Consensus Study Report on "Enhancing the Resilience of the Nation's Electricity System," July 2017.

Questions?

Kate Davis

(katedavis@tamu.edu)