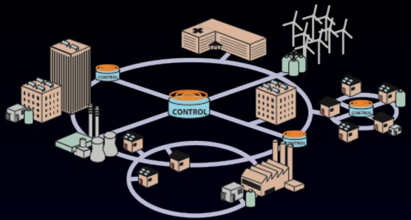


Cyber-Physical Security and the Smart Grid

Deepa Kundur
Professor
Electrical & Computer Engineering
University of Toronto

Cyber-Physical Security =

Cyber Security + Physical System Security

Distributed Signal Processing =

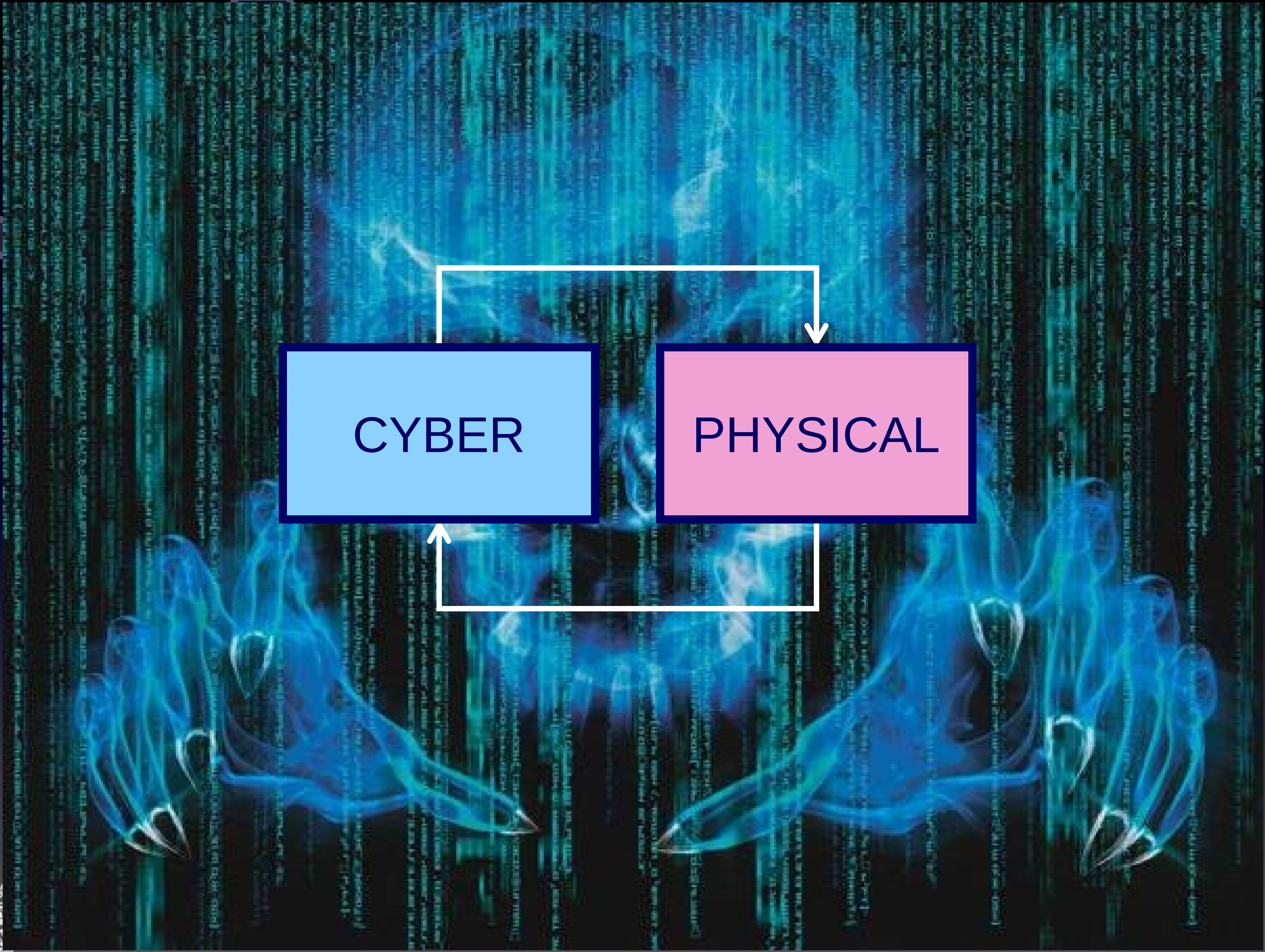
Distributed Computing +

Signal Processing

Objectives of Talk

1. To give an appreciation of the motivations for cyber-physical security;
2. To give insight on the novel challenges in cyber-physical system security;
3. To consider two case studies of cyber-physical security problems to elucidate cyber and physical modeling and analysis.

STOP
CYBER ATTACKS AHEAD
RU5ErkJggg==")base64,iVBORw0KGg
P0C1V9QD4NEOxs9xBQHQVCwSJFV
4hwVYBldLn9vkLp79QcBCTDMiy3w2g
IQtfMBSO DANGER Uz4BDMled
0MledhqOu/AzVSmzlUJKUz4BDMledh
u/AzVSmzZ49CUjCC0yvim98iqtJT2L2
MQx8Q7hQYFek4Akjx
1zoL6QlxGjtd6lrahiqCi
password
PASSWORD
HACKER
ETECTED!!
EACH



CYBER

PHYSICAL

Instrumentation

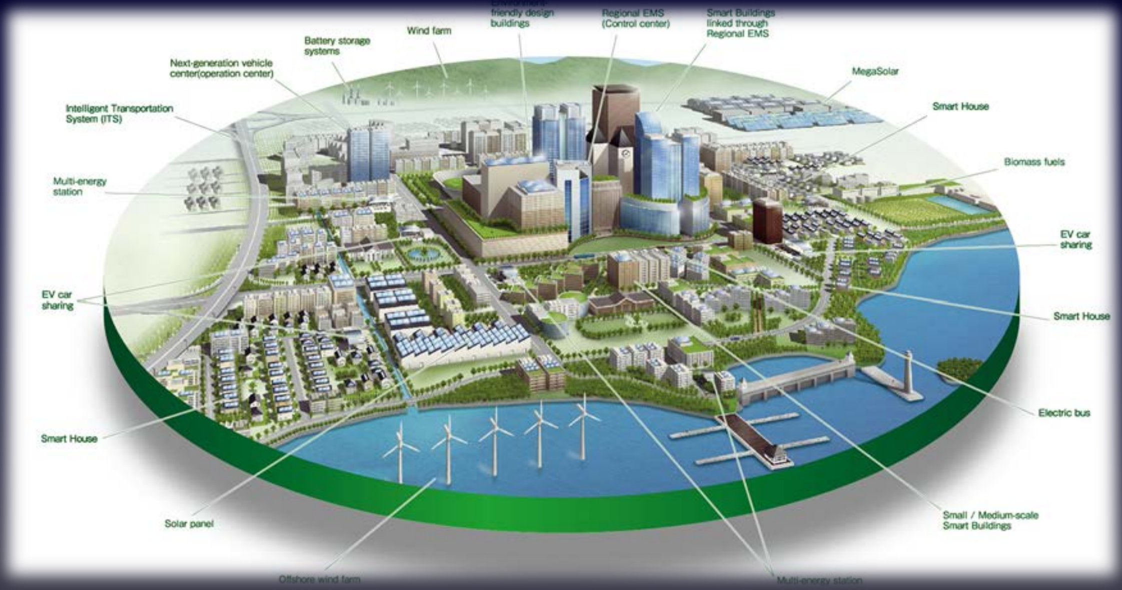
Interconnectedness

Intelligence

Instrumentation
Interconnectedness
Intelligence

Smart city

Uses information and communication technologies (ICT) to enhance quality and performance of urban services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens.

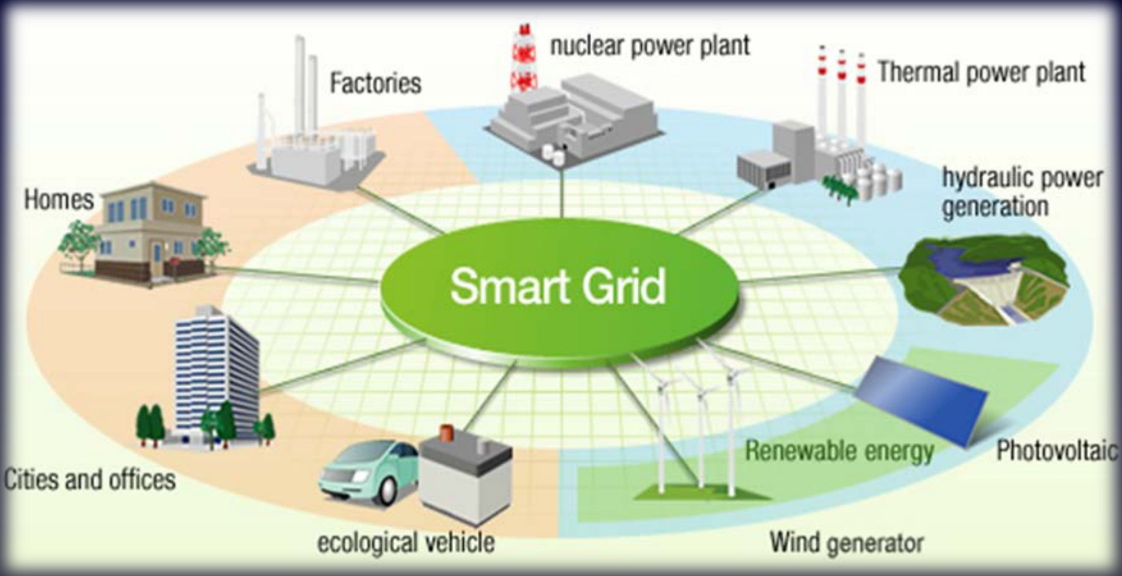

Environment-friendly design buildings
Regional EMS (Control center)
Smart Buildings linked through Regional EMS
Wind farm
Battery storage systems
Next-generation vehicle center(operation center)
MegaSolar
Intelligent Transportation System (ITS)
Smart House
Biomass fuels
Multi-energy station
EV car sharing
EV car sharing
Smart House
EV car sharing
Electric bus
Smart House
Small / Medium-scale Smart Buildings
Solar panel
Offshore wind farm
Multi-energy station

Instrumentation

Interconnectedness

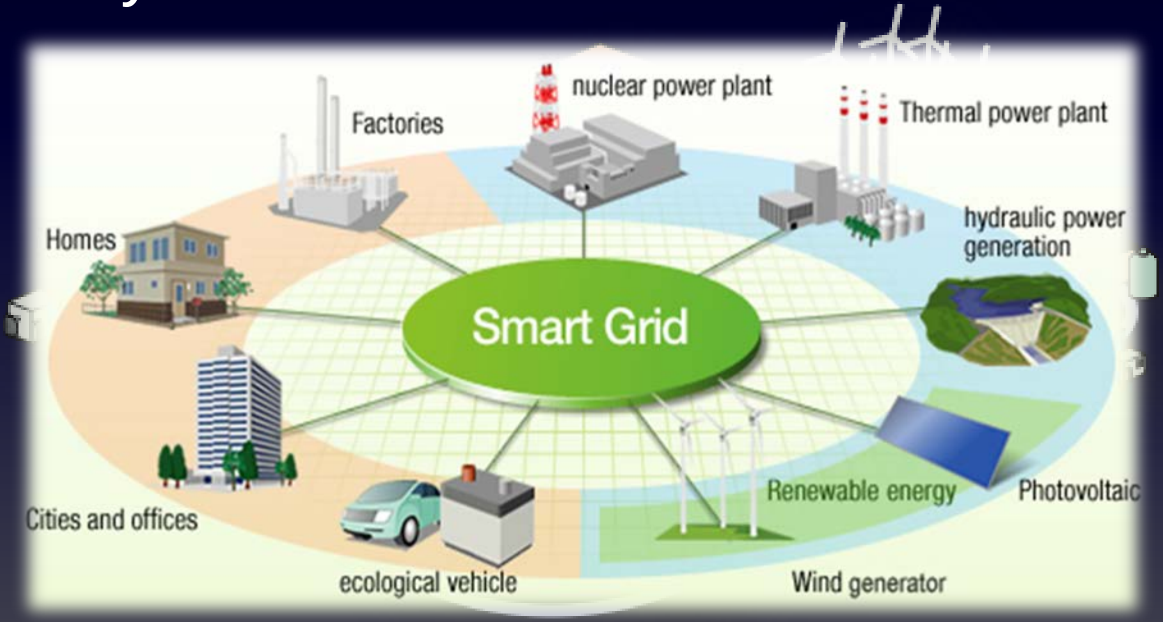
Intelligence

Smart grid



A Smarter Grid

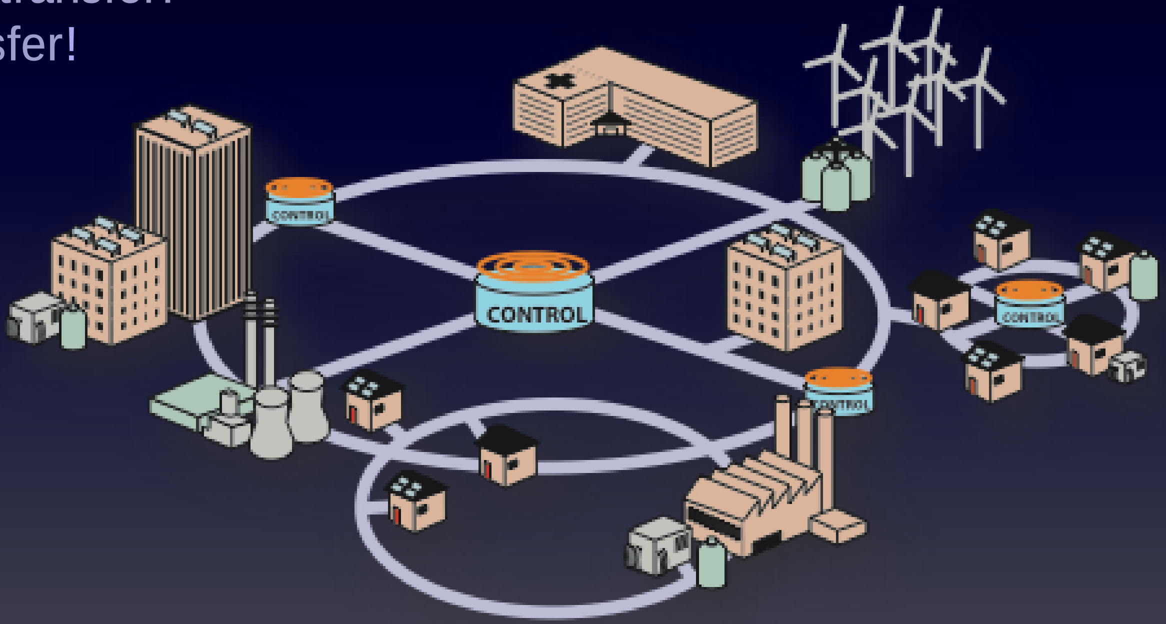
- Greater
  - Consumer-centricity
  - Reliability
  - Efficiency
  - Economics
  - Sustainability



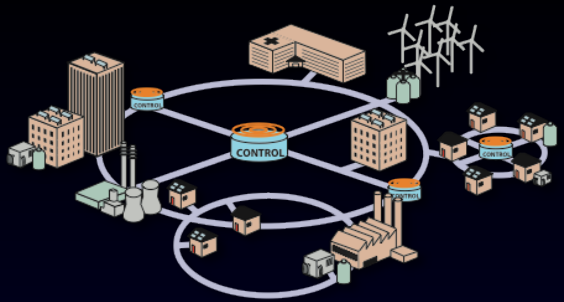
A Smarter Grid

MARRIAGE OF INFORMATION TECHNOLOGY WITH THE EXISTING ELECTRICITY NETWORK

Bidirectional information transfer!
Bidirectional energy transfer!



A Smart Grid



- North American Reliability Corporation (NERC) definition:
  - “the integration of real-time monitoring, advanced sensing, and communications, utilizing analytics and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure and reliable electric power system, from generation source to end-user”

Smart Grid Vision

"… facilitate distributed generation, interoperability, security, accessibility, liberalized market, reduced environmental impact, consumer engagement."
--European Union

"…open but secure system architecture, communications and standards to provide value and choice to consumers." --GridWise™

"… convergence of greater consumer choice and rapid advances in communications, computing and electronic industries." --IntelliGrid℠

"integration of real-time monitoring, advanced sensing, and communications… to accommodate existing and new forms of supply, delivery, and use … from generation source to end-user." --North American Electric Reliability Council

"…family of control systems and asset-management tools empowered by sensors, communication pathways and information tools … that's smarter for all of us." --General Electric

"Participatory network … comprising intelligent network-connected devices, distributed generation and consumer energy management tools." --IBM

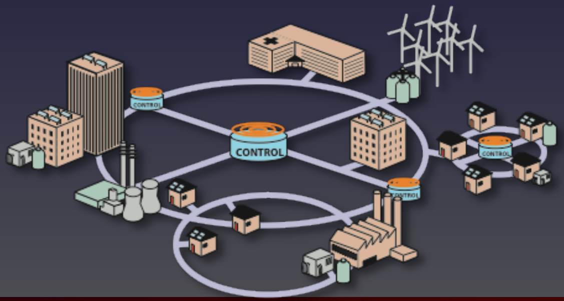
"... utilities, vendors, consumers, researchers and other stakeholders form partnerships and overcome barriers."
--US Dept of Energy/NETL

Open and Consumer-centric

- Requires information about the right thing to the right party/device at the right time

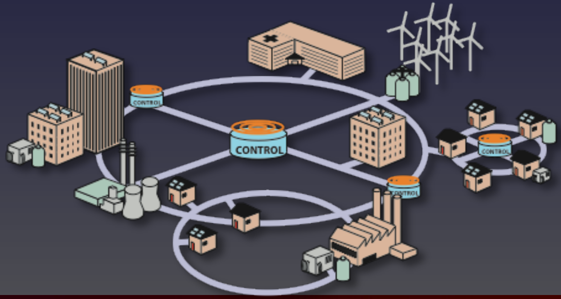
  - sensing
  - communication
  - computation
  - control

→ cyber-enablement



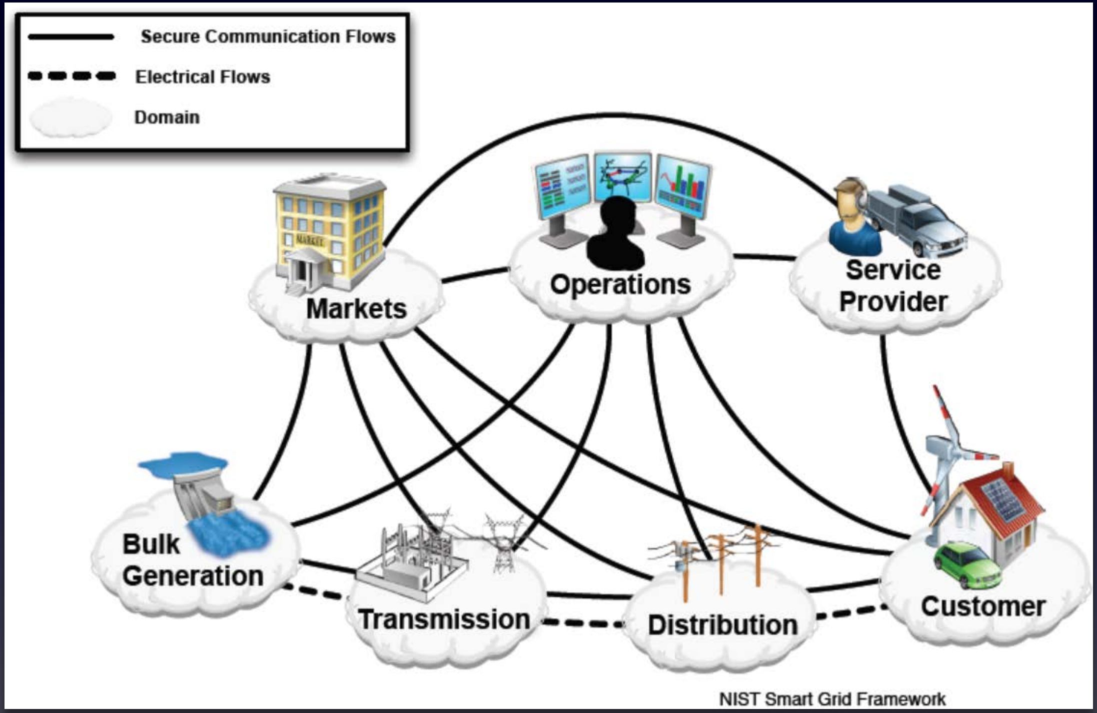
Open and Consumer-centric

- Requires distributed data acquisition, communications and computing
- Networked cyber and physical components communicate and coordinate to achieve a common goal
- To improve efficiency and performance

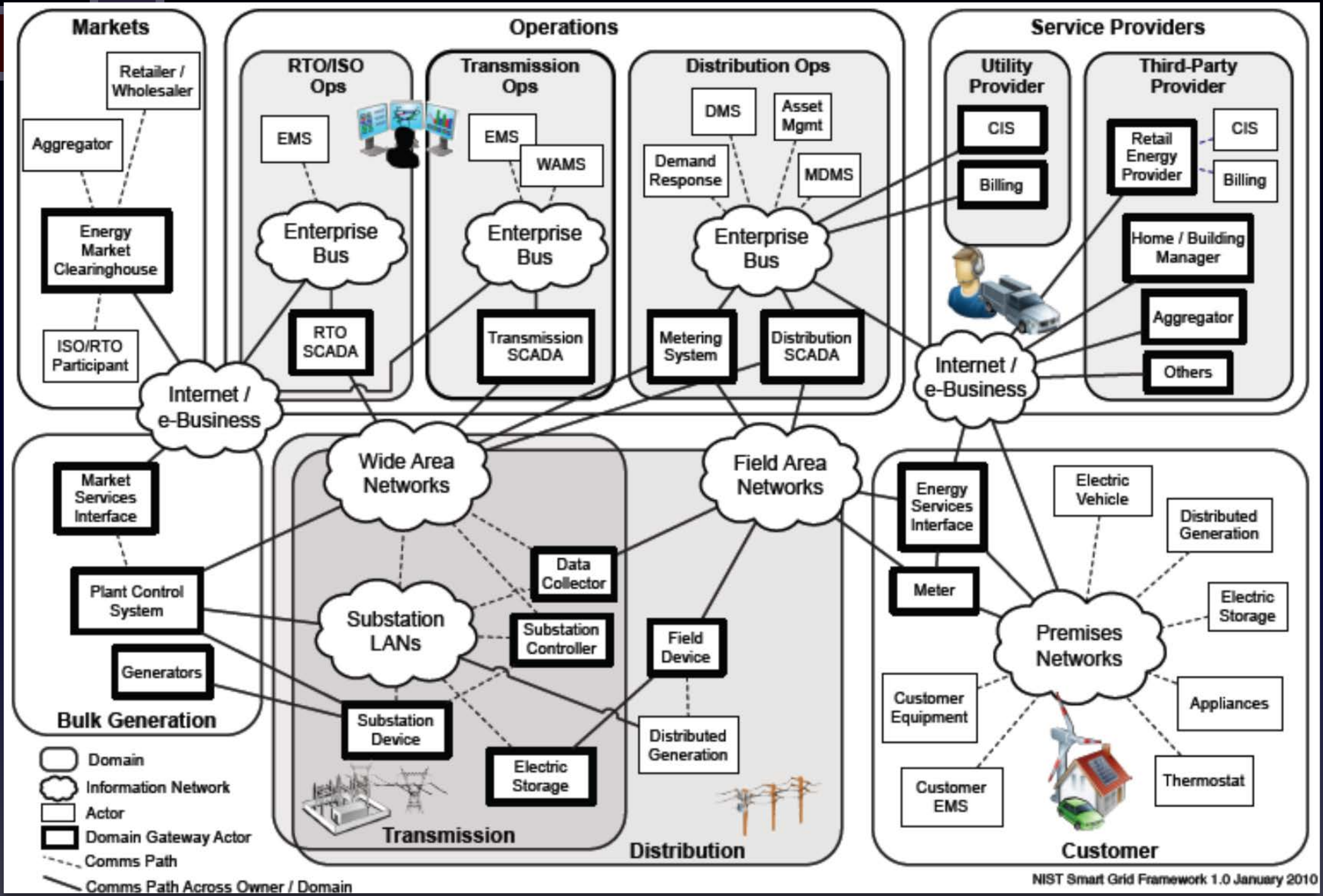


Information, Financial and Physical Transactions

- Advanced metering, home automation
- Billing, real-time pricing
- Wide area monitoring and SCADA



NIST Smart Grid Framework 2.0



NIST Smart Grid Framework 2.0

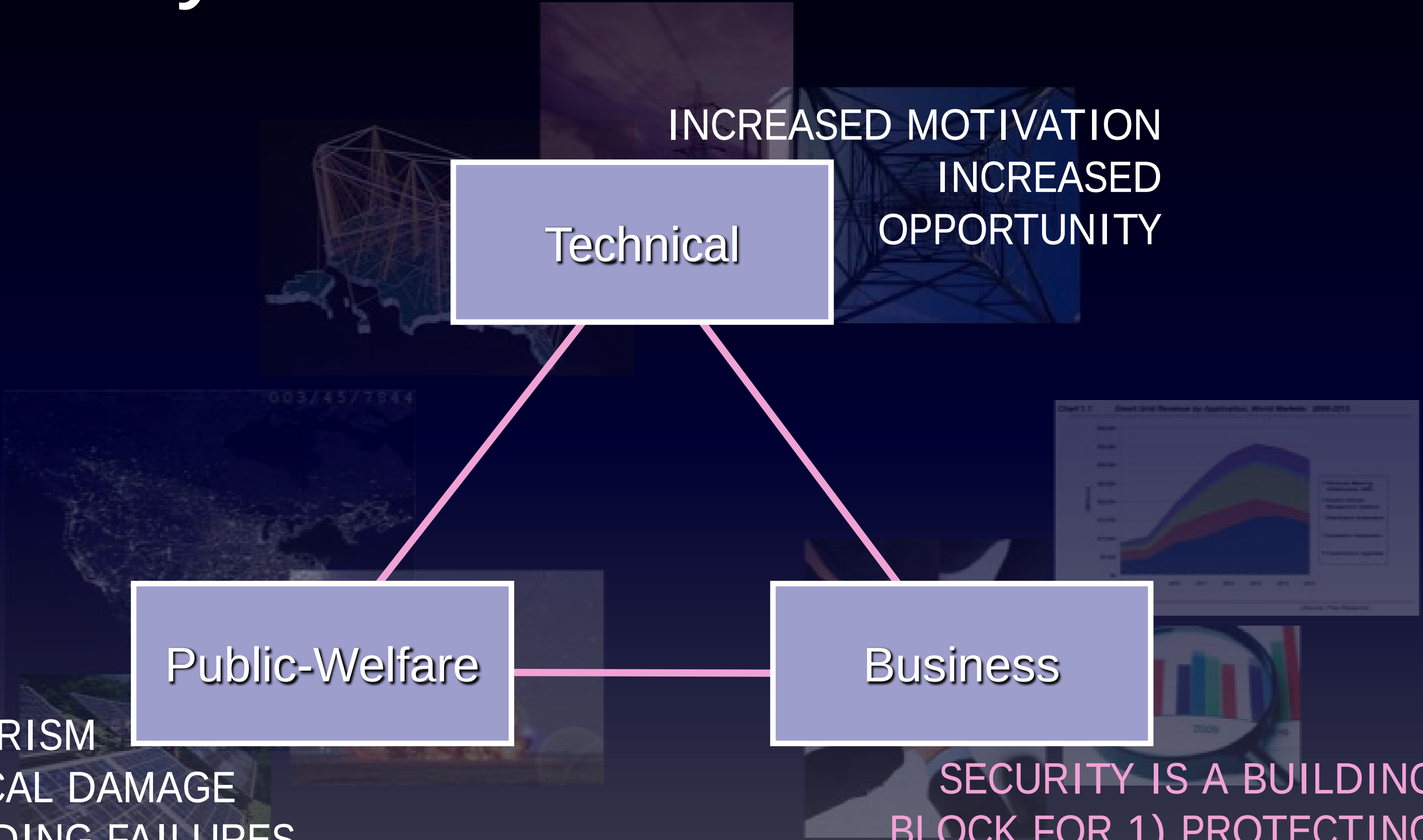
Distributed Transactions

- Wide Area Monitoring
  - to improve overall reliability through situational awareness and advanced decision-making and control
- Supervisory Control and Data Acquisition
  - to enable state estimation and local control by leveraging intelligent electronic devices (IEDs) and human-assisted control

Distributed Transactions

- Substation Integration and Automation
  - to remotely monitor and control substation that interfaces transmission and distribution systems
- Advanced Metering
  - to enable consumer-centricity by enabling higher granularity and two-way information flow between utility and customer

Why Protect the Grid?



INCREASED MOTIVATION
INCREASED
OPPORTUNITY

TERRORISM
PHYSICAL DAMAGE
CASCADING FAILURES

SECURITY IS A BUILDING BLOCK FOR 1) PROTECTING BUSINESS VALUE; 2) DRIVING DIGITAL AGILITY; 3) ENABLING INNOVATION AND GROWTH

Current Cyber Security Landscape

- 76% of Energy Utilities Breached in Past Year (DarkReading 2016)
- Energy is the 2nd most targeted industrial sector after manufacturing (DHS Reports, 2015)
- Security of Industrial Automation (Stanford, 2016)
  - Increased attack surface
  - Diversity of threats
  - Differentiated protection and response

Current Cyber Security Landscape

- Polymorphic
  - Changes appearance
  - Constantly mutates to avoid pattern recognition
  - Typically bundled with Trojans/other malware; hidden in encrypted payloads
- High Degree of Investment
  - Time, money ==> patience and capability
  - No security through obscurity

Bodies Influencing Smart Grid Development

- Federal (National Energy Board, Natural Resources Canada, FERC, DoE, DHS, NIST)
- Provincial/State (OEB)
- NERC

NERC

North American Electric Reliability Council (NERC)

- nonprofit corporation originally established by the EPU industry to promote reliability
- for decades NERC provided guidelines for power system operation which were called policies.

NERC

North American Electric Reliability Corporation (NERC)

- the 2003 Northeast blackout instigated the Energy Policy Act of 2005 and established NERC as an Electric Reliability Organization
  - requiring that NERC policies be converted to standards
  - giving NERC the power to enforce these standards with fines of up to $1,000,000 per day for noncompliance

NERC CIPs

- NERC CIPs = NERC Critical Infrastructure Protection Standards
- officially called NERC 1300
- used to secure bulk electric systems
- focus on both network security administration as well as supporting best practice industrial processes

NERC CIPs

- comprised of eight primary standards classified as:
  1. electronic security
  2. physical and personal security

- NERC CIPs are:
  - CIP-002 – Critical cyber asset identification
  - CIP-003 – Security management controls
  - CIP-004 – Personnel and training
  - CIP-005 – Electronic security protection
  - CIP-006 – Physical security of critical cyber assets
  - CIP-007 – System security management
  - CIP-008 – Incident reporting and response planning
  - CIP-009 – Disaster recovery

Compliance vs. Security

Is compliance equivalent to security?

Compliance vs. Security

- No.
  - Demonstrates organization’s adherence to documented requirements within an arbitrary time frame such as an annual audit.
  - Are generally vague and are not updated frequently enough to keep with the constantly changing information security threat landscape.
  - Many organizations treat compliance as an after-thought until the months leading up to an audit.

Compliance vs. Security

- There are great opportunities for research that takes a systematic view of smart grid protection in order to provide engineering principles of general use.

- The research community can provide design insights, novel strategies and development tools to bridge the gap between compliance and true security.

What has history taught us about Security?

- Commerce IMPERSONATION
  - eCommerce has provided greater consumer- and vendor-centricity
- Entertainment PIRACY
  - Digital entertainment has enabled more flexible business models
- Friendship PRIVACY
  - Social networking has allowed us to keep in touch with geographically distant friends

Lessons Learned

- Cyber security should be part of system design.
- Cyber security is a support service that should not hinder usability
- Cyber security is a process; no system is completely secure.

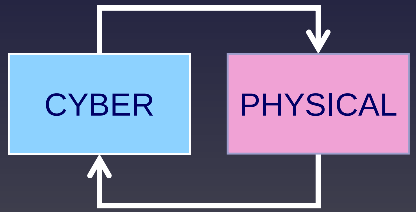
Cyber-Physical Interface

Cyber-Physical Interface

- complexity
- connectivity
- collaboration

Cyber-Physical System (CPS)

- Tight integration and coordination of the cyber and physical components



- Enables greater
  - adaptability
  - autonomy
  - efficiency
  - functionality
  - reliability
  - safety
  - usability

Cyber-Physical Security

Cyber Security

- Concerned with securing the safety of computers and computer systems in a networked environment
- C-I-A (Confidentiality, Integrity, Availability)

Power system security

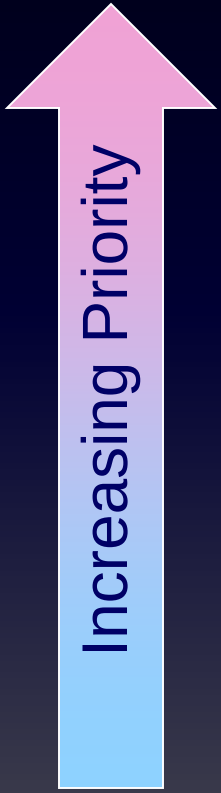
- Degree of risk in a power system’s ability to survive imminent disturbances (contingencies) without interruption to customer service
- Availability most important

Cyber-Physical Security

- Employing strategies at both the cyber system and the physical system to achieve
  - Security,
  - Reliability and
  - Resilience

  of power delivery.

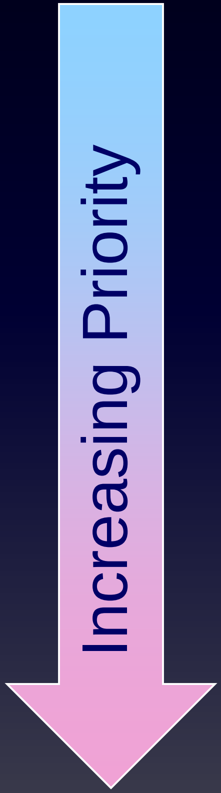
Pillars of Cyber Security



Increasing Priority

- Confidentiality
  - Assets are accessible only to authorized parties; related to security and privacy
- Integrity
  - Assets can only be modified by authorized parties and in authorized ways
- Availability
  - Assets are accessible to authorized parties

Pillars of Cyber-Physical Security



- Confidentiality
  - Assets are accessible only to authorized parties; related to security and privacy
- Integrity
  - Assets can only be modified by authorized parties and in authorized ways
- Availability
  - Assets are accessible to authorized parties

Risk

- Risk = Likelihood x Impact
- Risk = Threats x Vulnerabilities x Impact

THREATS

NATURALLY OCCURRING
UNTRAINED PERSONNEL
MALICIOUS INSIDERS
LONE ACTORS
ORGANIZED CRIME
TERRORISM
NATION-STATES

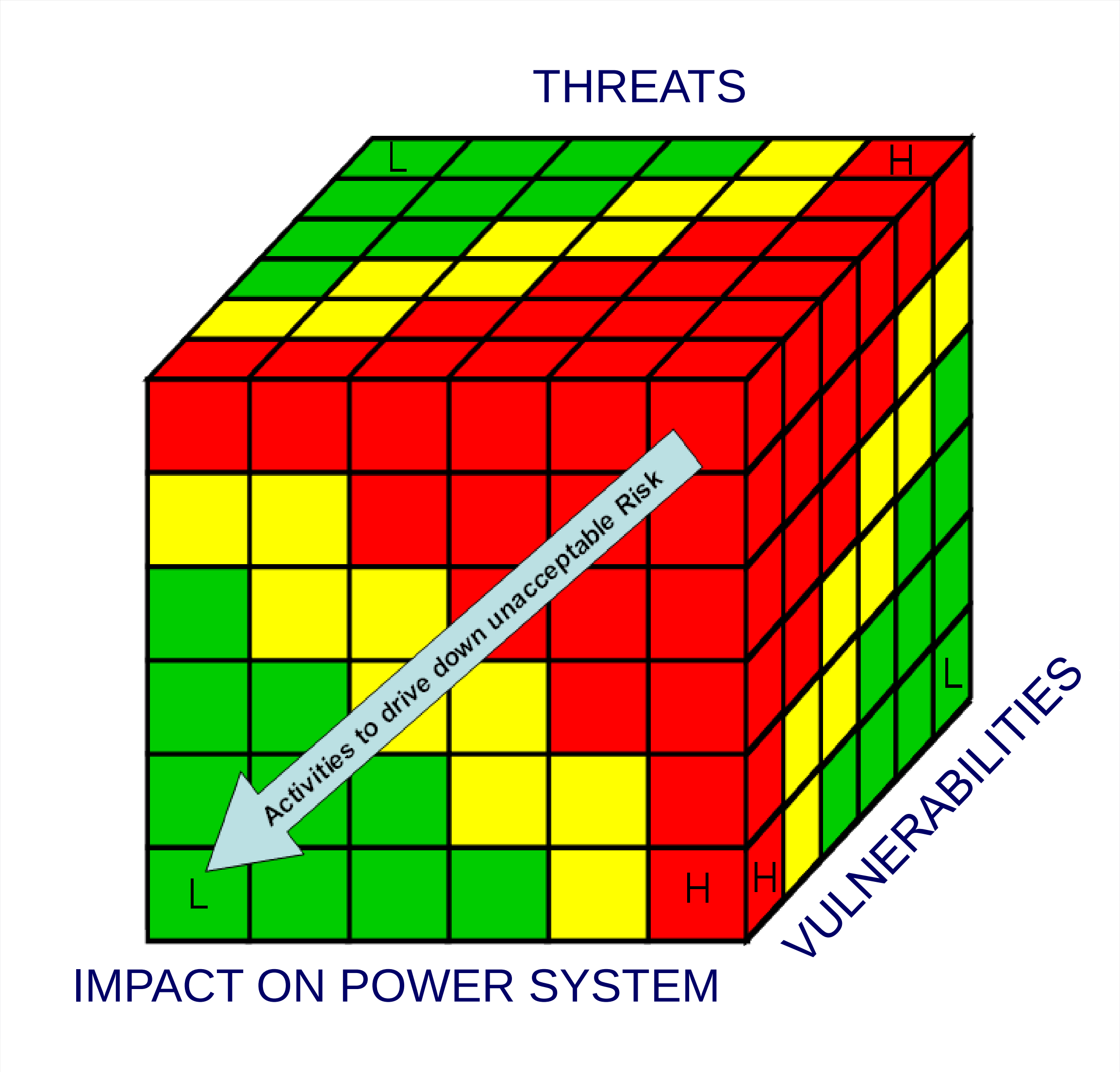
VLUNERABILITIES

COMMUNICATIONS
INTERNET
GRID COMPLEXITY
CONTROL SYSTEM COMPLEXITY
NEW SYSTEMS
NEW DEVICES

IMPACT AREAS

GENERATION SENSORS
GENERATION ACTUATORS
XMISSION SENSORS
XMISSION ACTUATORS
DISTRIB SENSORS
DISTRIB ACTUATORS
DISTRIB GNERATION
MICROGRIDS

Risk


THREATS
L
H
Activities to drive down unacceptable Risk
L
H
H
L
VULNERABILITIES
IMPACT ON POWER SYSTEM

Fundamental R&D Questions

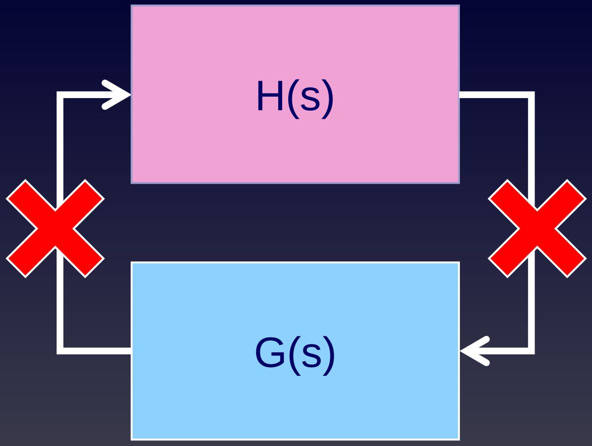
- What are the electrical system impacts of a cyber attack?
- How should security resources be prioritized for the greatest advantage?
- Is the new data/control worth the security risk?

Prior Art: Linear/Static Approaches

- Conte de Leon et al. (2002)
- McMillin et al. (2006, 2008)
- Govindarasu (2007, 2013, 2014, 2015)
- Mohsenian-Rad and Leon-Garcia (2010, 2014, 2015)

Prior Art: Resilient Control

- Cárdenas et al. (2008, 2010, 2014)
- How do you make decisions with lack of or delayed information?

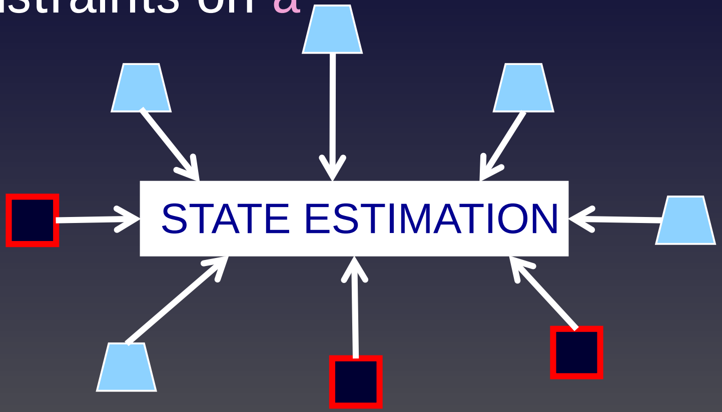


Prior Art: False Data Injection

- Liu et al. (2009, 2011), NC State
- Dán et al. (2010 – 2013, 2015), KTH
- Bobba et al. (2010, 2012, 2014), UIUC
- Kosut et al. (2010, 2011, 2015), Cornell/ASU

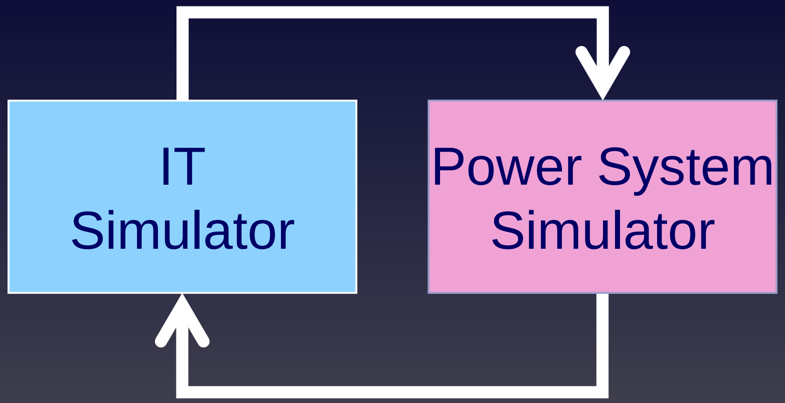
- Corruption of measurements:
  - $z_a = z + a$, for $a = Hc$ and constraints on a

- Figures of merit:
  - Likelihood of finding a
  - Impact = $||x'_a - x'||$



Co-Modeling and Simulation

- Dudenhoeffer et al. (2006)
- Shukla et al. (2010)
- Manbachi (2015)

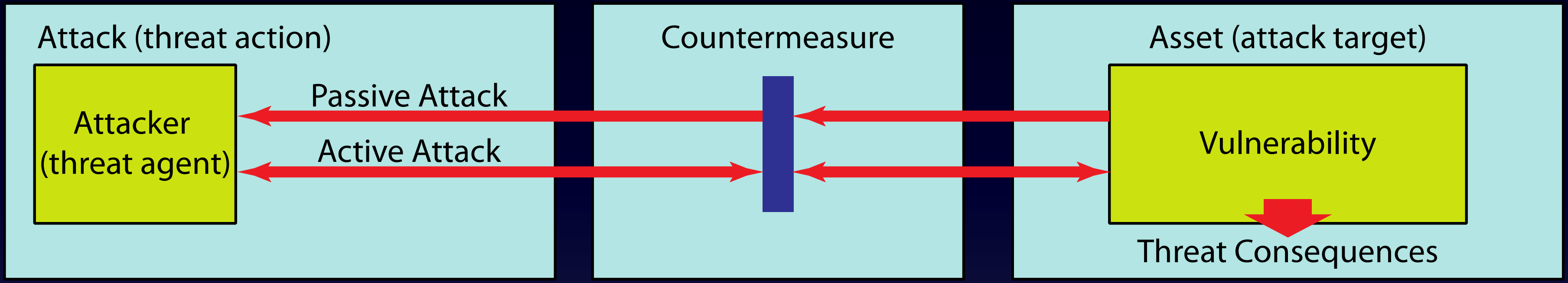


Of Interest to the EPU Community

- Attacks on information accuracy
  - False data injection attacks
- Attacks on access control
  - Reconfiguration attacks
- Attacks on timely delivery
  - Denial of information access

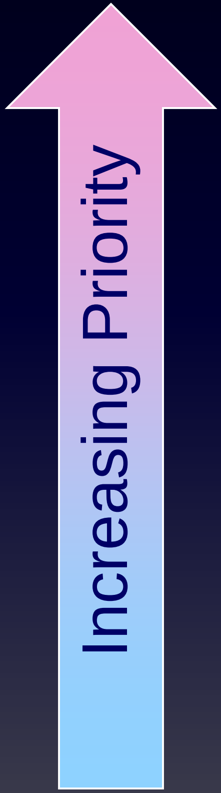
Prevention, Detection, Reaction and Resilience

Cyber Security

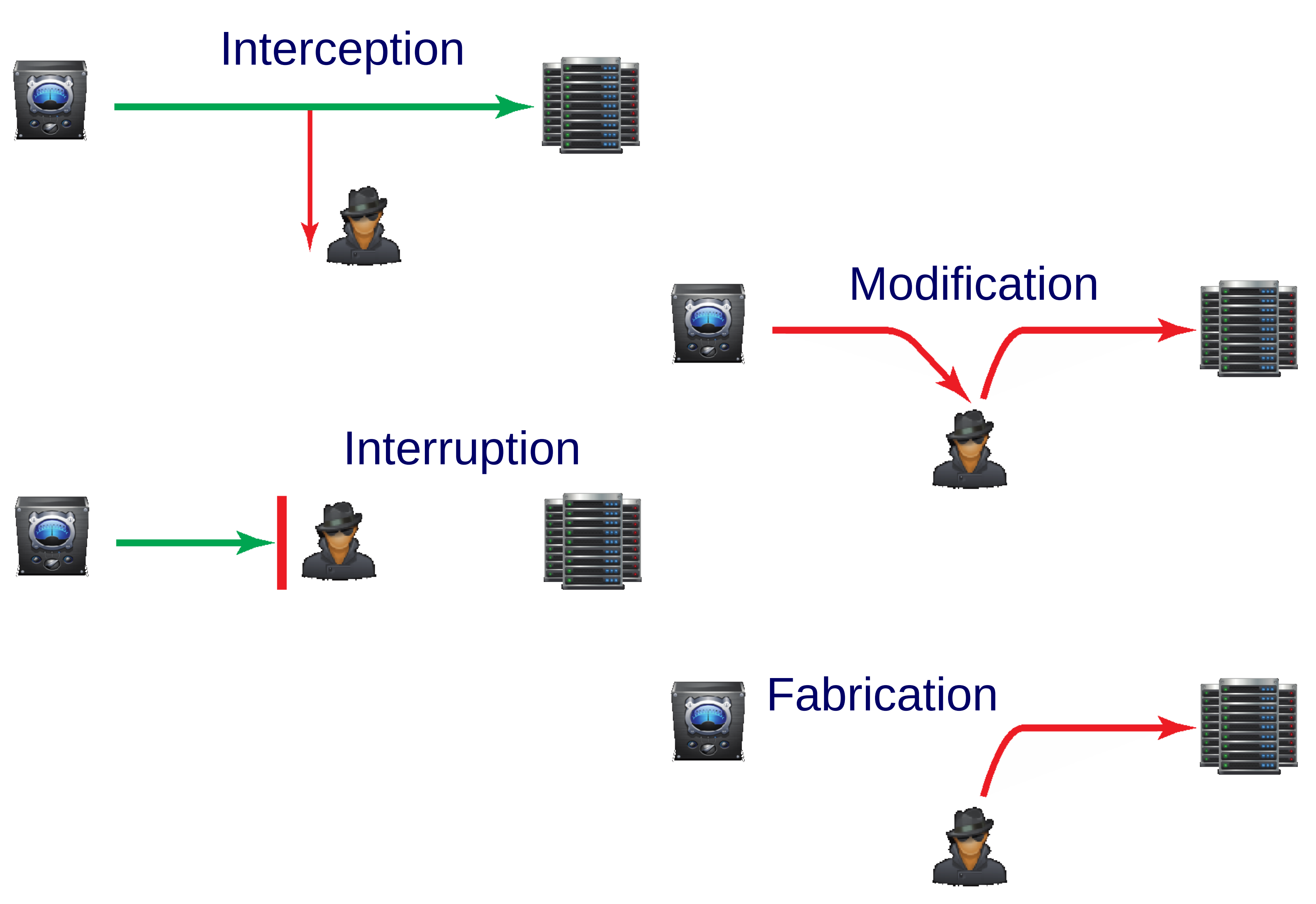


- Vulnerability
- Threat
- Attack
- Countermeasure

Pillars of Cyber Security: C-I-A



- Confidentiality
  - Assets are accessible only to authorized parties; related to security and privacy.
- Integrity
  - Assets can only be modified by authorized parties and in authorized ways.
- Availability
  - Assets are accessible to authorized parties on demand.



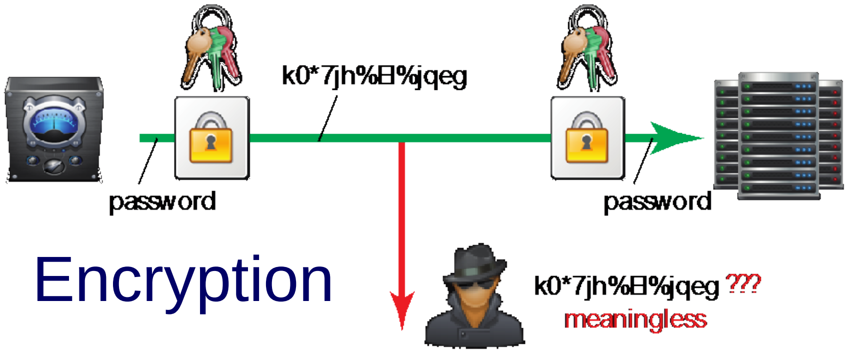
Interception

Modification

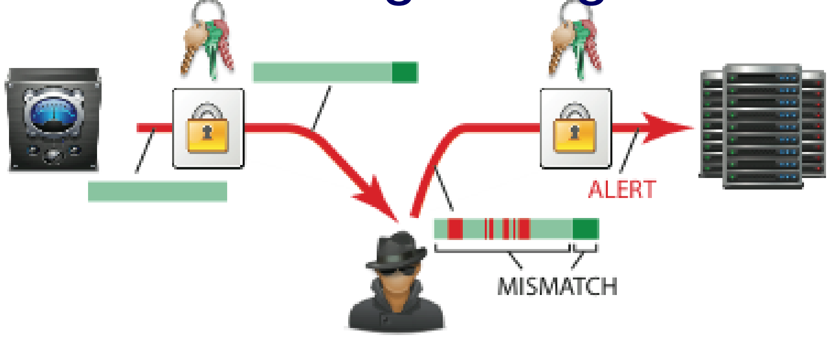
Interruption

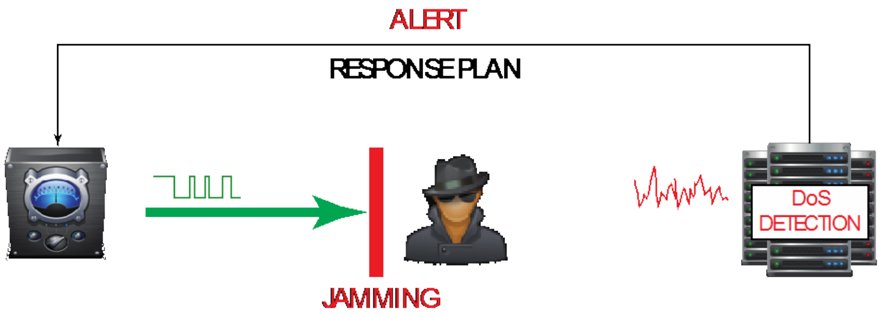
Fabrication

Encryption



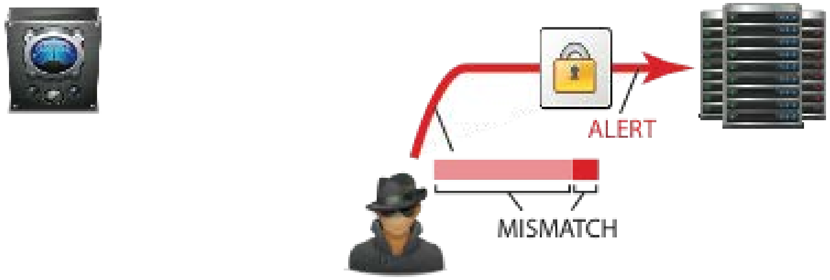
Digital Signatures





DoS Response

Authentication

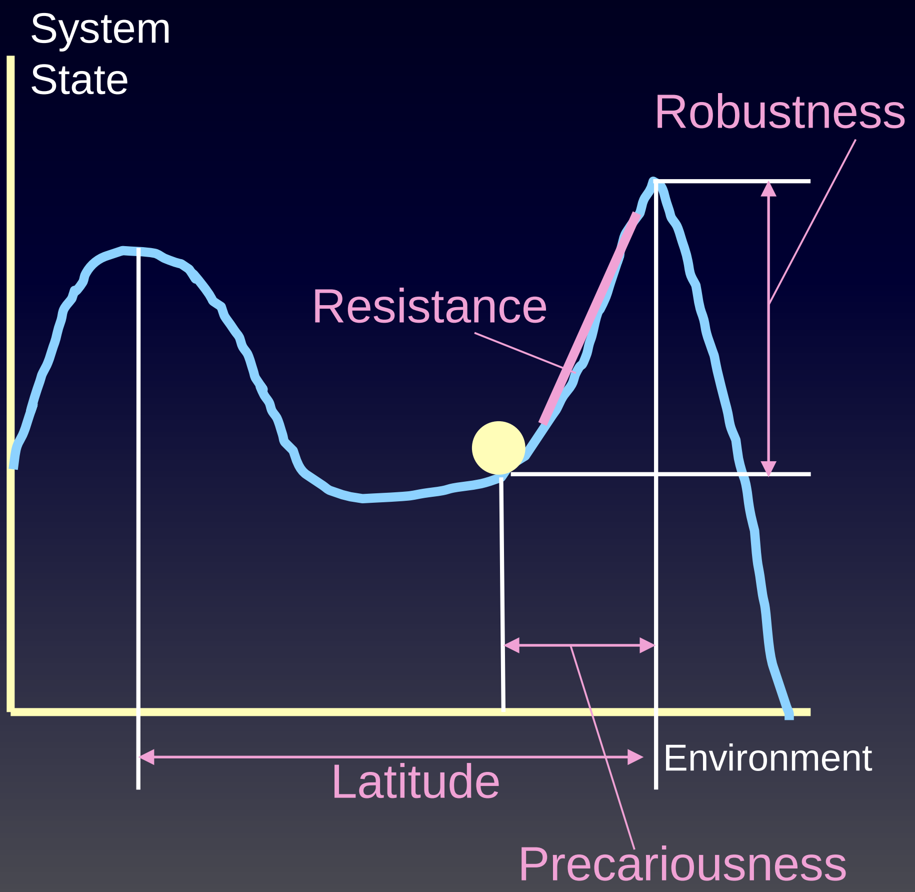


Resilience

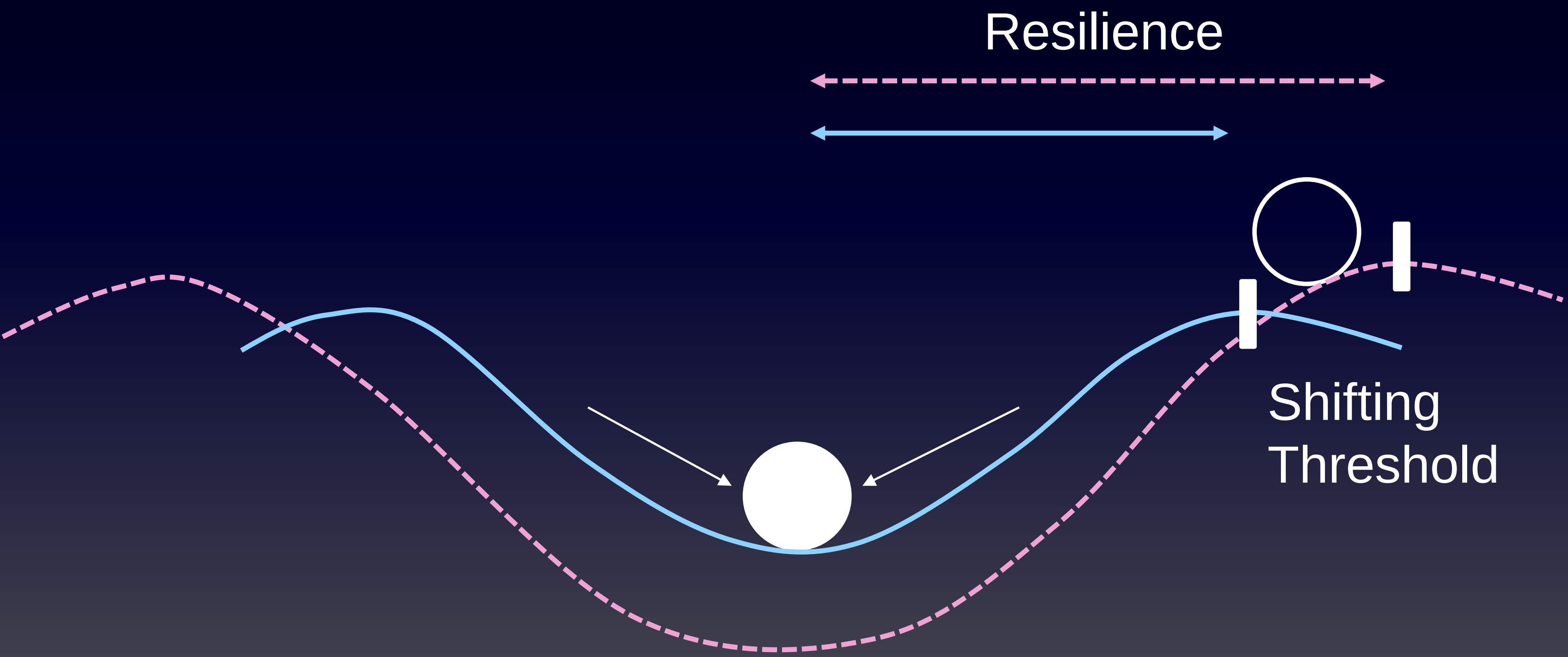
- Ability to bounce back after a disturbance or interruption
- Capacity to adapt to changing conditions and to maintain or regain functionality and vitality in the face of stress or disturbance

Resilient Systems: Characteristics

- Latitude: max amount a system can be changed before losing ability to recover
- Resistance: difficulty of changing system
- Precariousness: how close the current state is to a limit



Improving Resilience



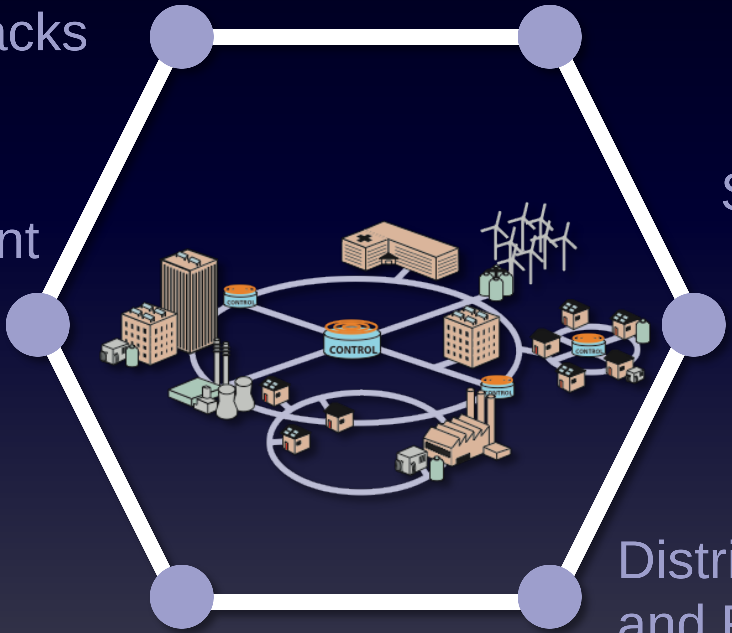
Resilience

Shifting Threshold

Resilience Best Practices

- Adaptive response
  - Automatic task reassignment
  - Isolation or stand-alone safe mode?
- Analytic monitoring
  - Threat/attack recognition and notification
- Redundancy, Parallelism, and Hierarchy
- Distributed Control
  - Coordinated defense

Ongoing Research Thrusts



Coordinated Variable-Structure Switching Attacks

Cyber-Physical Co-Simulation

Flocking-Based Multi-agent Power System Protection

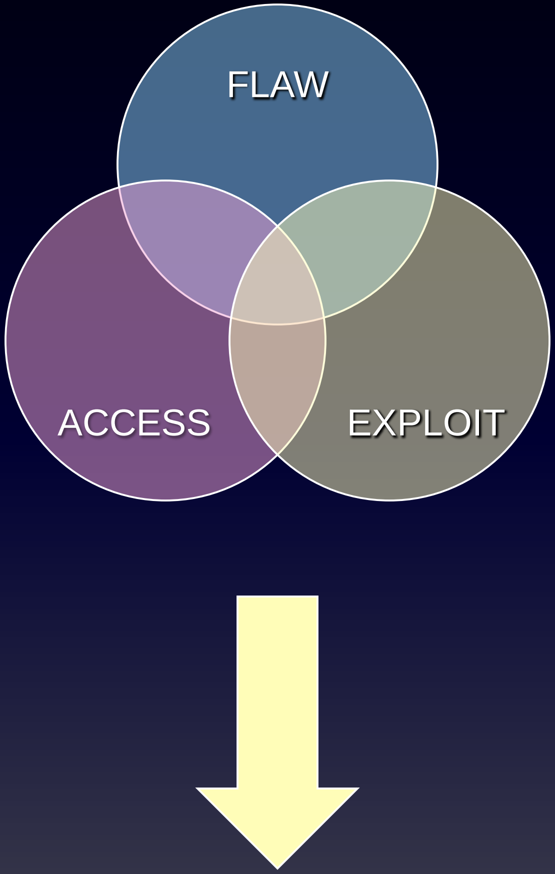
Secure Demand Response and Dispatch

Self-Organizing Microgrid Networks

Distributed Control and Resilience of Smart Grid

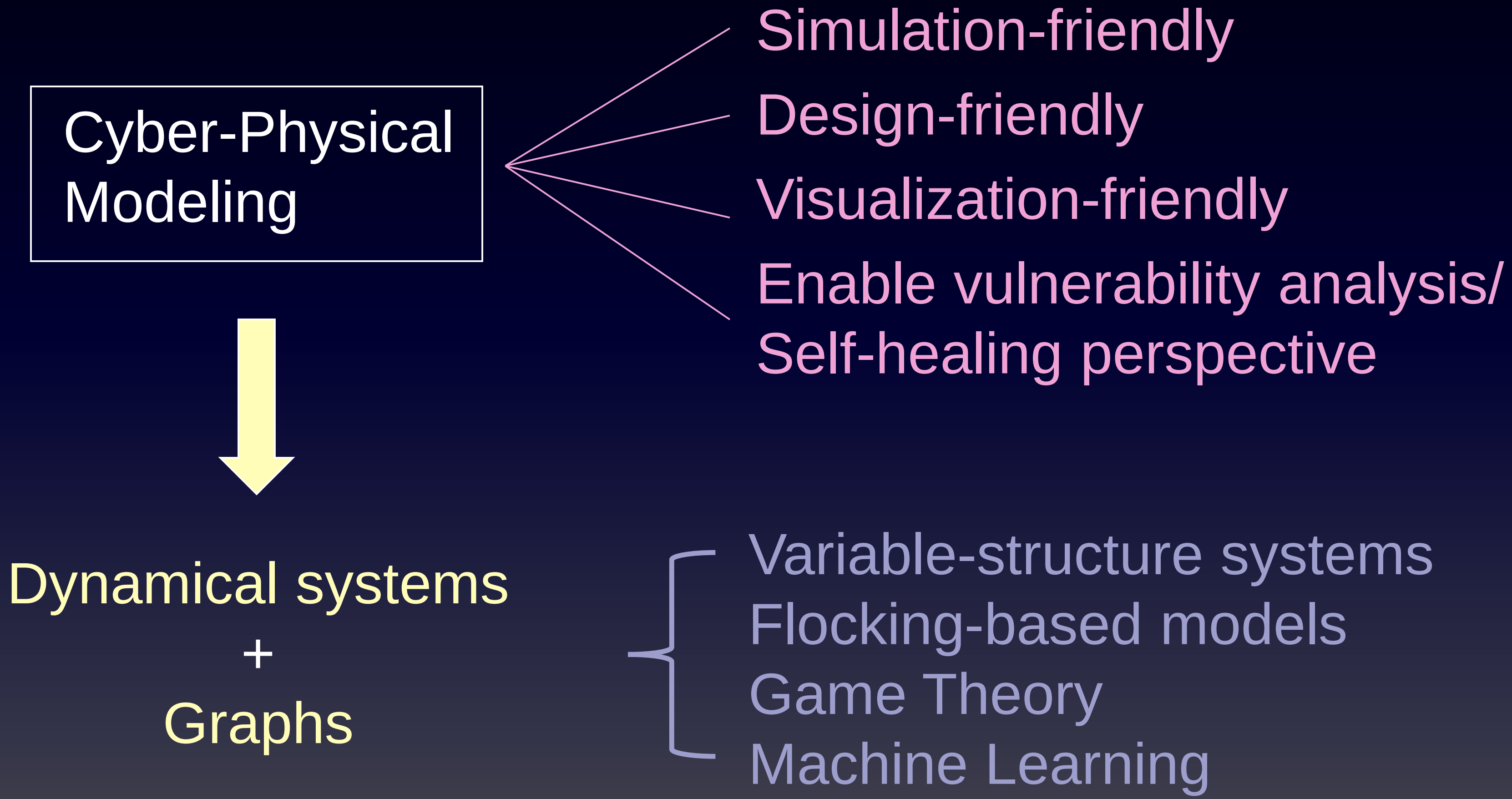
CPS Vulnerabilities

- Complexity
  - Emergent properties
- Connectivity
  - Accessibility to weaknesses
- Collaboration
  - Increases capabilities



Modeling

Modeling



Cyber-Physical Modeling

- Simulation-friendly
- Design-friendly
- Visualization-friendly
- Enable vulnerability analysis/ Self-healing perspective

Dynamical systems
+
Graphs

- Variable-structure systems
- Flocking-based models
- Game Theory
- Machine Learning

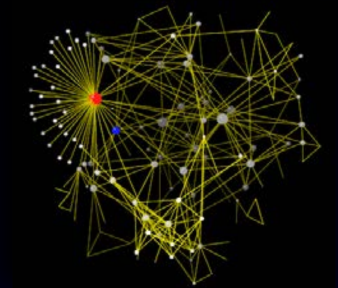
Dynamical Systems

- Describes time evolution of state vector:

$$\dot{x} = f(x, u)$$
$$y = g(x, u)$$

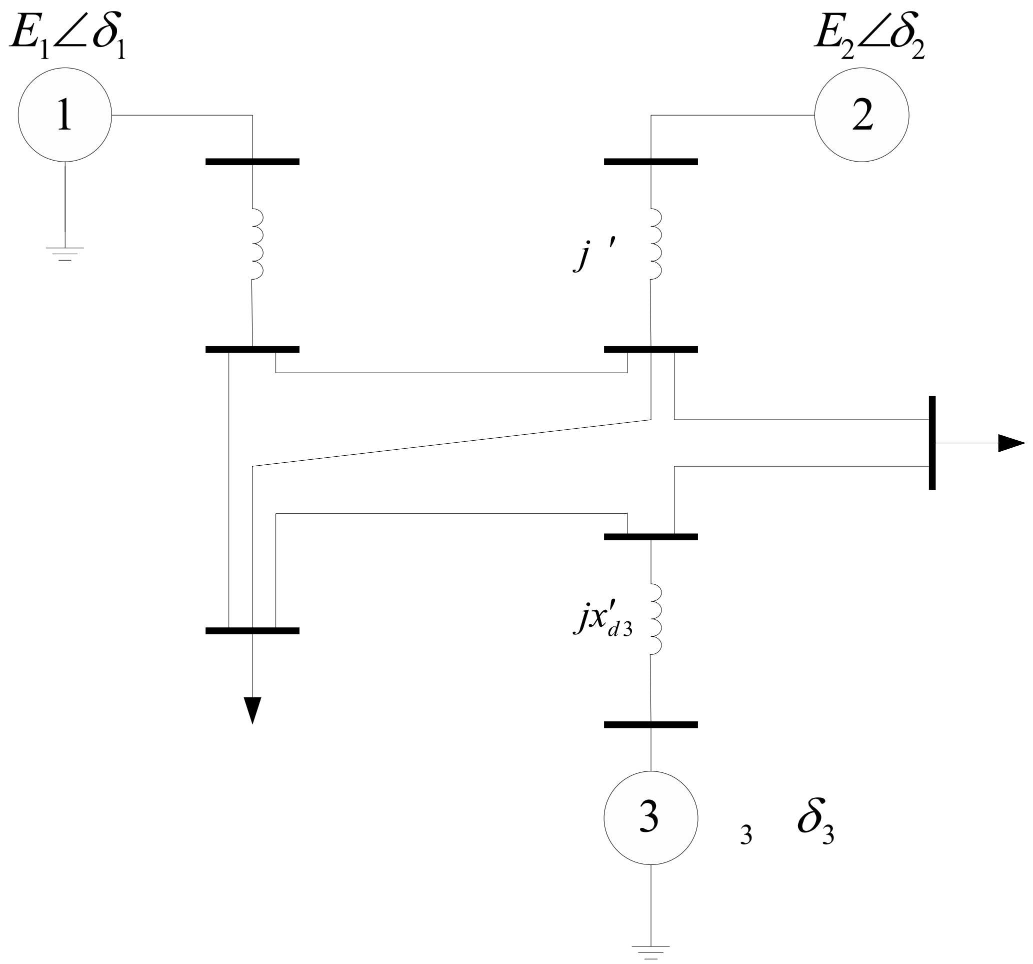
- Models physics of power systems effectively

Graphs

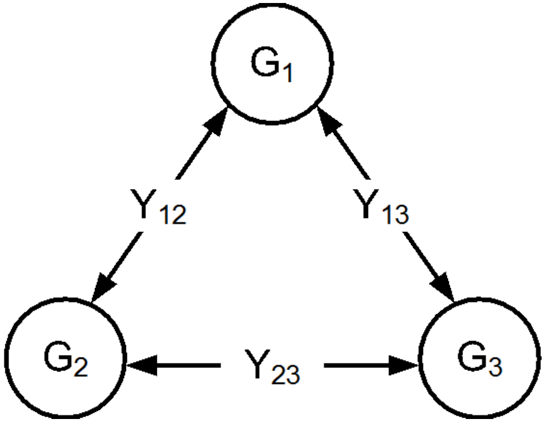


- Defined by collection of vertices and edges.
- Represents pairwise relationships between a set of objects.
- Convenient and compact way to relate cyber-physical dependencies.

WECC 3-machine system



Kron-reduced WECC 3-machine system



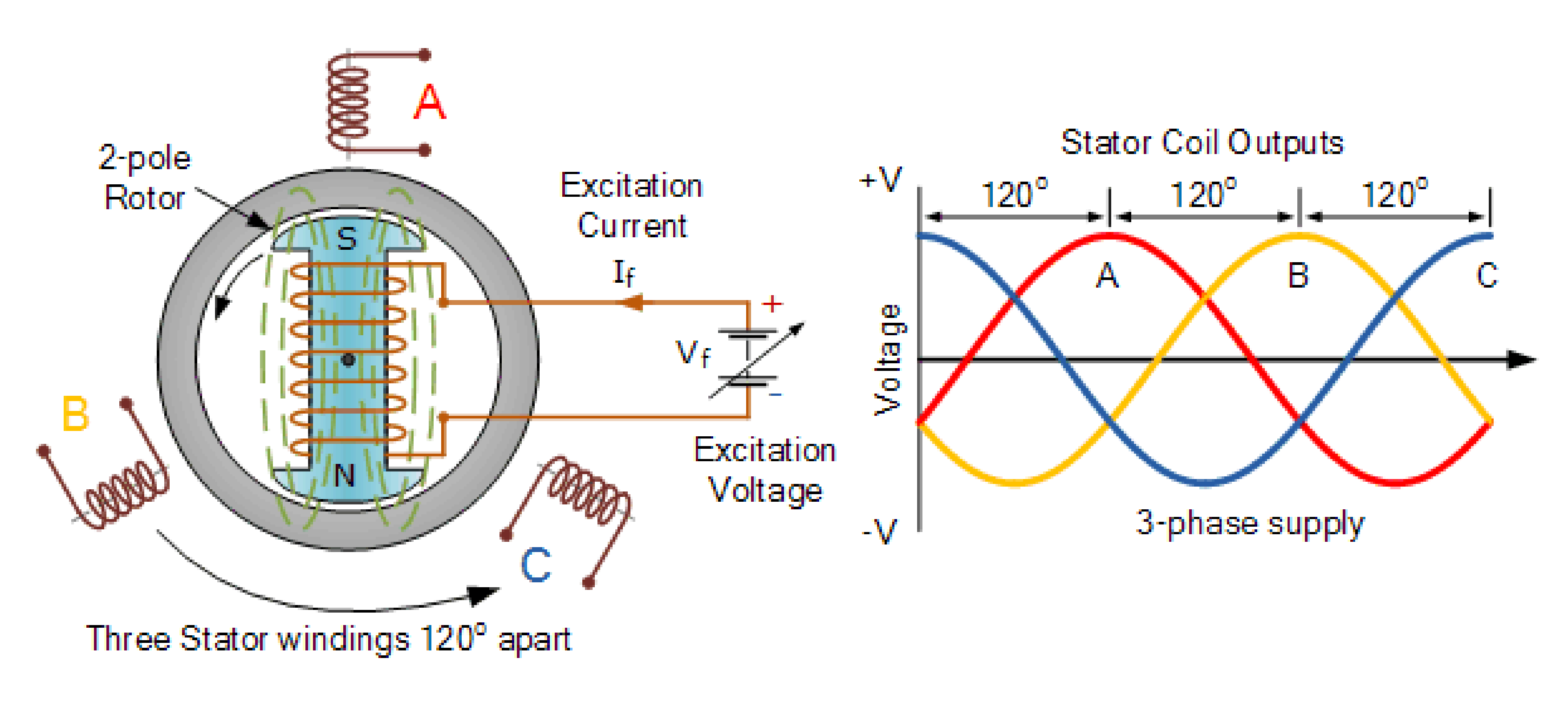
Synchronous Generator

- Represent majority source of commercial electrical energy
- convert the mechanical power output of
  - steam turbines
  - gas turbines
  - reciprocating engines
  - hydro turbines

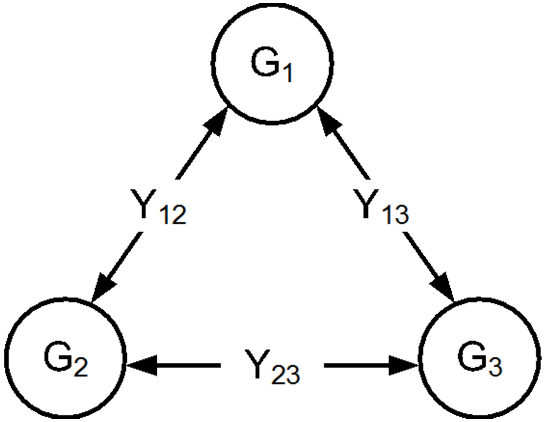
into electrical power

for the grid

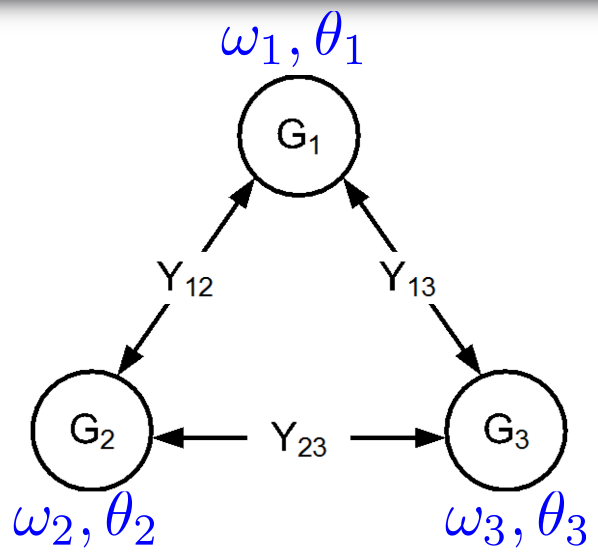
Synchronous Generator



Kron-reduced WECC 3-machine system



swing equation generator model + Kron-reduced WECC 3-machine system

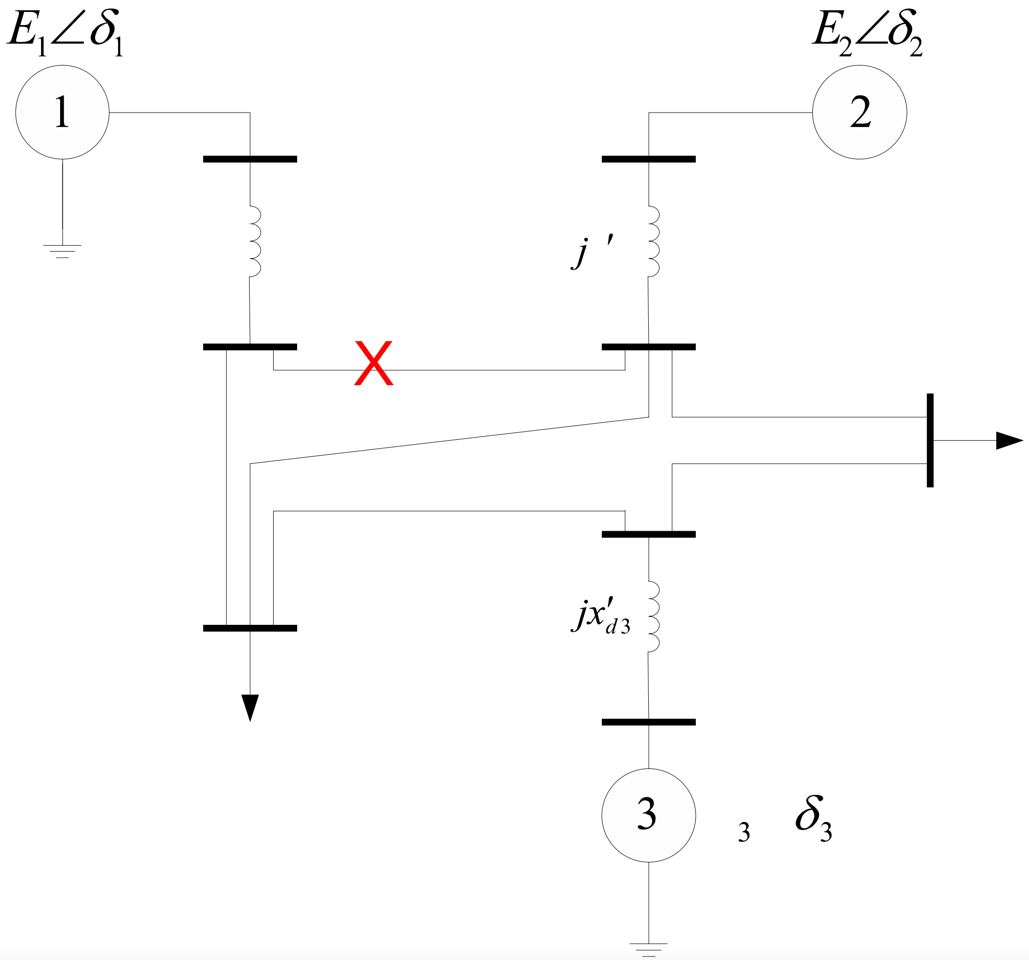


$$M_i \dot{\omega}_i = -D_i \omega_i + P_{m,i} - |E_i|^2 G_{ii} - \sum_{j=1}^{N} |E_i||E_j||Y_{ij}| \sin(\theta_i - \theta_j + \varphi_{ij})$$

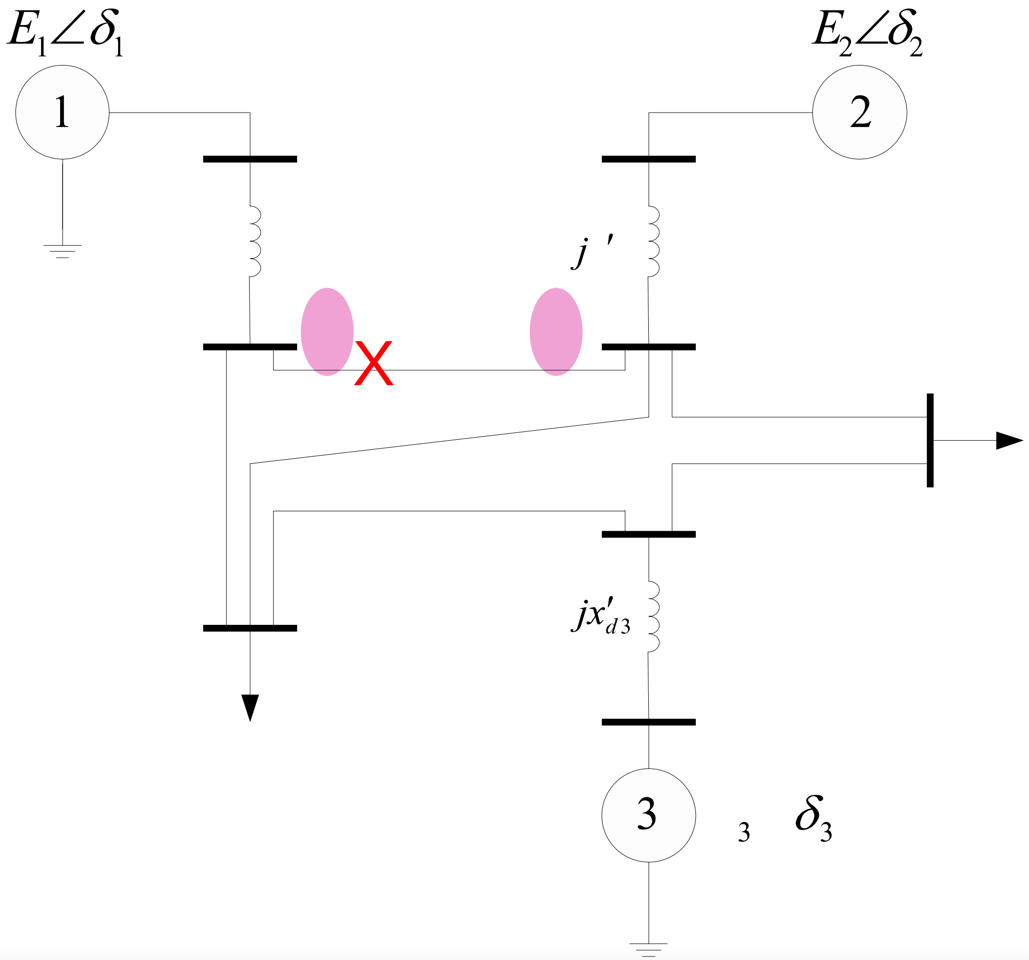
$$\begin{aligned} \boldsymbol{\theta} &= [\theta_1 \ \theta_2 \ \cdots \ \theta_N]^T \\ \boldsymbol{\omega} &= [\omega_1 \ \omega_2 \ \cdots \omega_N]^T \end{aligned}$$

$$\boxed{\begin{aligned} \dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega}) \end{aligned}}$$

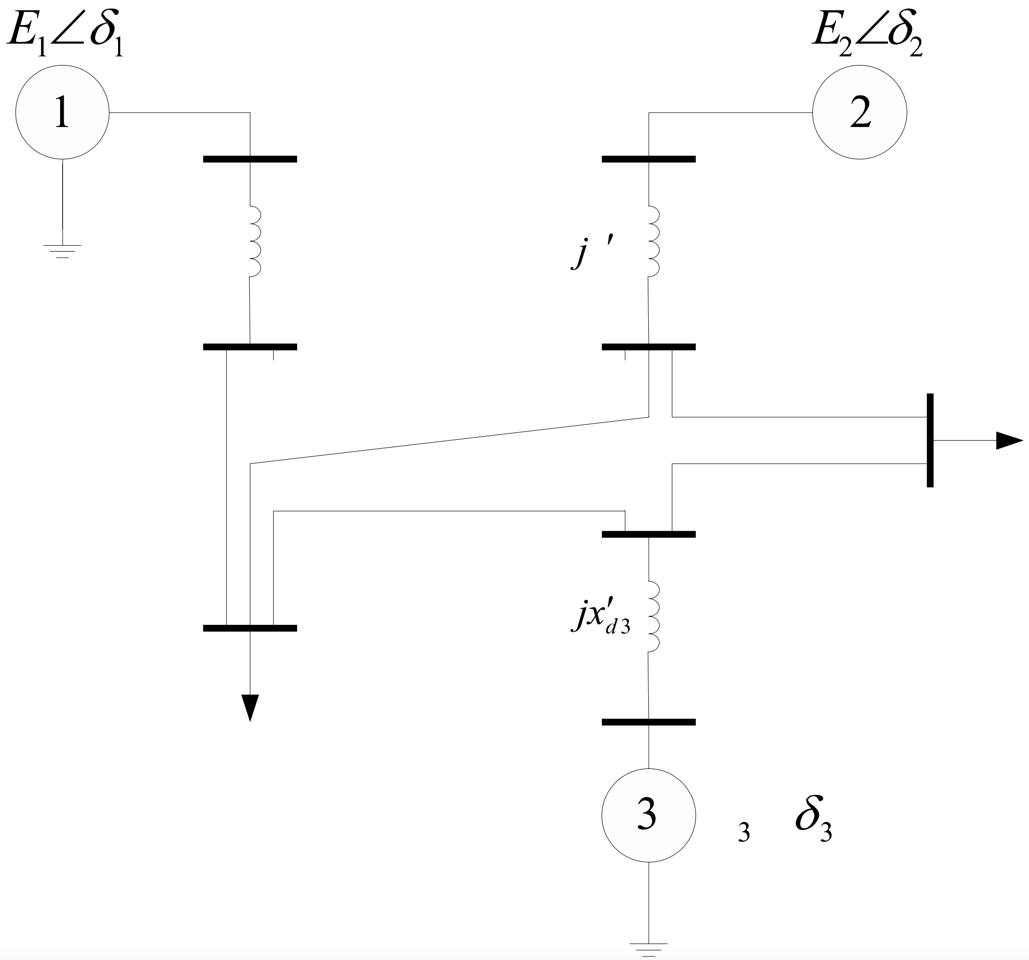
WECC 3-machine system

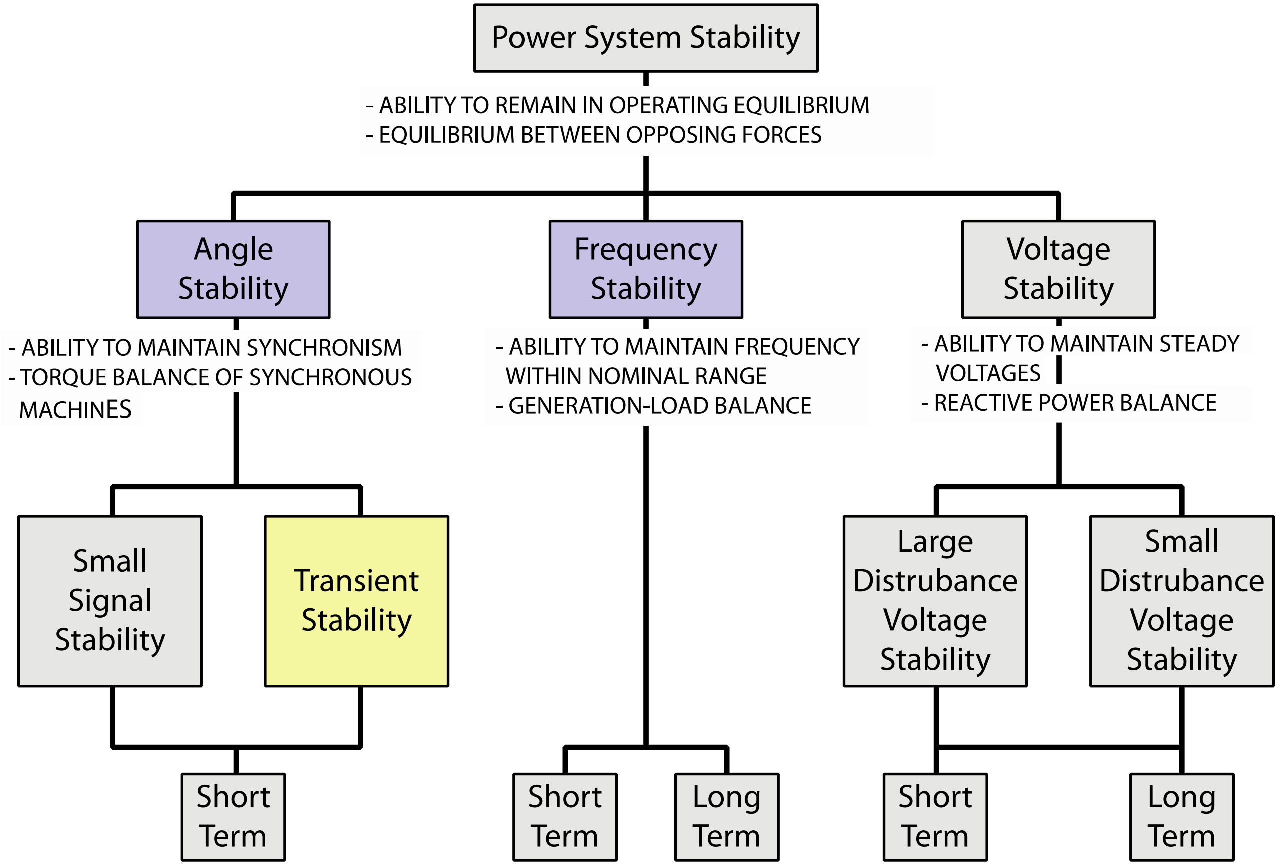


WECC 3-machine system



WECC 3-machine system





Power System Stability

- ABILITY TO REMAIN IN OPERATING EQUILIBRIUM
- EQUILIBRIUM BETWEEN OPPOSING FORCES

Angle Stability

- ABILITY TO MAINTAIN SYNCHRONISM
- TORQUE BALANCE OF SYNCHRONOUS MACHINES

Frequency Stability

- ABILITY TO MAINTAIN FREQUENCY WITHIN NOMINAL RANGE
- GENERATION-LOAD BALANCE

Voltage Stability

- ABILITY TO MAINTAIN STEADY VOLTAGES
- REACTIVE POWER BALANCE

Physical Impact Focus

- Transient stability:
  - Ability of a synchronous generator to maintain electromagnetic and mechanical torque in the face of large system disturbance (cyber or physical in nature)

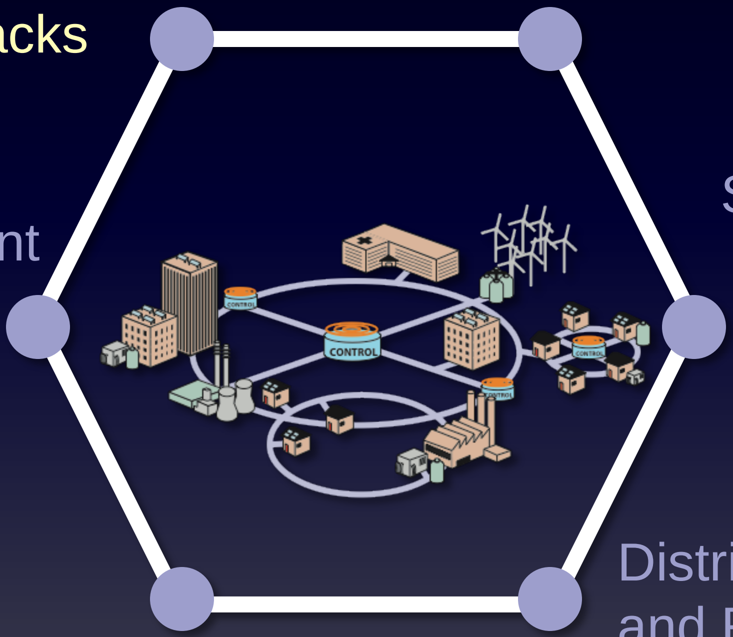
$$\theta_i, \omega_i$$

Ongoing Research Thrusts

Coordinated Variable-Structure Switching Attacks

Cyber-Physical Co-Simulation

Flocking-Based Multi-agent Power System Protection



Secure Demand Response and Dispatch

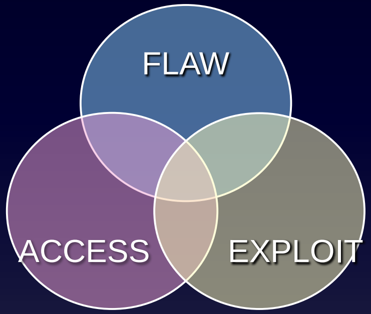
Self-Organizing Microgrid Networks

Distributed Control and Resilience of Smart Grid

Questions

- How can cyber work against physical?

- What new vulnerabilities arise?



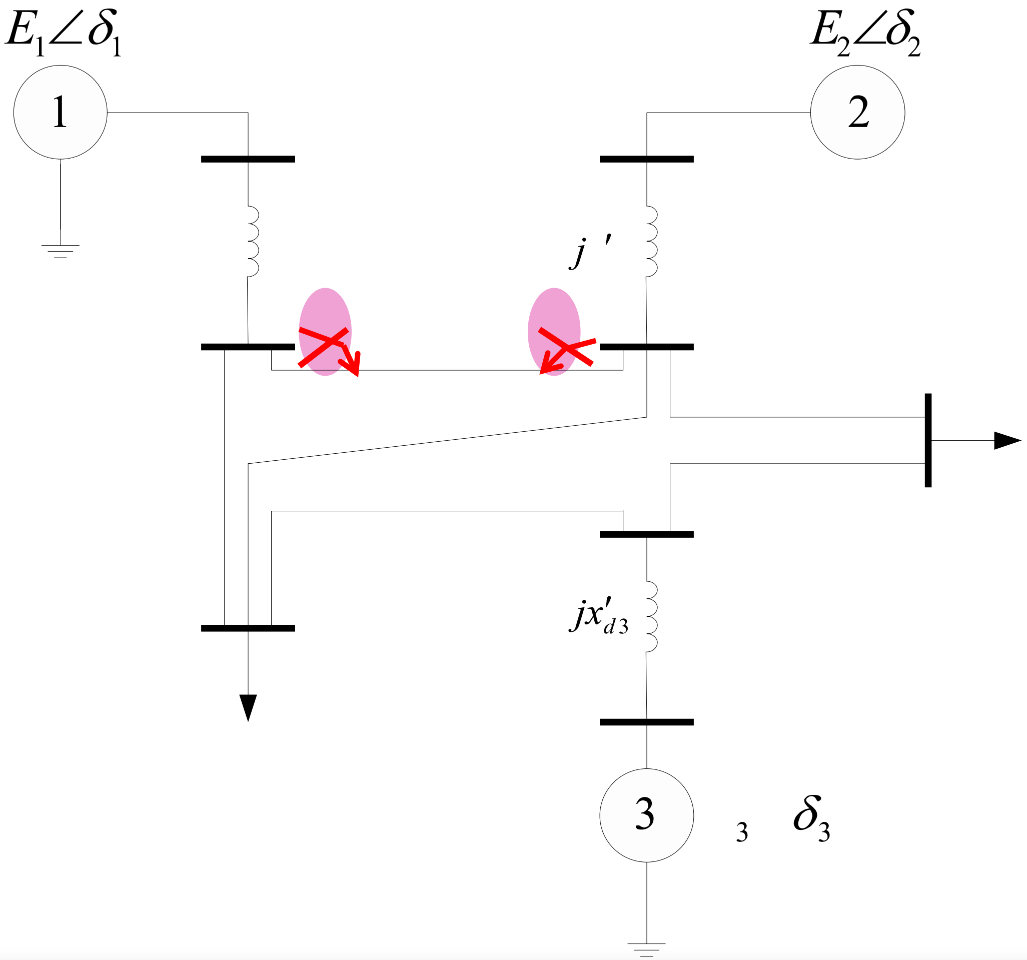
- What grid topologies and device characteristics make the system less vulnerable?

Coordinated Switching Attacks

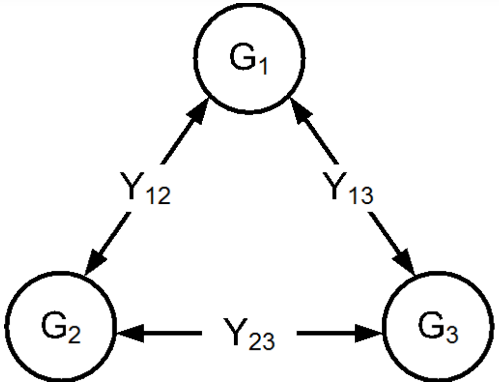
- Goal: physical disruption of target generator through transient instability

- Assumptions:
  1. Knowledge of local model of smart grid including existence of target generator
  2. Knowledge of target generator states
  3. Electromechanical switching control over associated breaker(s)

WECC 3-machine system

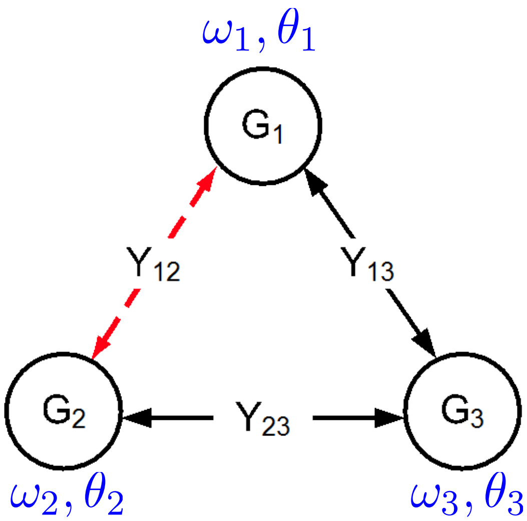


$$\begin{aligned} \dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega}) \end{aligned}$$

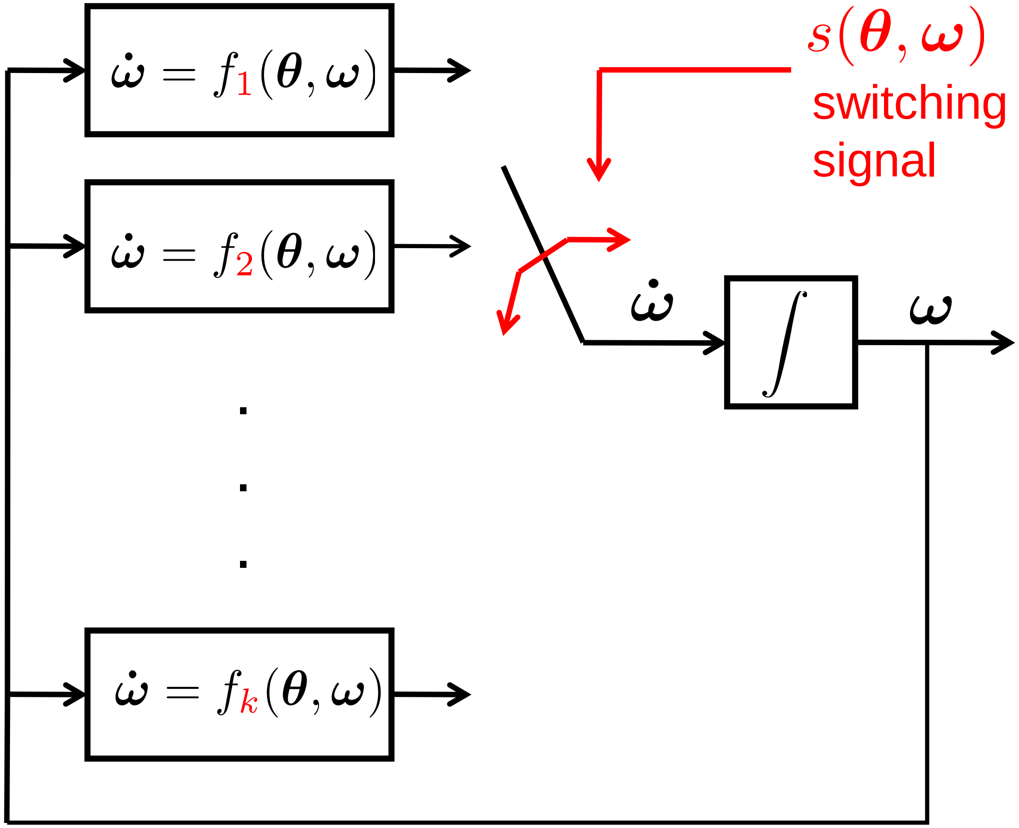


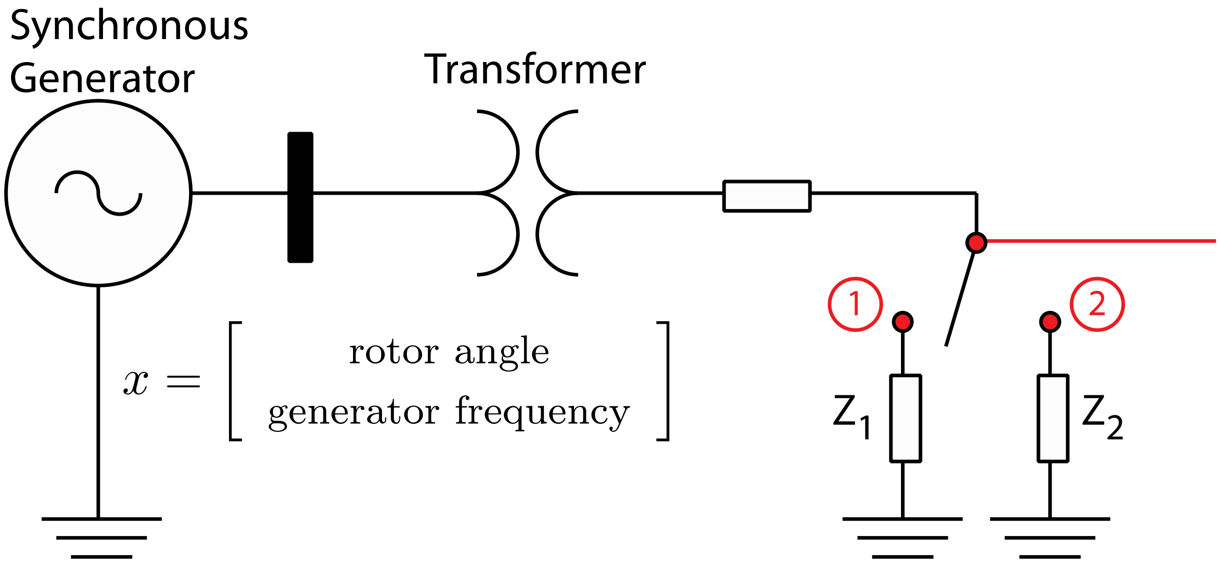
cyber-controlled switching signal

$$\begin{aligned} \dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= \begin{cases} f_1(\boldsymbol{\theta}, \boldsymbol{\omega}) & s = 1 \\ f_2(\boldsymbol{\theta}, \boldsymbol{\omega}) & s = 2 \\ \vdots & \vdots \\ f_k(\boldsymbol{\theta}, \boldsymbol{\omega}) & s = k \end{cases} \end{aligned}$$



Variable Structure System


$\dot{\boldsymbol{\omega}} = f_1(\boldsymbol{\theta}, \boldsymbol{\omega})$
$\dot{\boldsymbol{\omega}} = f_2(\boldsymbol{\theta}, \boldsymbol{\omega})$
$\dot{\boldsymbol{\omega}} = f_k(\boldsymbol{\theta}, \boldsymbol{\omega})$
$s(\boldsymbol{\theta}, \boldsymbol{\omega})$
switching signal
$\dot{\boldsymbol{\omega}}$
$\int$
$\boldsymbol{\omega}$



$$x = \begin{bmatrix} \text{rotor angle} \\ \text{generator frequency} \end{bmatrix}$$

Two-Subsystem Variable Structure Model

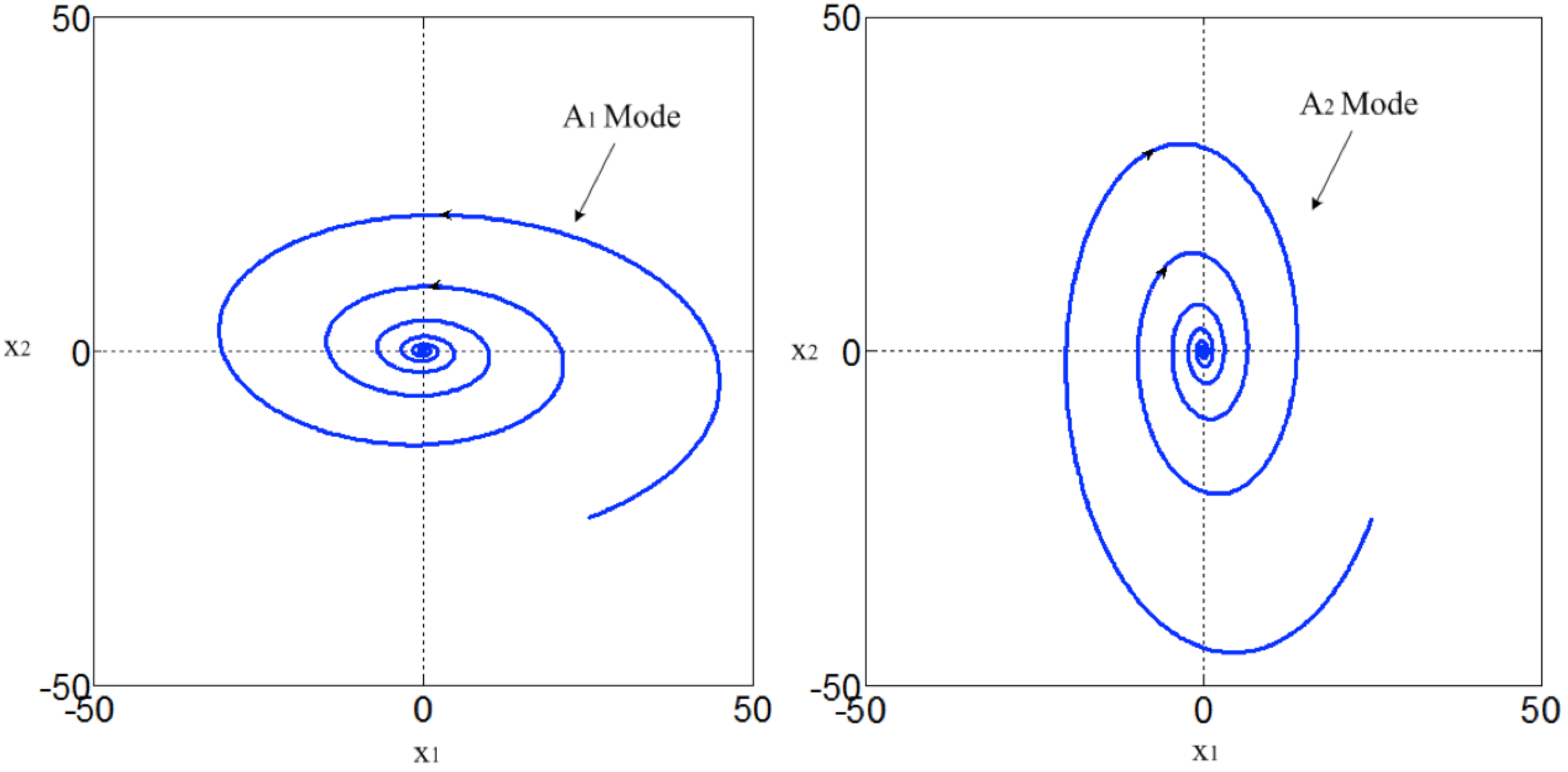
$$\boldsymbol{x} \quad = \quad [\ x_1\ x_2\ ]^T$$

$$\boxed{\dot{\boldsymbol{x}} \quad = \quad \begin{cases} f_1(\boldsymbol{x},t) & s(\boldsymbol{x},t) > 0 \\ f_2(\boldsymbol{x},t) & s(\boldsymbol{x},t) \leq 0 \end{cases}}$$

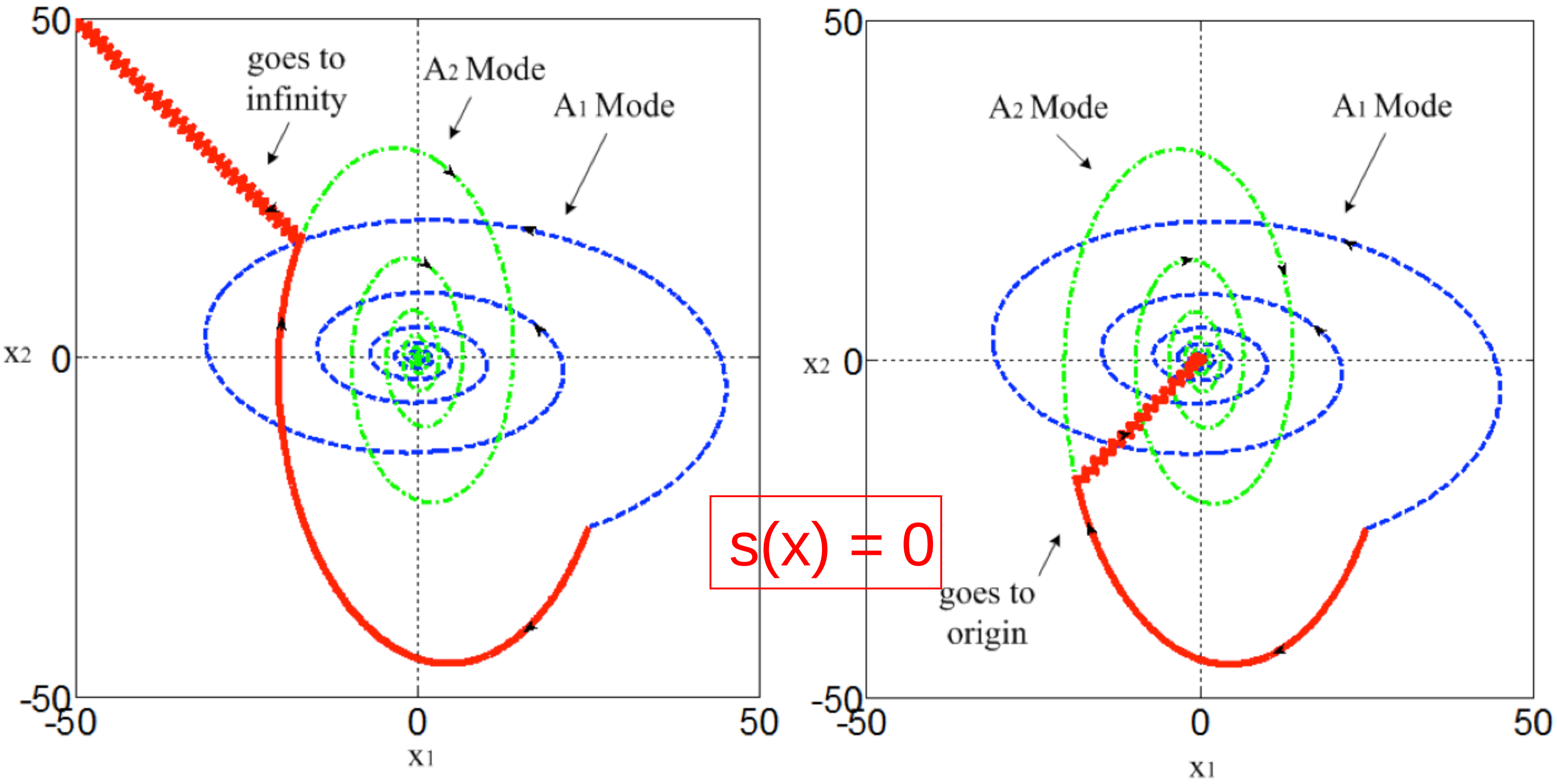
Example:

$$\dot{\boldsymbol{x}} = \begin{cases} A_1\boldsymbol{x}, & s(\boldsymbol{x}) > 0, \text{ where } A_1 = \begin{bmatrix} -1 & -10 \\ 3 & -0.3 \end{bmatrix} \\ A_2\boldsymbol{x}, & s(\boldsymbol{x}) \leq 0, \text{ where } A_2 = \begin{bmatrix} -0.3 & 3 \\ -10 & -1 \end{bmatrix} \end{cases}$$

Static Switch Phase Portraits



Sliding Mode Existence:



s(x) = 0

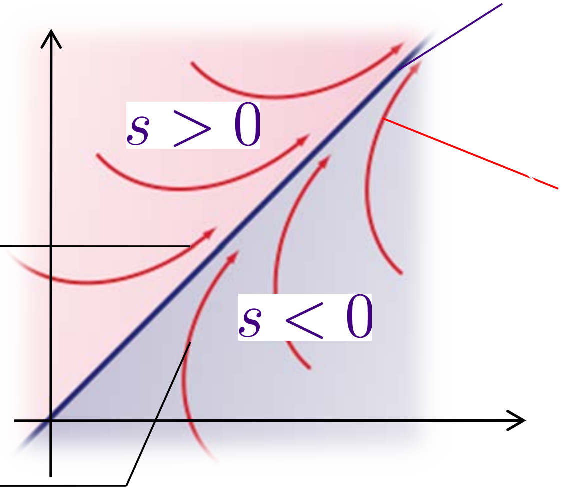
$$s(\boldsymbol{x}) = x_1 + x_2 \qquad s(\boldsymbol{x}) = -x_1 + x_2$$

The Sliding Mode

- "Emergent" property from switching that has characteristics different from individual subsystems
- Motion of state trajectory along a chosen line/plane/surface s(x) = 0
- IDEA: exploit the sliding mode for destabilizing the system

Existence of the Sliding Mode

$$\lim_{s\to 0^+} \dot{s} \leq 0 \quad \text{and} \quad \lim_{s\to 0^-} \dot{s} > 0 \quad \Longrightarrow \quad s\dot{s} < 0$$



sliding surface

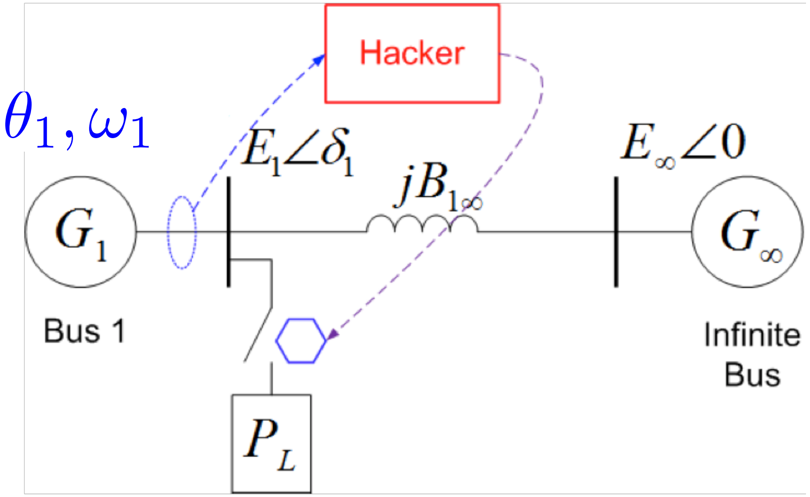
state-space trajectories

$$\dot{\boldsymbol{x}} = \begin{cases} f_1(\boldsymbol{x},t) & s(\boldsymbol{x},t) > 0 \\ f_2(\boldsymbol{x},t) & s(\boldsymbol{x},t) \leq 0 \end{cases}$$

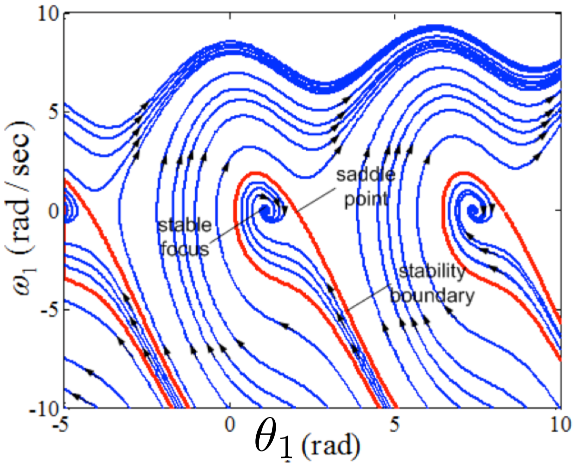
Step 1: Modeling

$$A_1 : \begin{cases} \dot{\theta}_1 = \omega_1 \\ \dot{\omega}_1 = -10\sin\theta_1 - \omega_1 \end{cases} \qquad \text{if } P_L \text{ connected}$$

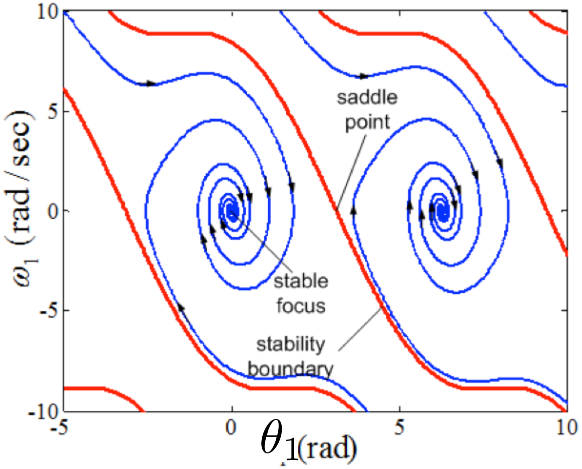
$$A_2 : \begin{cases} \dot{\theta}_1 = \omega_1 \\ \dot{\omega}_1 = 9 - 10\sin\theta_1 - \omega_1 \end{cases} \qquad \text{if } P_L \text{ not connected}$$



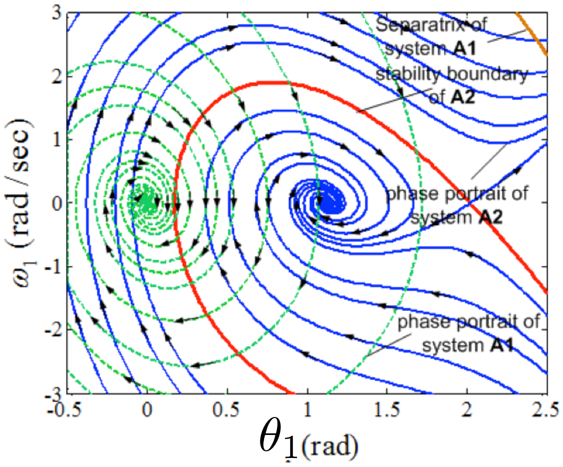
Step 2: Existence of Sliding Mode



Phase Portrait of A_1

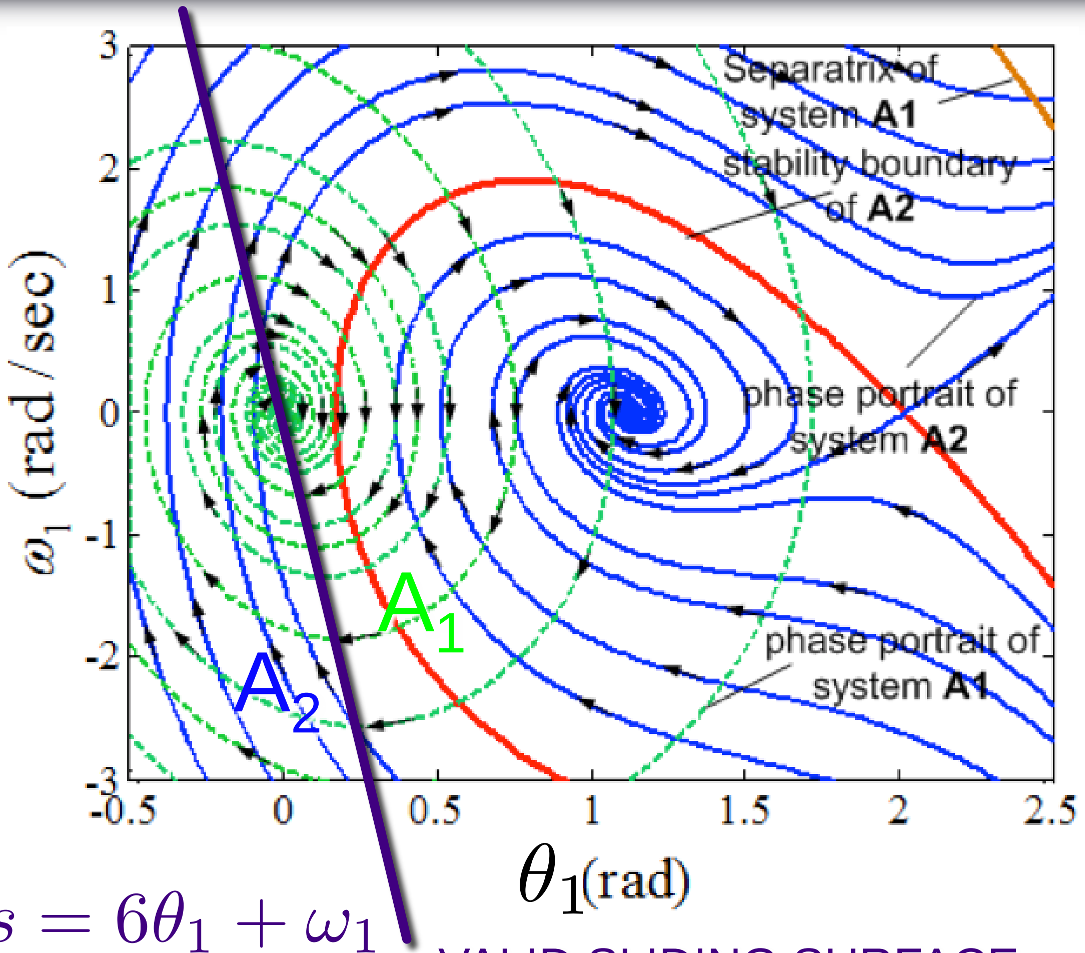


Phase Portrait of A_2



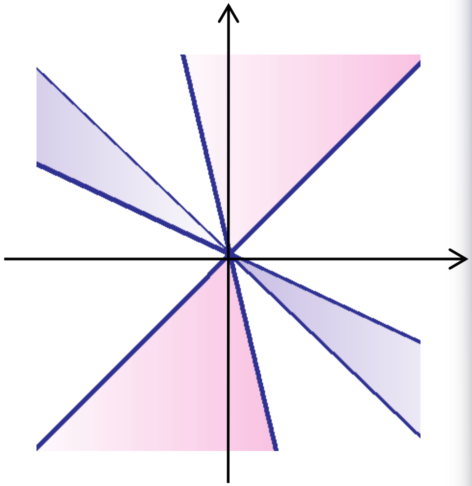
Overlapping Close-up

Step 2: Existence of Sliding Mode



$$s = 6\theta_1 + \omega_1$$

VALID SLIDING SURFACE



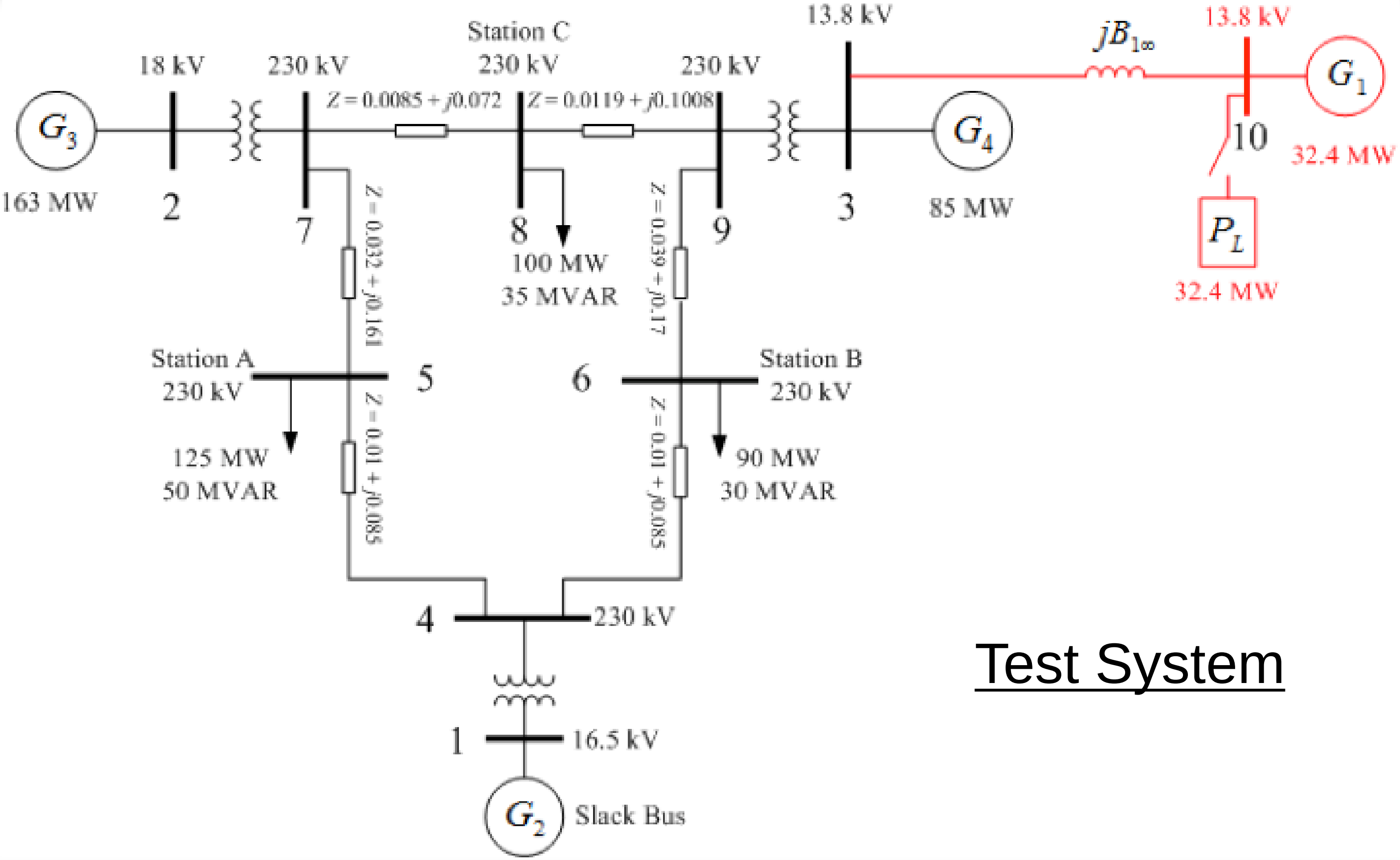
Step 3: Assign s(x) for attack

$$\boxed{s = 6\theta_1 + \omega_1}$$

Vulnerability Assessment

1. Represent smart grid system as variable structure system whereby s(x) is general.
2. Apply linearization techniques to derive a linear representation.
3. Determine parameter range for sliding mode existence.
4. Rank degree of vulnerability based on parameter range.

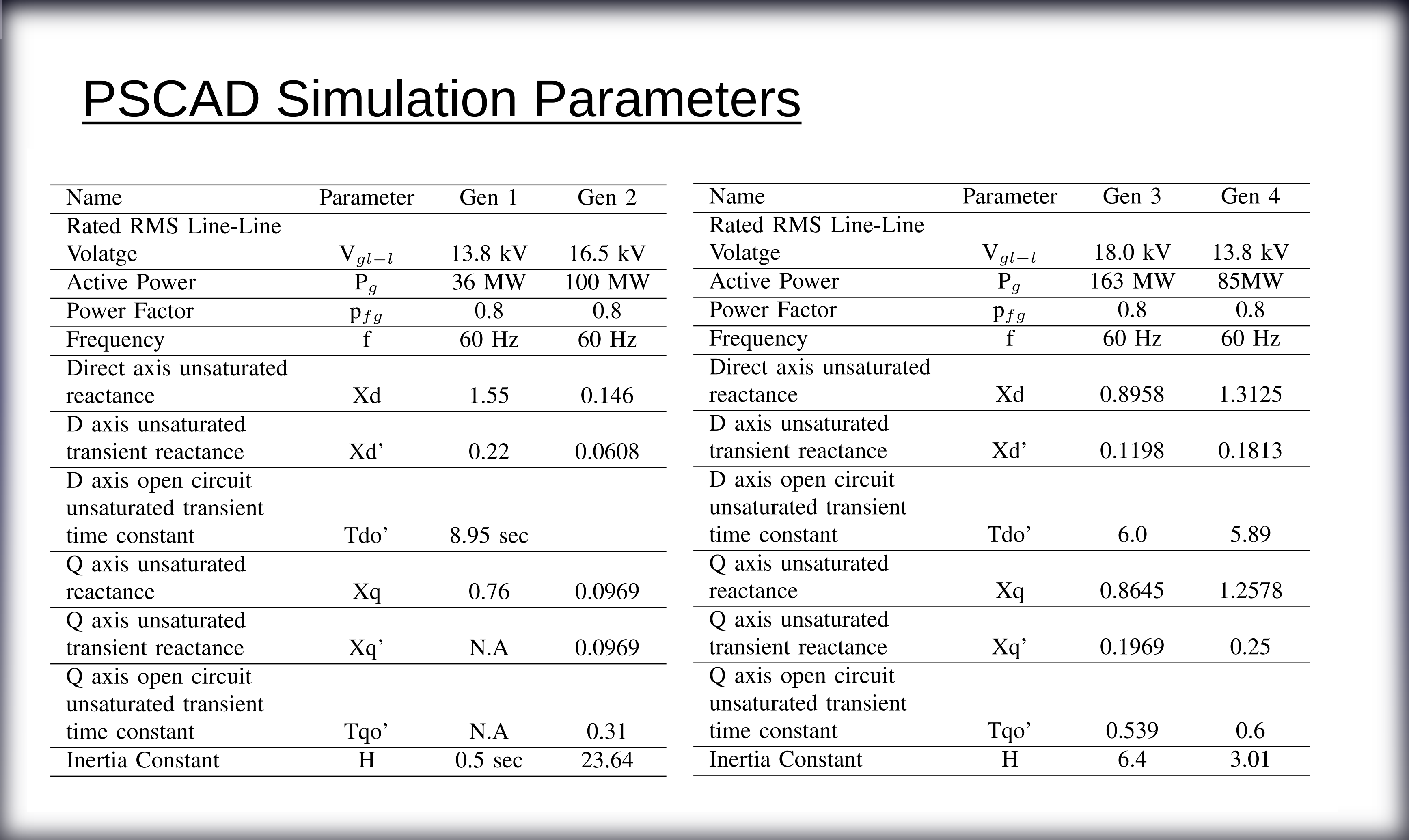
Attack Simulation



Test System

Attack Simulation

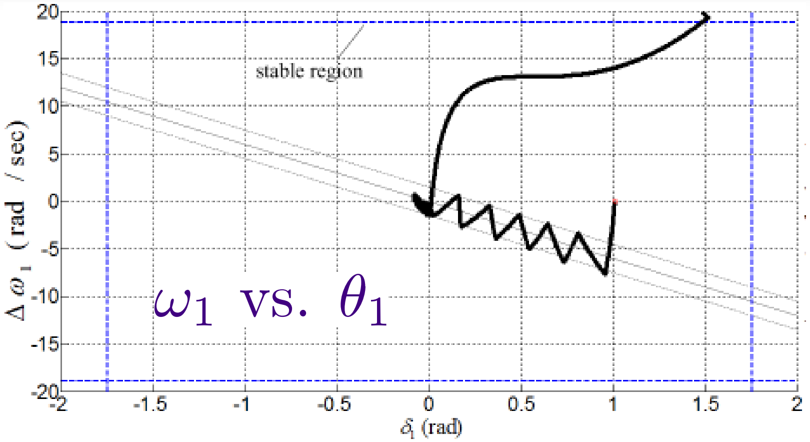
PSCAD Simulation Parameters



Name	Parameter	Gen 1	Gen 2
Rated RMS Line-Line Volatge	V$_{gl-l}$	13.8 kV	16.5 kV
Active Power	P$_g$	36 MW	100 MW
Power Factor	p$_{fg}$	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	1.55	0.146
D axis unsaturated transient reactance	Xd’	0.22	0.0608
D axis open circuit unsaturated transient time constant	Tdo’	8.95 sec	
Q axis unsaturated reactance	Xq	0.76	0.0969
Q axis unsaturated transient reactance	Xq’	N.A	0.0969
Q axis open circuit unsaturated transient time constant	Tqo’	N.A	0.31
Inertia Constant	H	0.5 sec	23.64

Name	Parameter	Gen 3	Gen 4
Rated RMS Line-Line Volatge	V$_{gl-l}$	18.0 kV	13.8 kV
Active Power	P$_g$	163 MW	85MW
Power Factor	p$_{fg}$	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	0.8958	1.3125
D axis unsaturated transient reactance	Xd’	0.1198	0.1813
D axis open circuit unsaturated transient time constant	Tdo’	6.0	5.89
Q axis unsaturated reactance	Xq	0.8645	1.2578
Q axis unsaturated transient reactance	Xq’	0.1969	0.25
Q axis open circuit unsaturated transient time constant	Tqo’	0.539	0.6
Inertia Constant	H	6.4	3.01

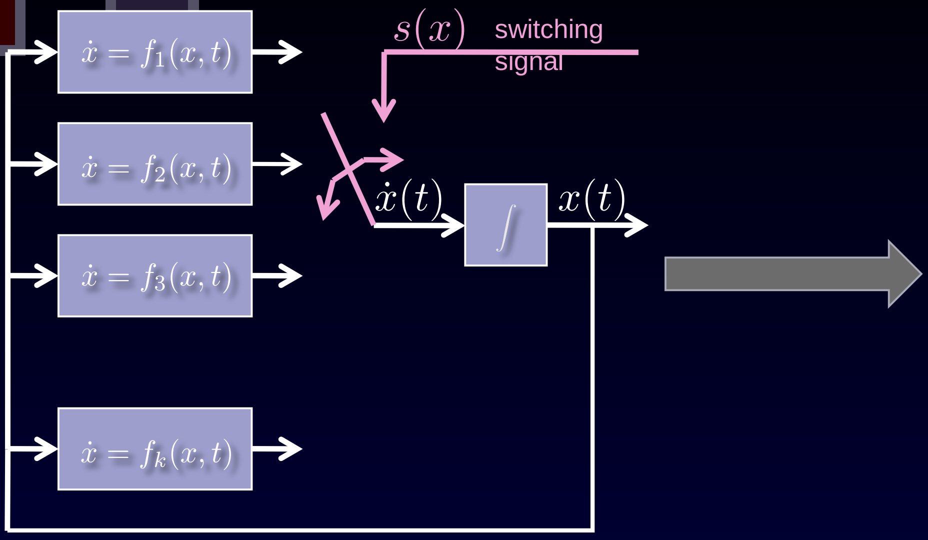
Simulation of Test System



$\omega_1(t)$

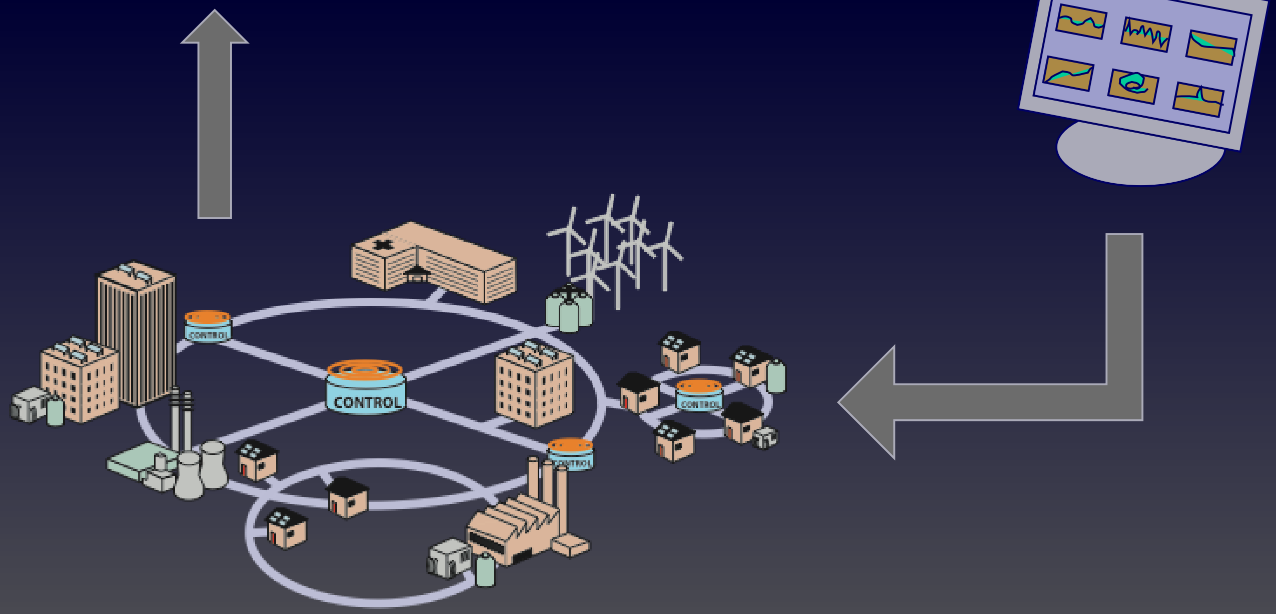
$V_1(t)$

$\theta_1(t)$



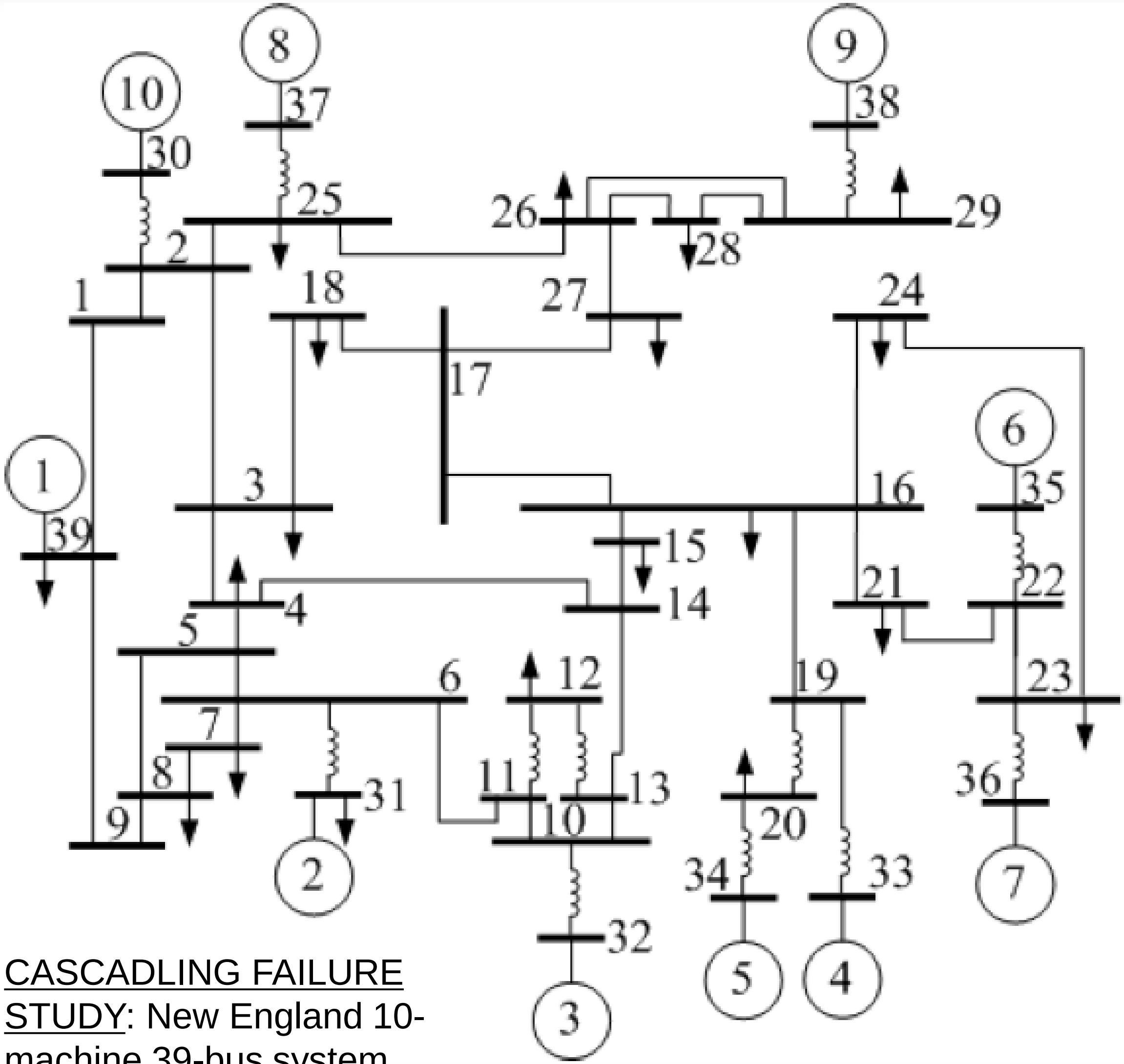
Outcomes

- Vulnerability analysis tool.
- Expanded definition of power system security.
- Secure smart grid development guidelines.

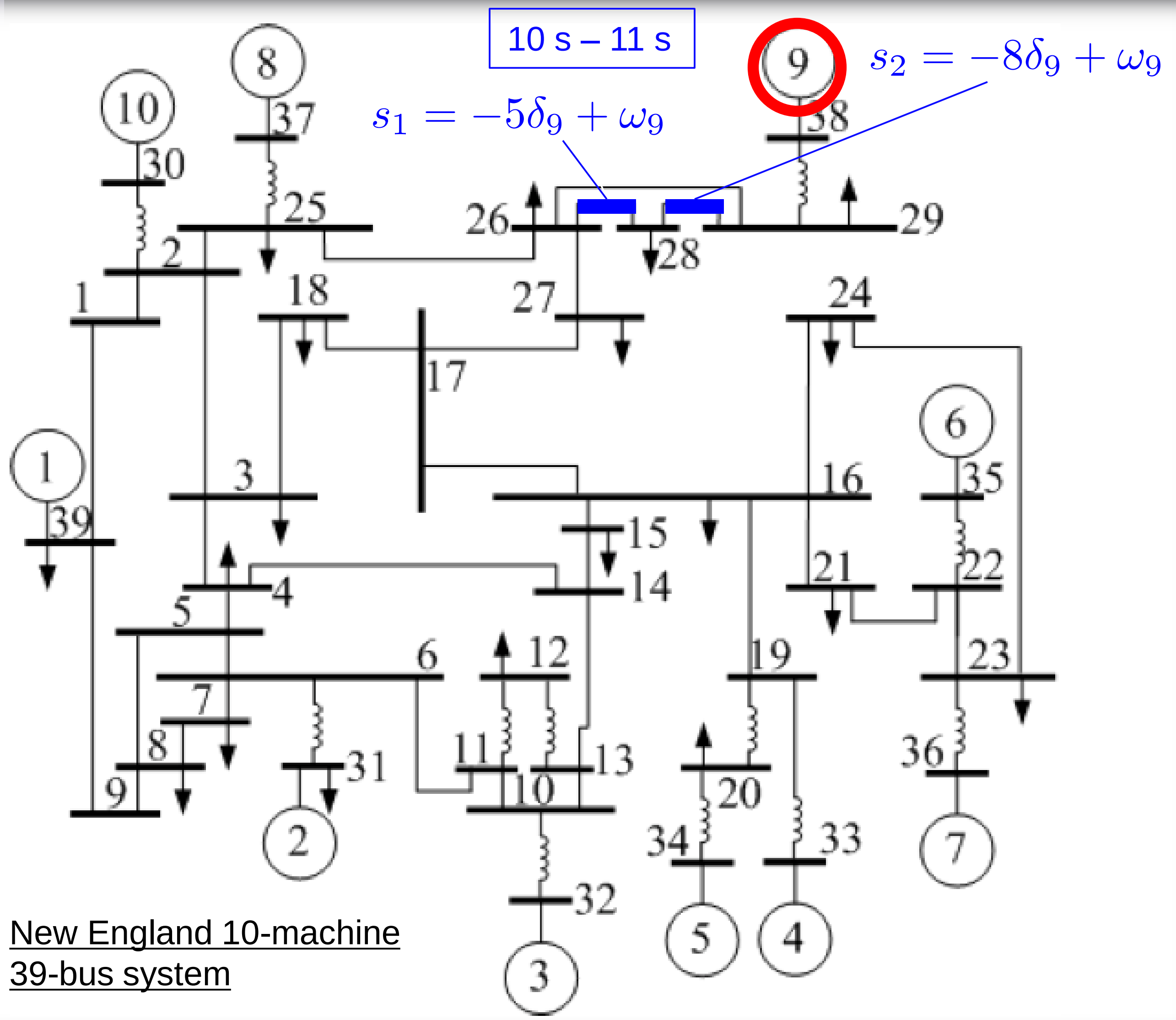


Insights on Switching Vulnerabilities

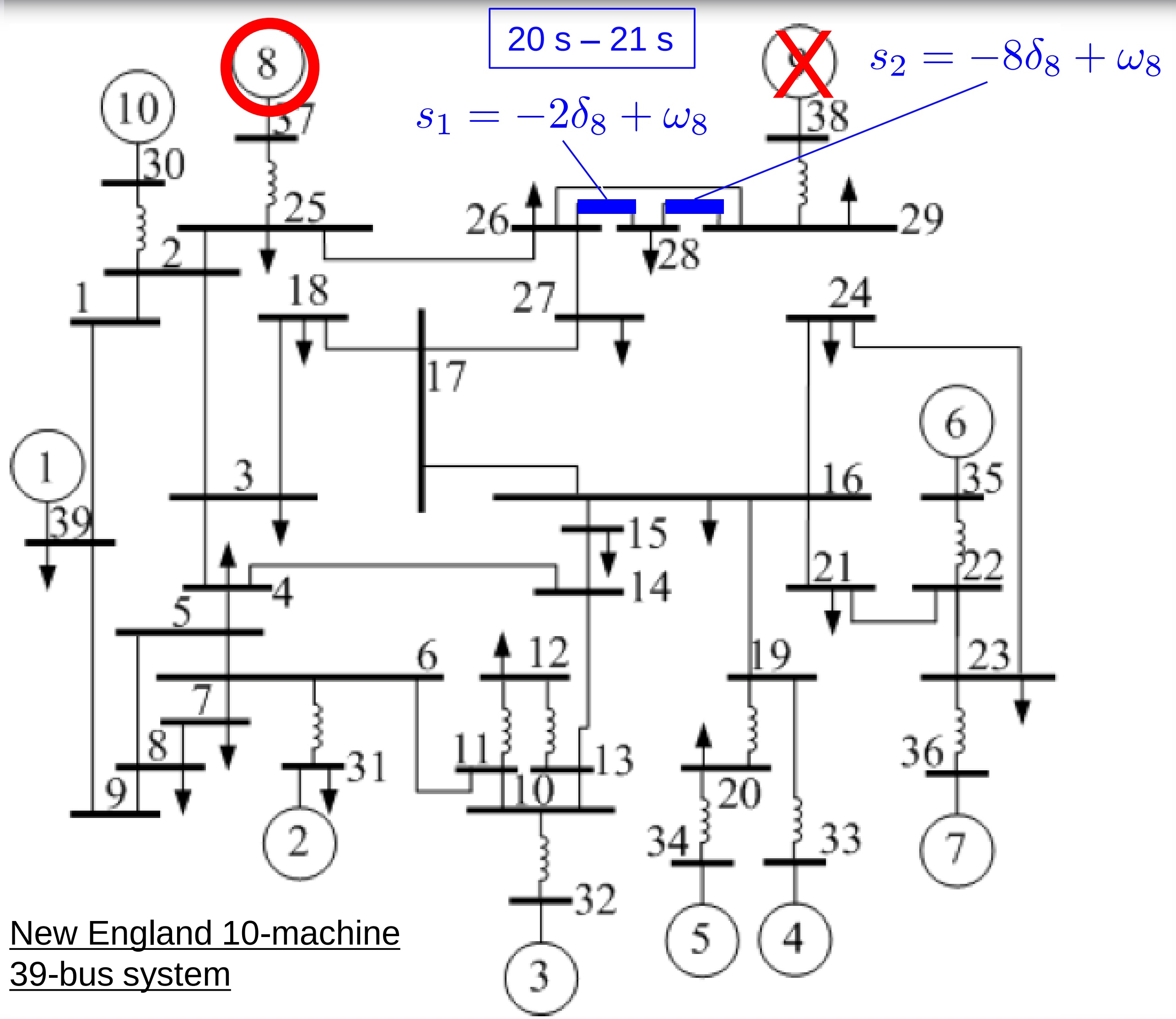
- Transmission line switches typically more susceptible than load switches
- Switches in close proximity to larger generators and loads more vulnerable
- Generators associated with longer transmission lines more vulnerable
- Load switches with small loads can bypass protection mechanisms reducing security margin of other components



CASCADLING FAILURE STUDY: New England 10-machine 39-bus system



New England 10-machine 39-bus system

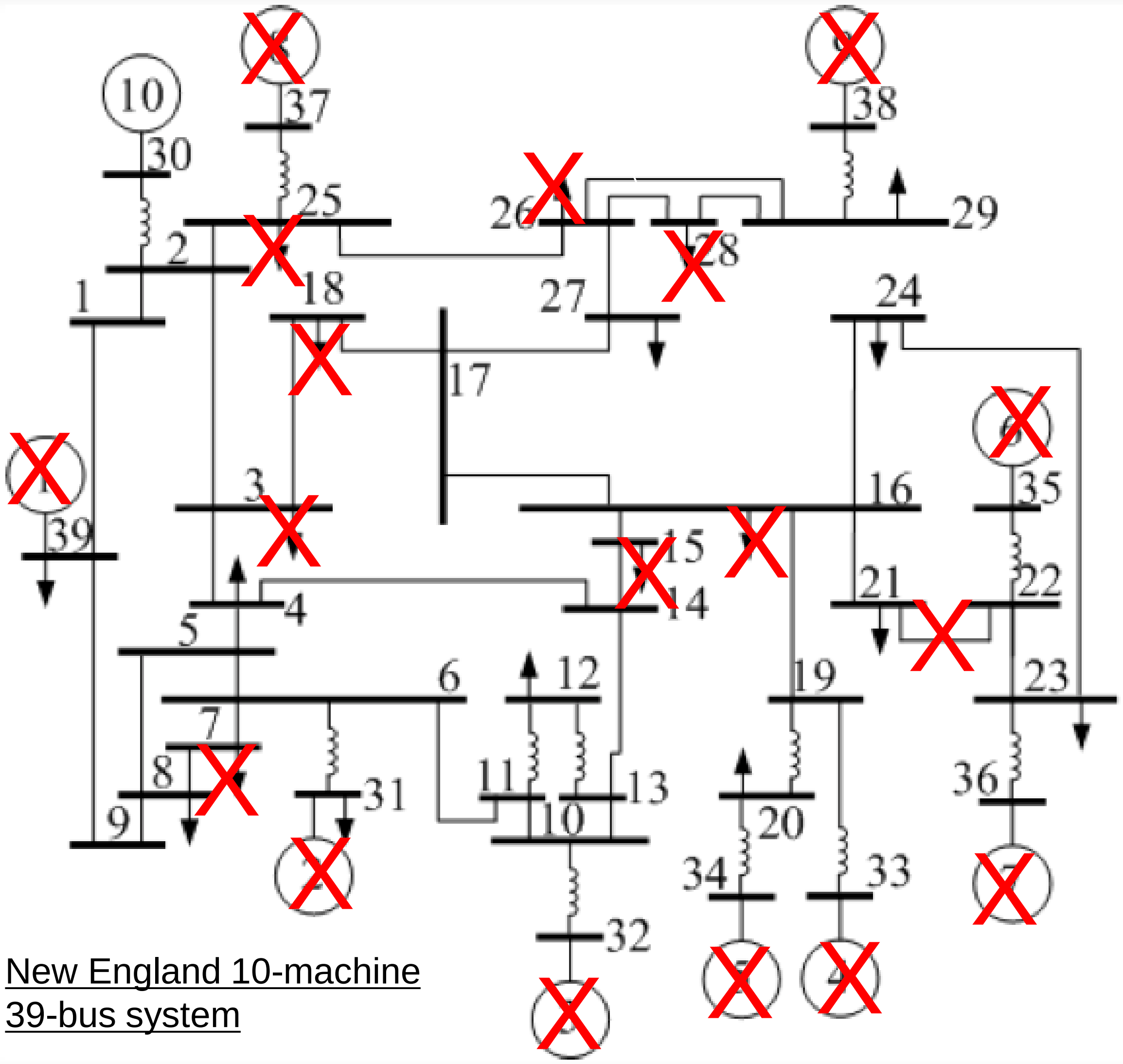


20 s – 21 s

$s_1 = -2\delta_8 + \omega_8$

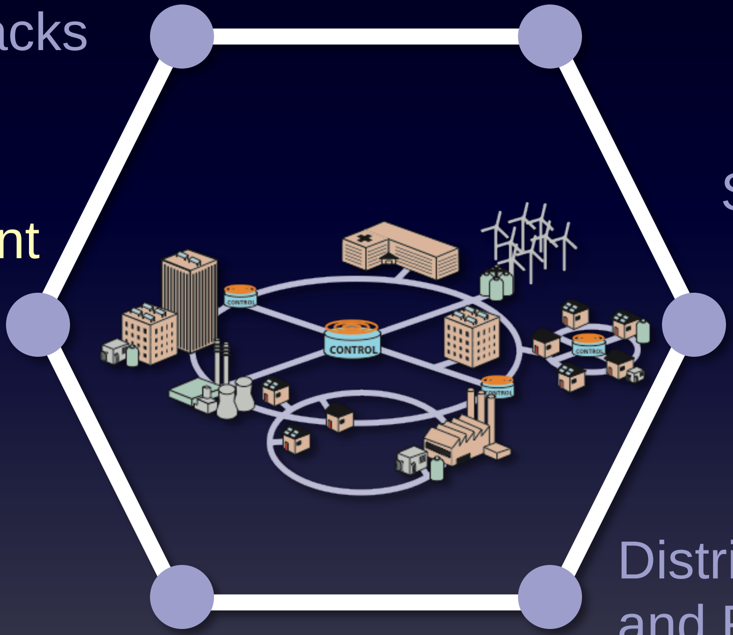
$s_2 = -8\delta_8 + \omega_8$

New England 10-machine 39-bus system



New England 10-machine
39-bus system

Ongoing Research Thrusts



Coordinated Variable-Structure Switching Attacks

Cyber-Physical Co-Simulation

Flocking-Based Multi-agent Power System Protection

Secure Demand Response and Dispatch

Self-Organizing Microgrid Networks

Distributed Control and Resilience of Smart Grid

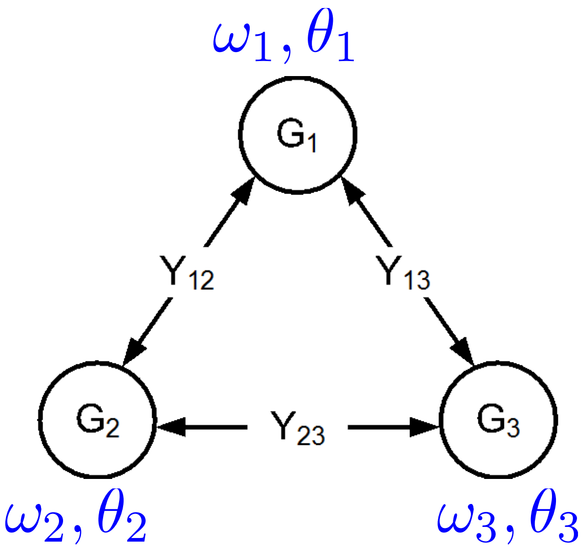
Questions

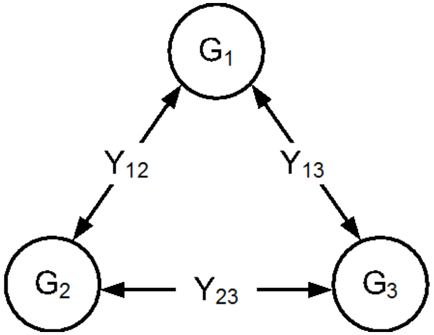
- How can cyber work synergistically with physical?
- How should synchronous machines and DERs cooperate for secure operation?

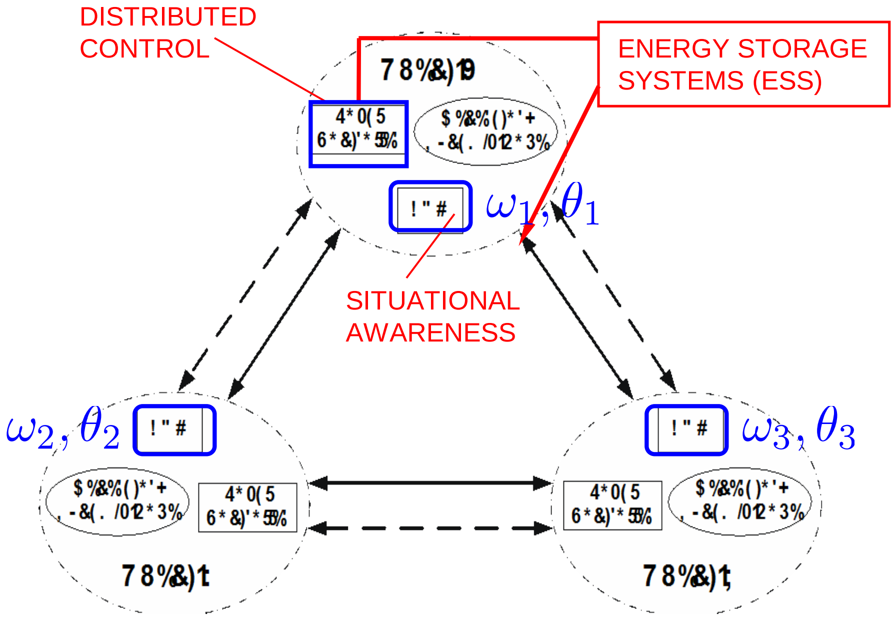
$$M_i\dot{\omega}_i = -D_i\omega_i + P_{m,i} - |E_i|^2 G_{ii} - \sum_{j=1}^{N} |E_i||E_j||Y_{ij}|\sin(\theta_i - \theta_j + \varphi_{ij})$$

$$\begin{aligned} \boldsymbol{\theta} &= [\theta_1\ \theta_2\ \cdots\ \theta_N]^T \\ \boldsymbol{\omega} &= [\omega_1\ \omega_2\ \cdots \omega_N]^T \end{aligned}$$

$$\boxed{\begin{aligned} \dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega}) \end{aligned}}$$







DISTRIBUTED CONTROL

ENERGY STORAGE SYSTEMS (ESS)

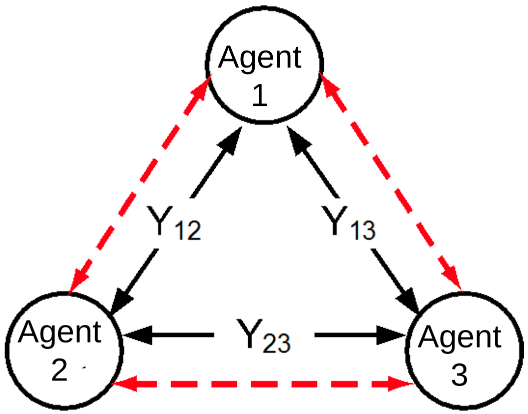
SITUATIONAL AWARENESS

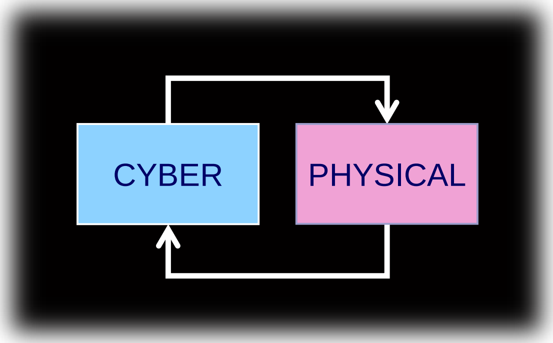
$$\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega}\\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega})\end{aligned}$$

$$\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega}\\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega}) + \boldsymbol{u}\end{aligned}$$

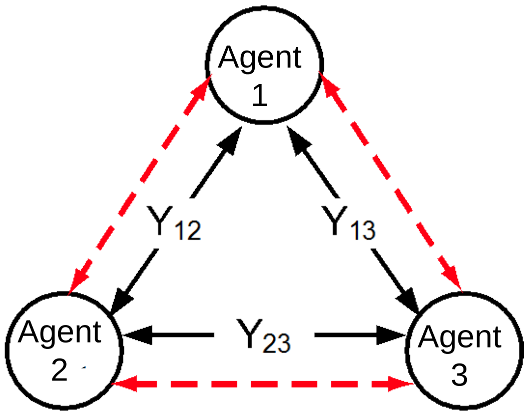
$$\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega}\\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta},\boldsymbol{\omega}) + \boldsymbol{u}\end{aligned}$$

$$M_i\dot{\omega}_i = -D_i\omega_i + P_{m,i} - |E_i|^2 G_{ii} - \sum_{j=1}^{N} |E_i||E_j| \underbrace{|Y_{ij}|}_{\text{physical §}} \sin(\theta_i - \theta_j + \underbrace{\varphi_{ij}}_{\text{physical §}}) + \underbrace{u_i}_{\text{cyber §}}$$





$$\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta},\boldsymbol{\omega}) + \boldsymbol{u}\end{aligned}$$



Transient Stability

Exponential Frequency Synchronization:

$$\underset{\uparrow}{\omega_i}(t) \;\rightarrow\; 0 \text{ as } t \;\rightarrow\; \infty$$

normalized frequency

Phase Angle Cohesiveness:

$$|\theta_i(t) - \underset{\uparrow}{\theta_{COI}}(t)| \;\leq\; \gamma, \;\forall\; t$$

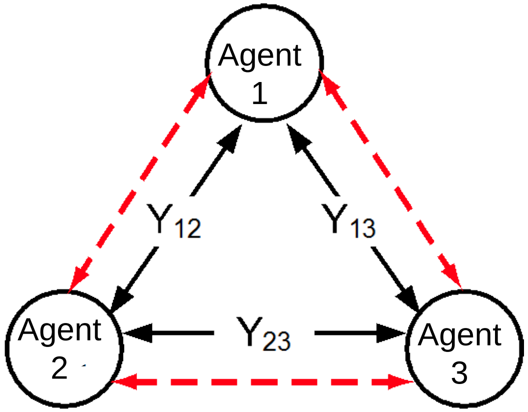
center of inertia

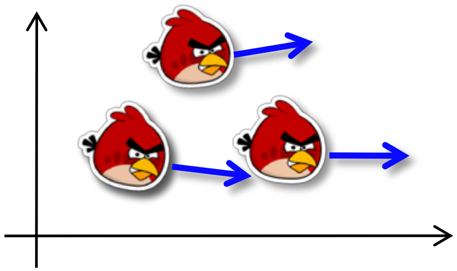
$$\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega}\\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega}) + \boldsymbol{u}\end{aligned}$$

Goal: design $\boldsymbol{u}$ such that:

$$\boldsymbol{\omega} \to \mathbf{0} \text{ as } t \to \infty$$

$$|\boldsymbol{\theta} - \boldsymbol{\theta}_{COI}| \leq \gamma \mathbf{1} \text{ for all } t$$





Flocking

- Aggregate behavior amongst agents to achieve a shared group behavior

Flocking

- Goal seeking
  - Each agent has a desired velocity towards a specified position in global space
- Velocity matching
  - Agents attempt to match velocity of nearby agents
- Flock centering
  - Agents attempt to stay close to nearby neighbors

$$
\begin{aligned}
\dot{\boldsymbol{q}} &= \boldsymbol{p}\\
\dot{\boldsymbol{p}} &= \tilde{\boldsymbol{u}}
\end{aligned}
$$

$\boldsymbol{q}$ - position vector

$\boldsymbol{p}$ - velocity vector

$$
\tilde{\boldsymbol{u}} = \underbrace{\overset{\substack{\text{Goal Seeking}\\ \downarrow}}{-\nabla V(\boldsymbol{q})}}_{\substack{\text{system}\\ \text{objectives}}} - \underbrace{\overset{\substack{\text{Velocity}\\ \text{Matching}\\ \downarrow}}{\mathbf{L}\cdot\boldsymbol{p}}}_{\substack{\text{velocity}\\ \text{consensus}\\ \text{protocol}}} + \underbrace{\overset{\substack{\text{Flock Centering}\\ \downarrow}}{F\left(\boldsymbol{p},\boldsymbol{q},\boldsymbol{p_r},\boldsymbol{q_r}\right)}}_{\substack{\text{navigational}\\ \text{feedback for}\\ \text{tracking}}}
$$

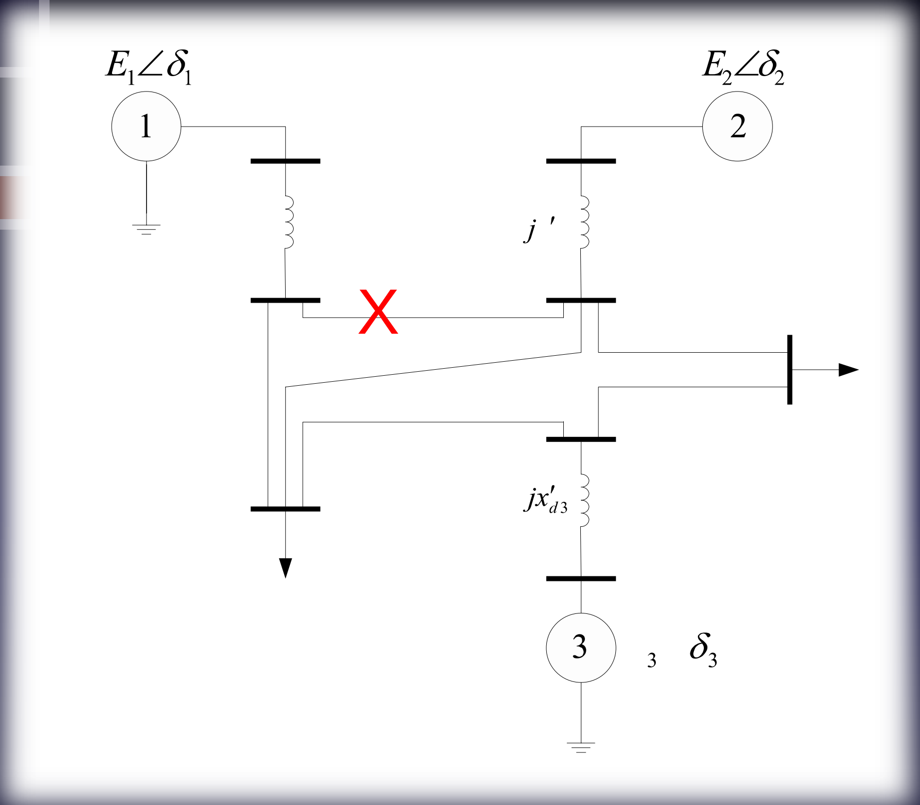
$$
\begin{aligned}
\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega}\\
\dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta},\boldsymbol{\omega}) + \boldsymbol{u} = \tilde{\boldsymbol{u}}
\end{aligned}
$$

$$\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= f(\boldsymbol{\theta}, \boldsymbol{\omega}) + \boldsymbol{u} = \tilde{\boldsymbol{u}}\end{aligned}$$

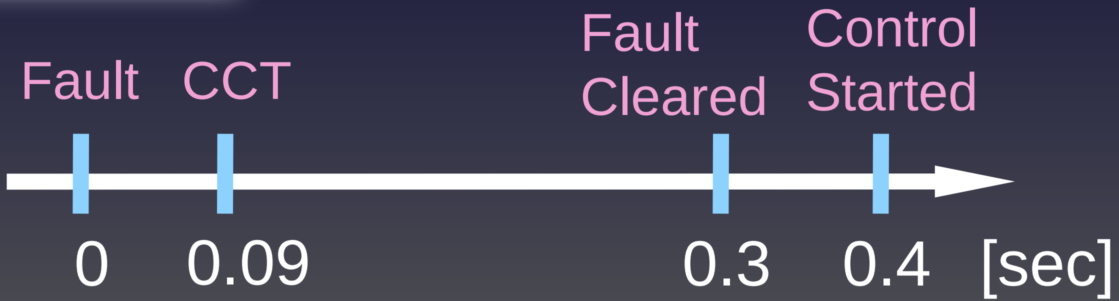
$$\boxed{\begin{aligned}\dot{\boldsymbol{\theta}} &= \boldsymbol{\omega} \\ \dot{\boldsymbol{\omega}} &= \underbrace{-\mathbf{M}^{-1}\nabla V(\boldsymbol{\theta})}_{\text{phase cohesiveness}} - \underbrace{\widetilde{\mathbf{L}}\boldsymbol{\omega} + \mathbf{M}^{-1}F(\boldsymbol{\omega}, \boldsymbol{\omega}_r)}_{\text{frequency synchronization}}\end{aligned}}$$

effective cyber-physical system dynamics

Results

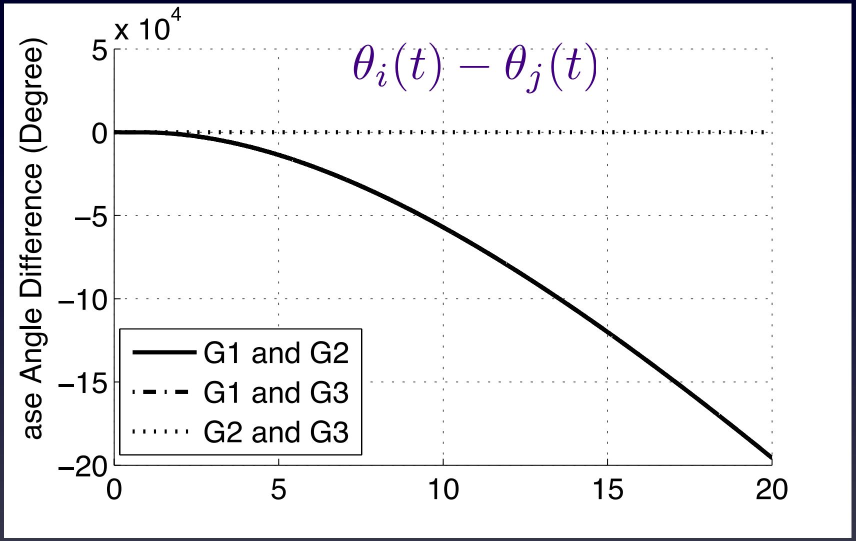


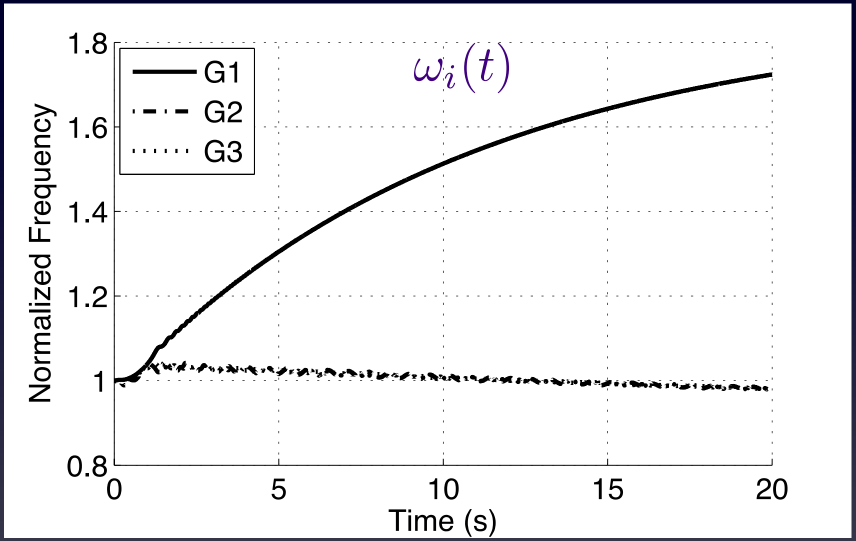
WECC 3-machine system


Fault
CCT
Fault Cleared
Control Started
0
0.09
0.3
0.4
[sec]

Results

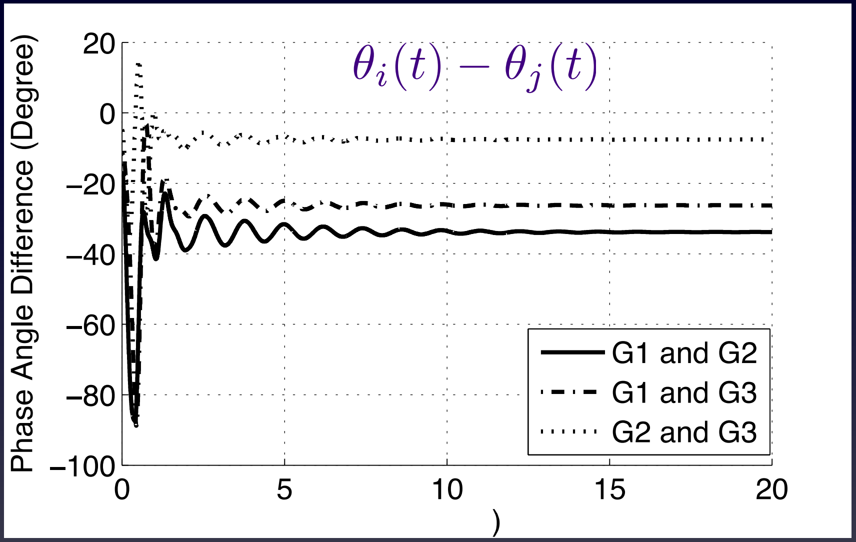
- Breaker opens 0.3 s (CCT = 0.09 s)
- No distributed control.

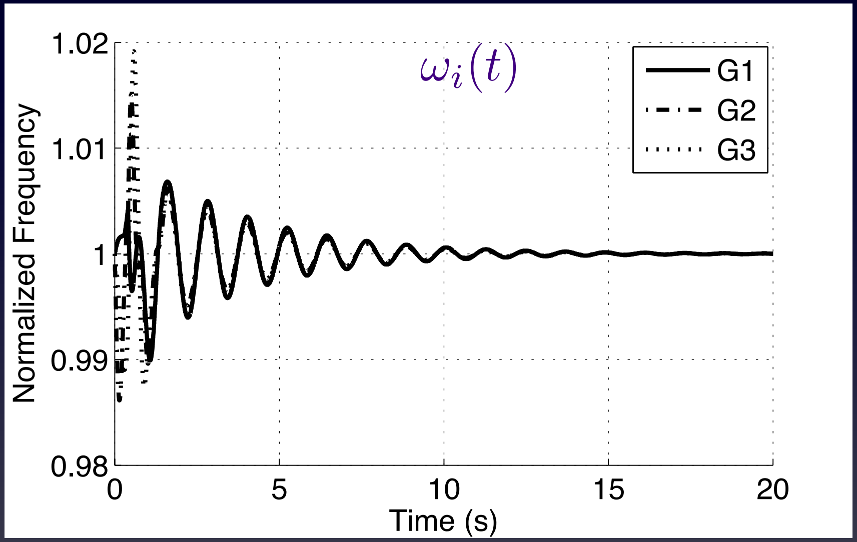




Results

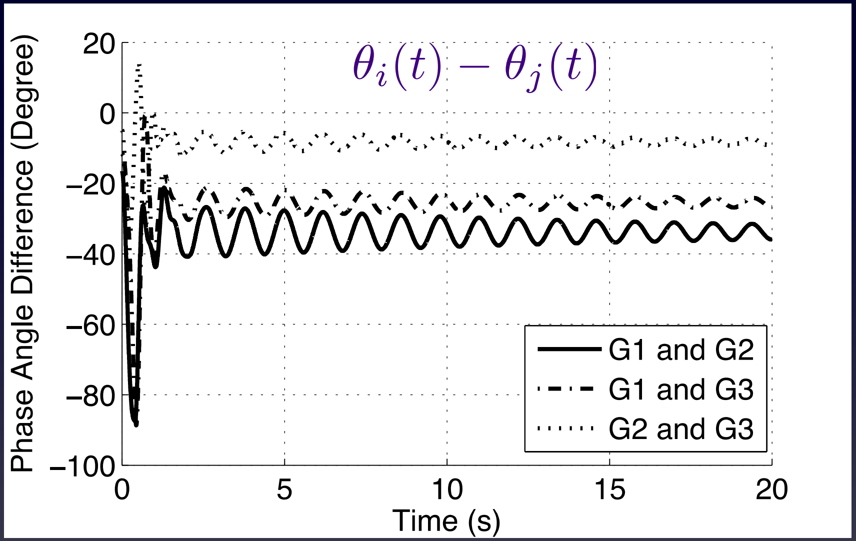
- Breaker opens 0.3 s (CCT = 0.09 s)
- Flocking-based control.

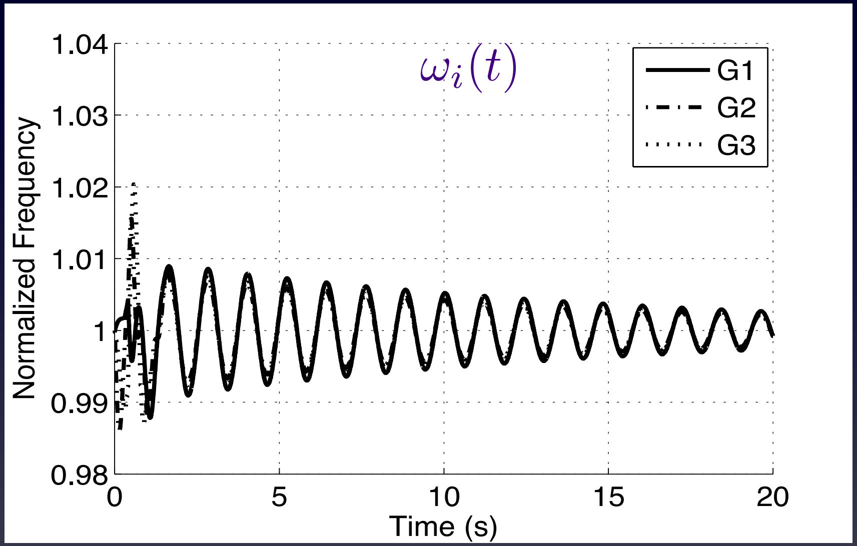




Results

- Breaker opens 0.3 s (CCT = 0.09 s)
- Flocking-based control with 15 ms delay.





Delays above 16 ms, do not stabilize the system.

Resilience to Cyber Attack

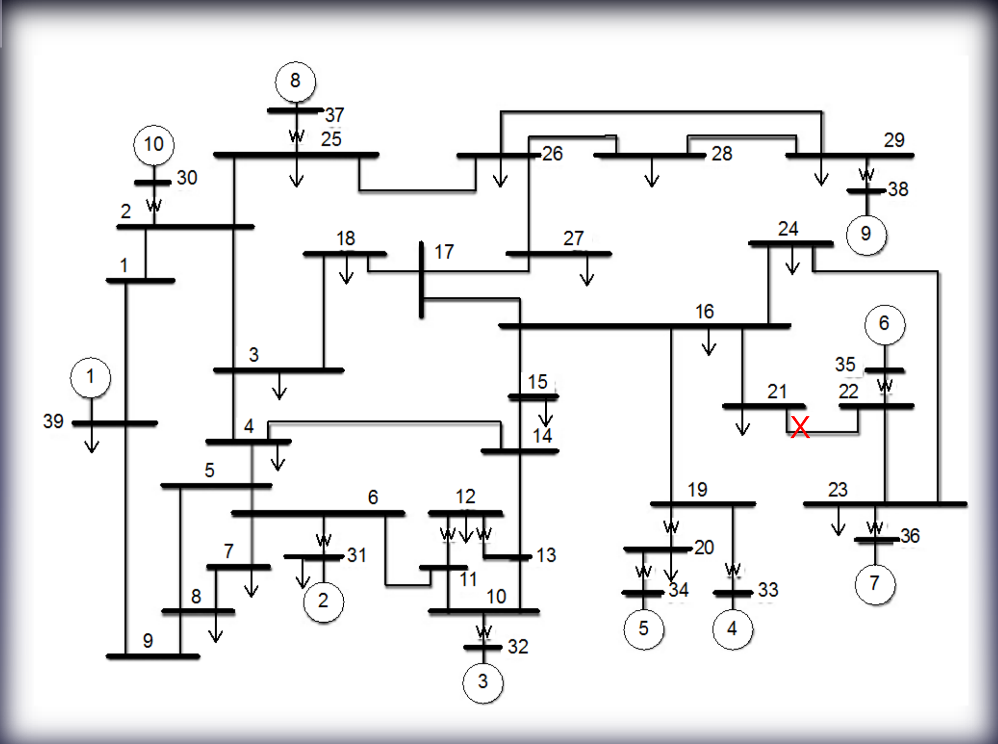
Hierarchy

- Leverage physical couplings to aid in protection
- Cyber-control used selectively where needed

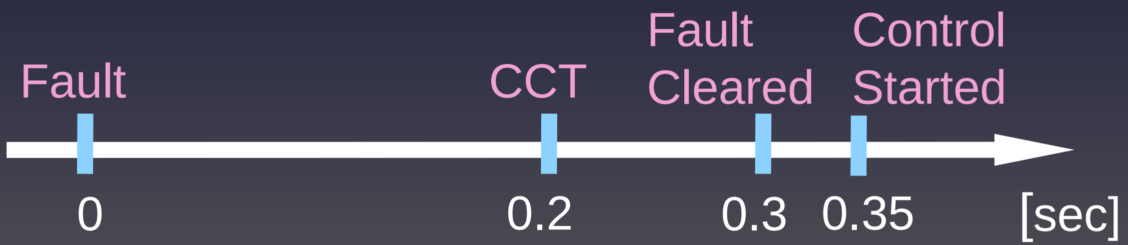
Communications Routing

- Employ flocking-based approach to routing to overcome network DoS
- Network packet = flockmate

Simulations



39-bus New England Test System


Fault

CCT

Fault Cleared

Control Started

0

0.2

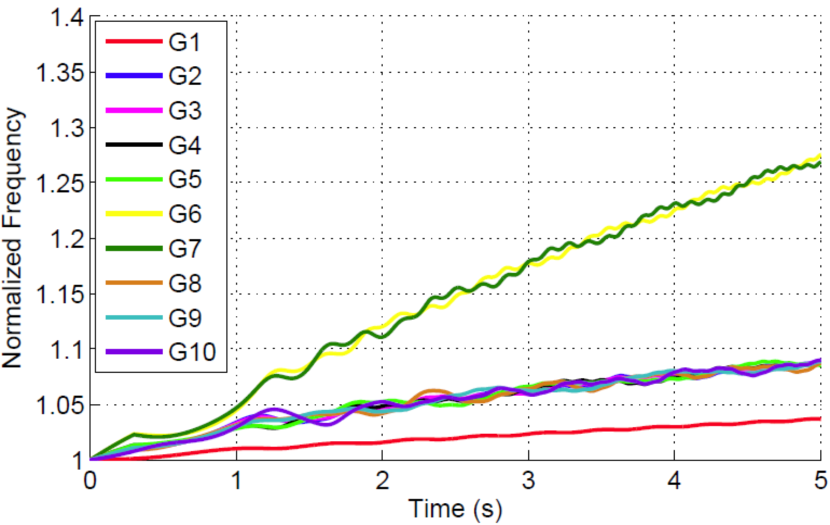
0.3

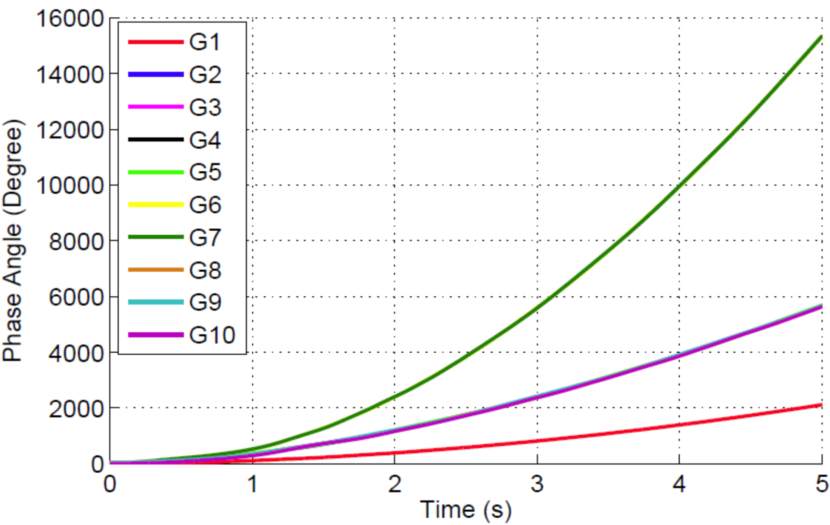
0.35

[sec]

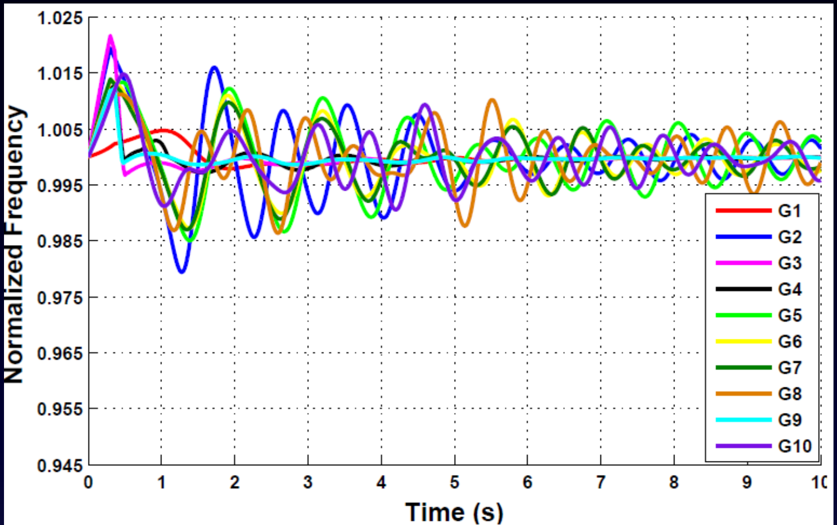
Simulations

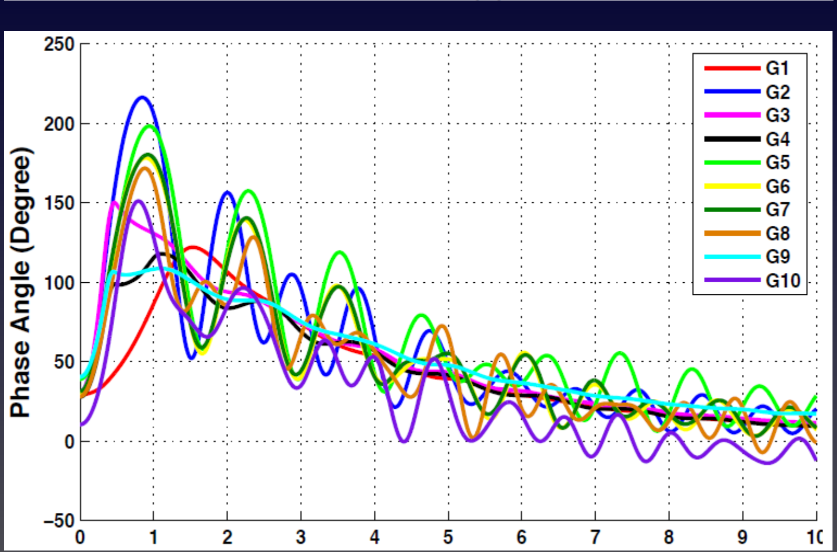
Without flocking control





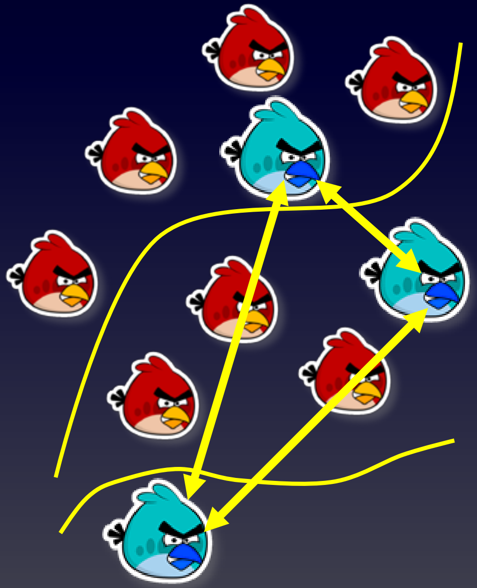
With flocking control



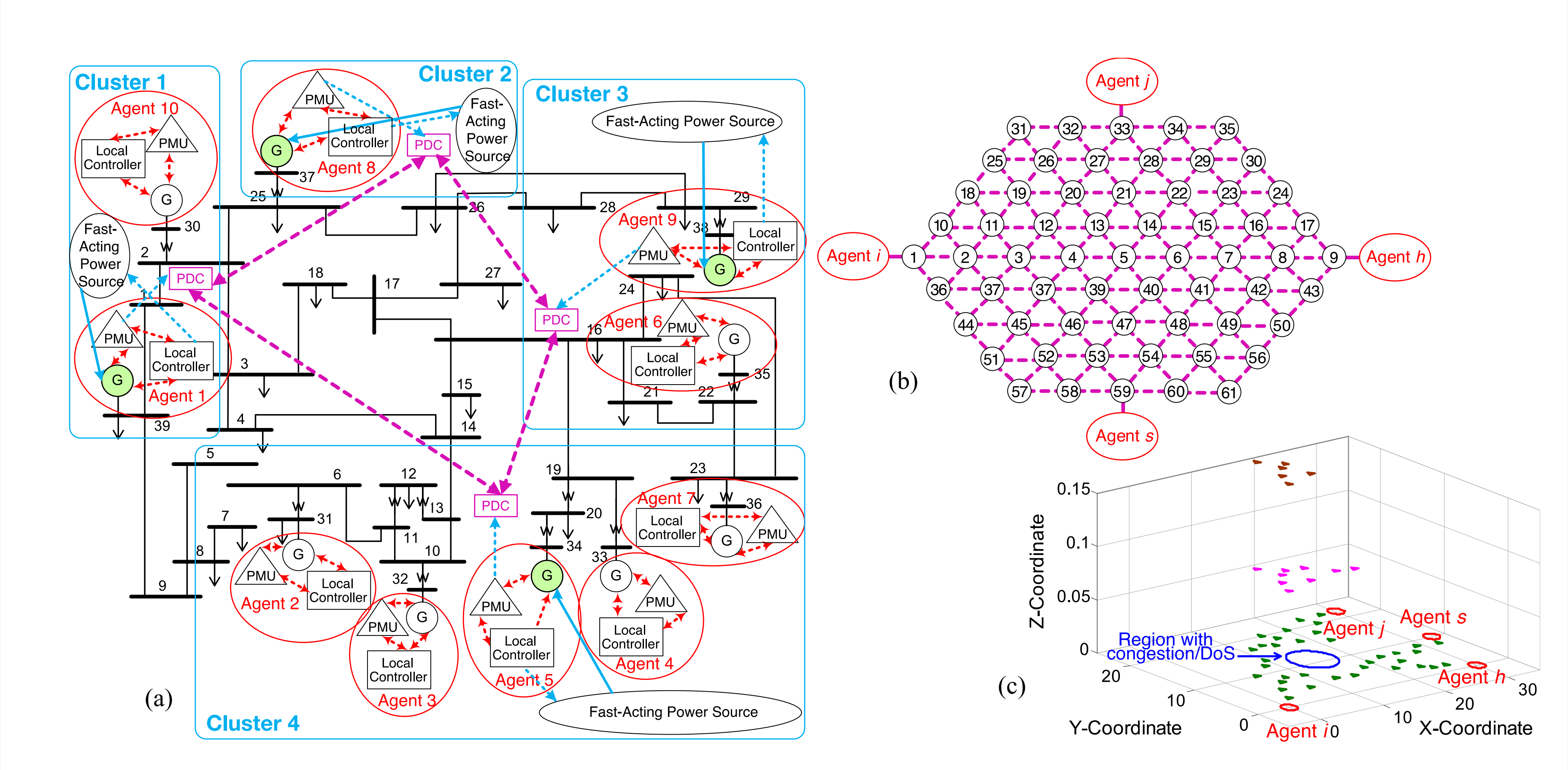


- Analogy (without control)

- Analogy (with control)



What about Information Flow Dynamics?



GOAliE for Communication Routing

- GOAliE: Goal-Seeking Obstacle and Collision Evasion

- Aim: dynamic resilient multi-objective multicast routing

- Approach: flocking-based quality of experience (QoE) routing

Flocking Analogy to Routing

Flocking Principles

- Goal seeking
- Obstacle evasion
- Collision avoidance
- Behavioral transitions

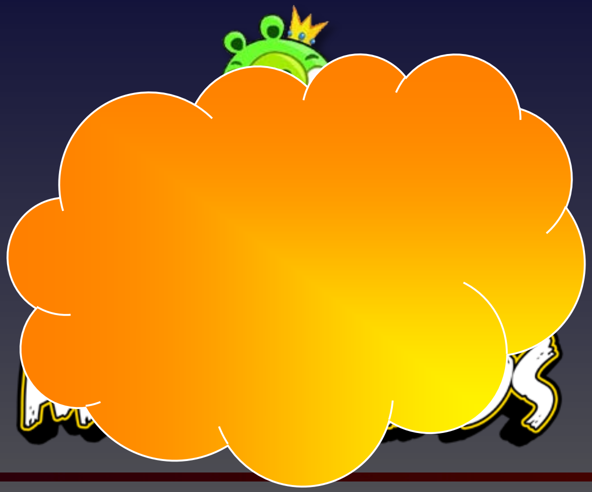
Routing Goals

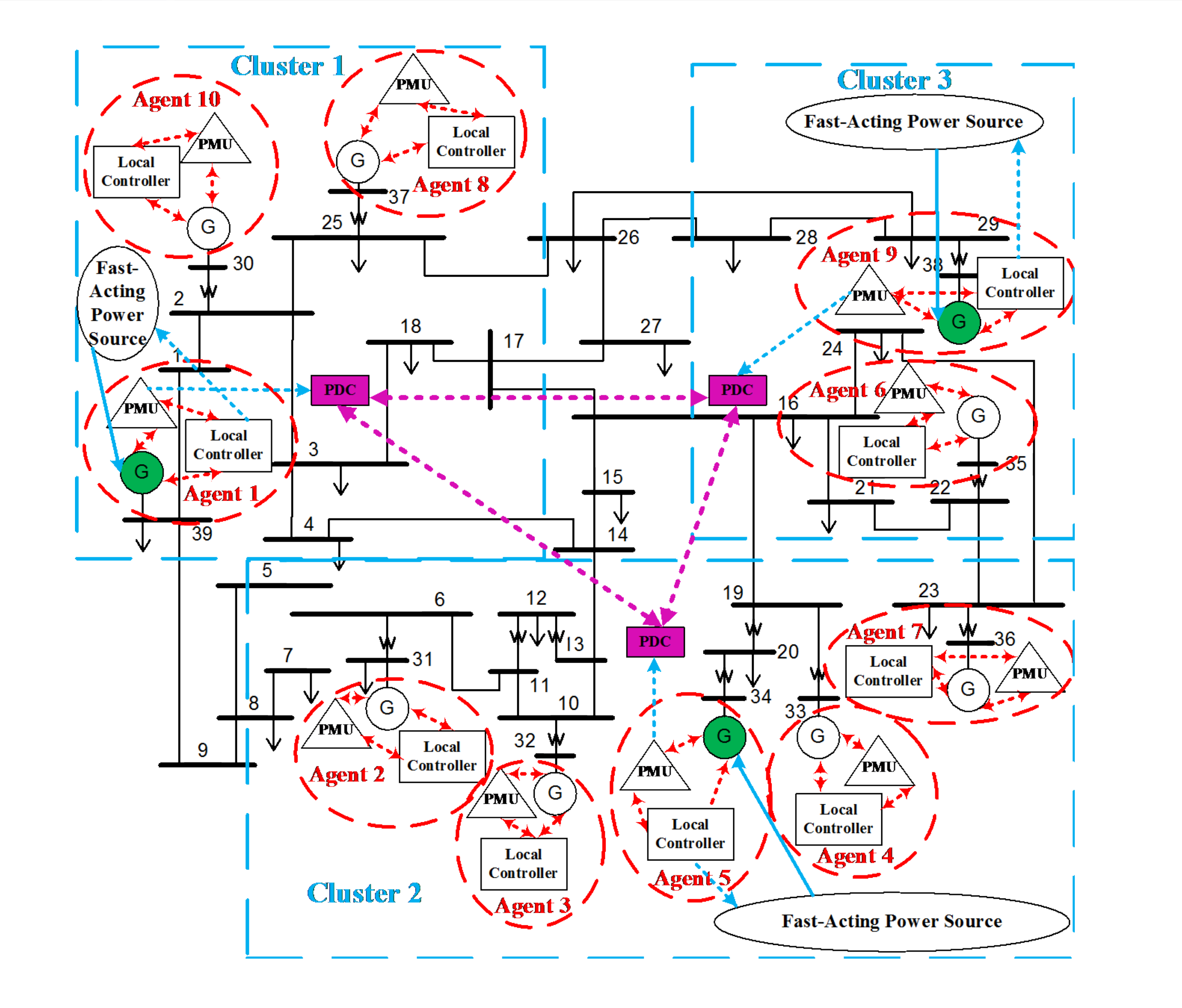
- Low latency
- Buffer overflow management
- Adaptability to changing network conditions

Communication Routing

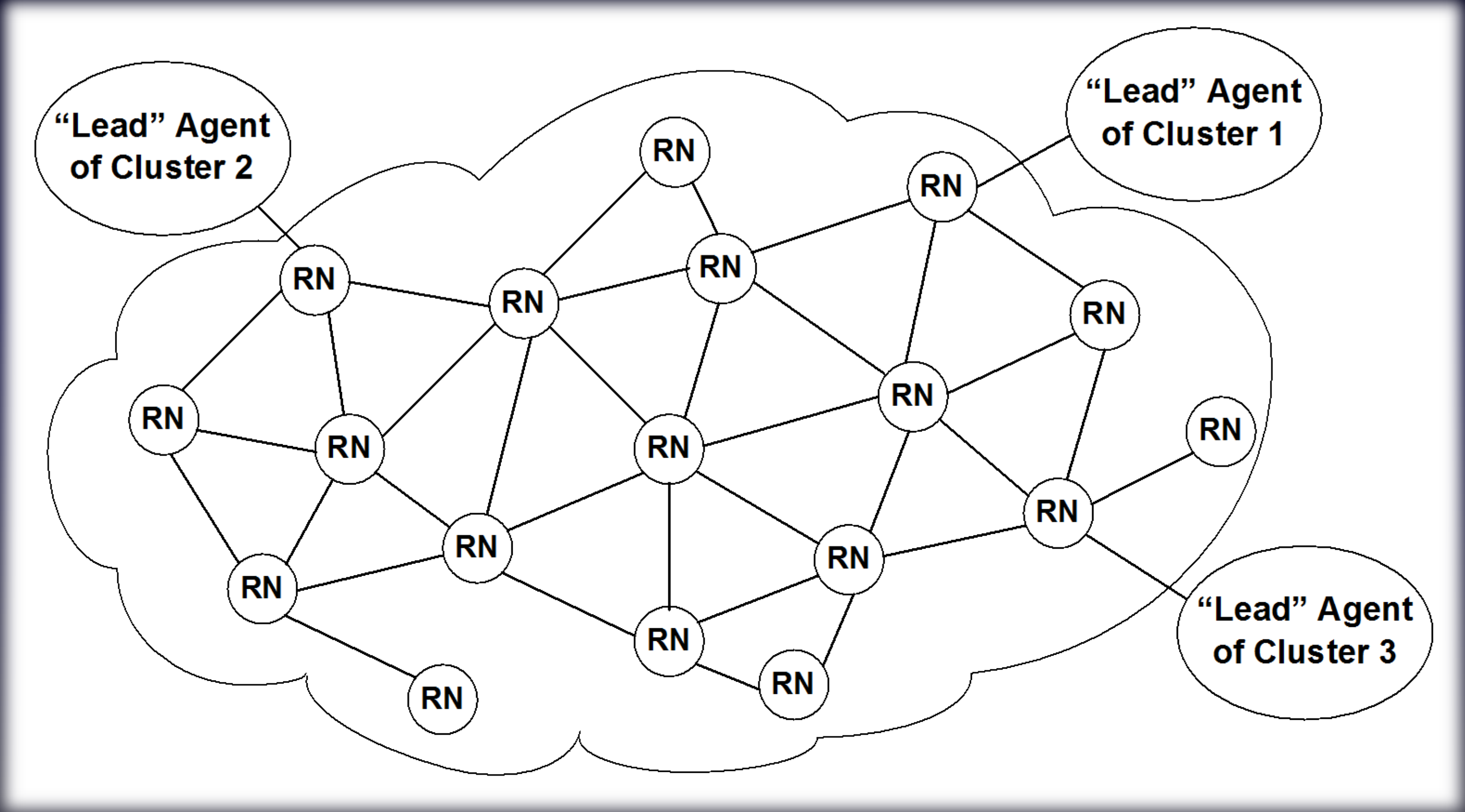
- Goal Seeking:
  - Each agent has a desired velocity toward a specified position in global space.
- Obstacle Evasion:
  - agents avoid obstacles by steering away from approaching their goals
- Collision Avoidance:
  - agents avoid collisions with nearby flockmates
- Behavioral Transitions:
  - the history of an agent's state influences future collective behavior

Intuition: Why obstacle avoidance is a good strategy for network routing.



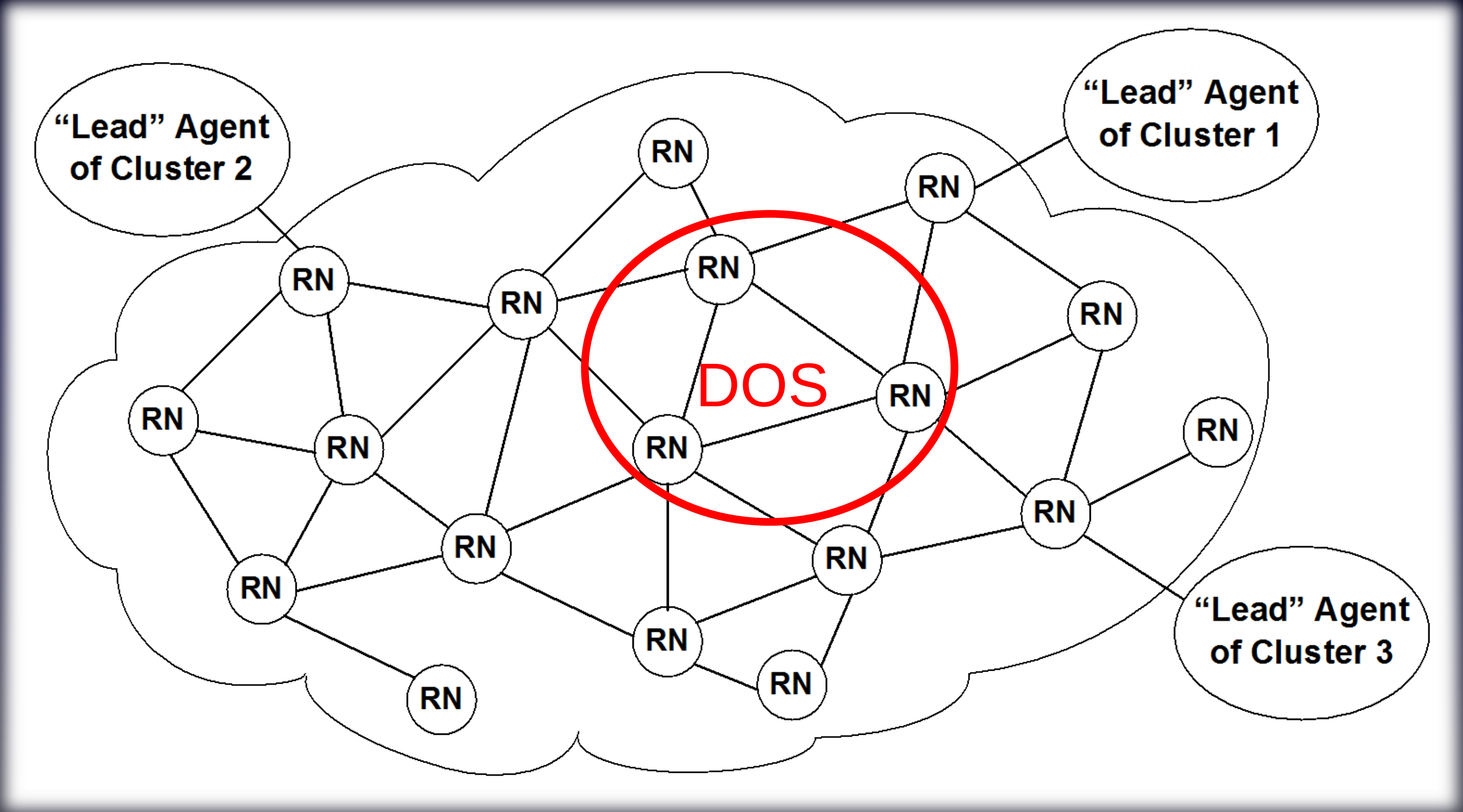

Cluster 1
Agent 10
PMU
Local Controller
G
Agent 8
PMU
Local Controller
G
37
25
30
2
Fast-Acting Power Source
1
PMU
Local Controller
G
Agent 1
39
3
4
PDC
18
17
27
26
28
Cluster 3
Fast-Acting Power Source
29
Agent 9
38
PMU
Local Controller
G
24
PDC
16
Agent 6
PMU
G
Local Controller
21
22
35
15
14
5
6
12
13
7
31
8
11
10
9
PMU
G
Local Controller
Agent 2
32
PMU
G
Local Controller
Agent 3
Cluster 2
PDC
19
20
34
PMU
G
Local Controller
Agent 5
23
Agent 7
36
Local Controller
G
PMU
33
G
PMU
Local Controller
Agent 4
Fast-Acting Power Source

Communication Routing

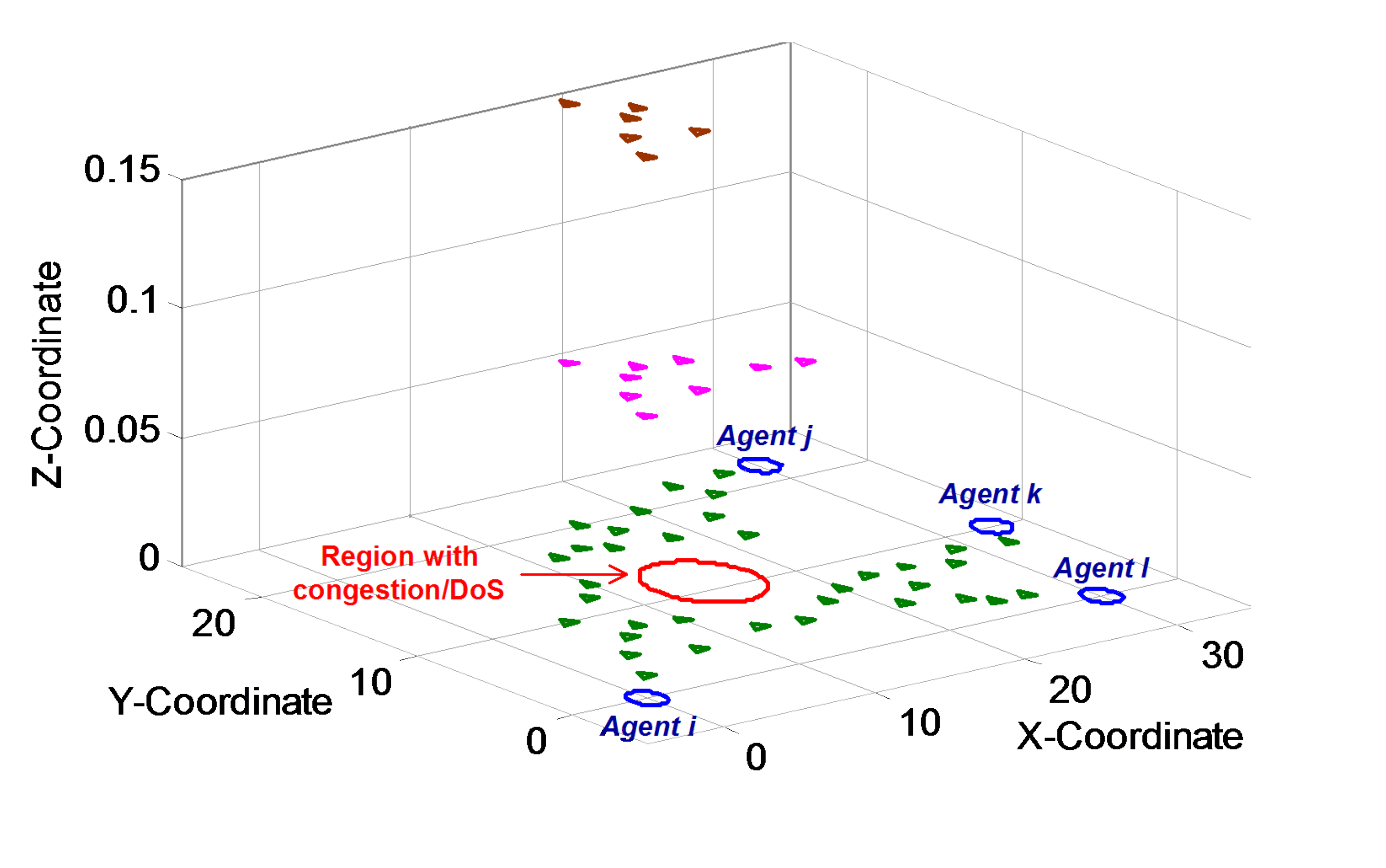


"Lead" Agent of Cluster 2
"Lead" Agent of Cluster 1
"Lead" Agent of Cluster 3
RN

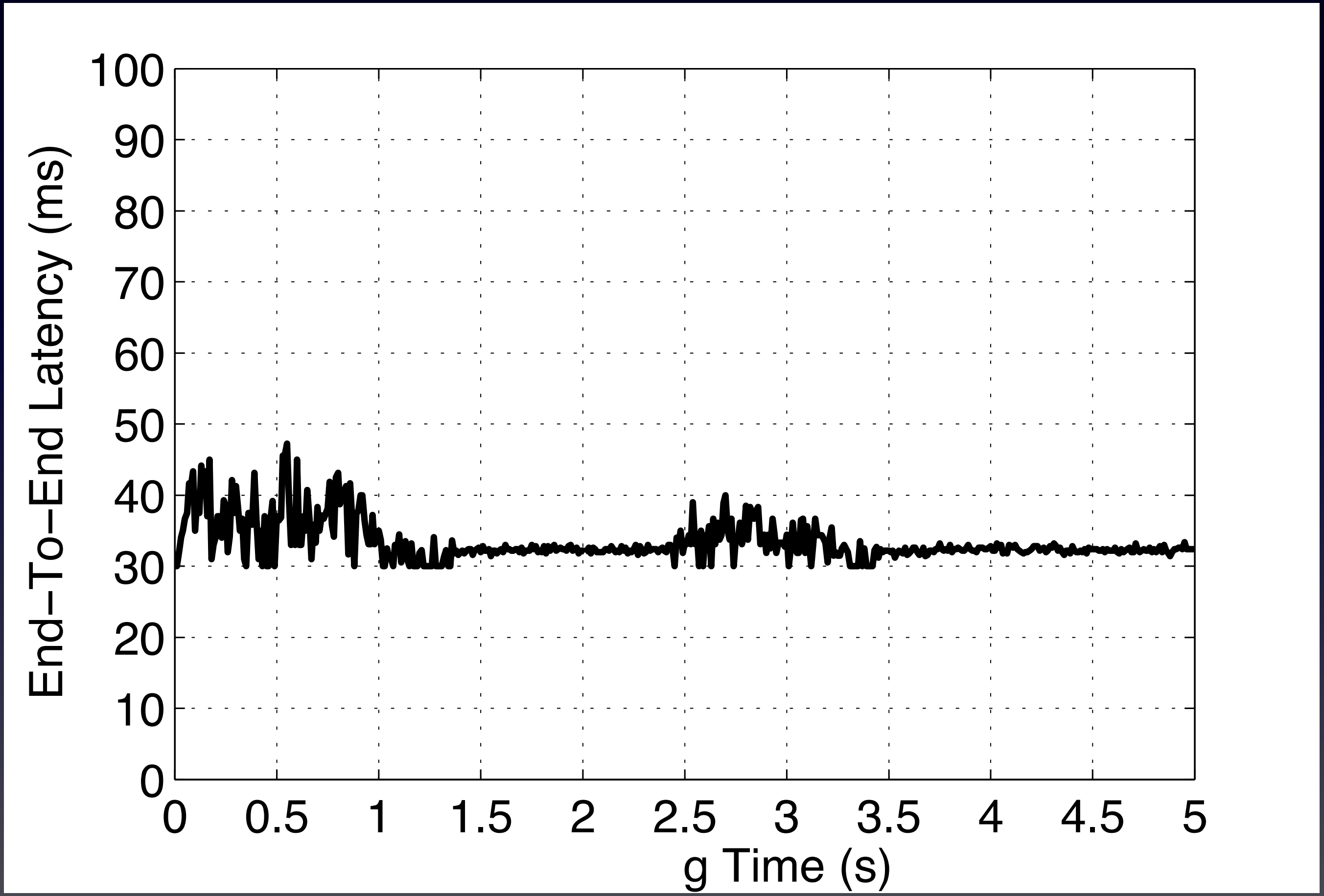
Communication Routing

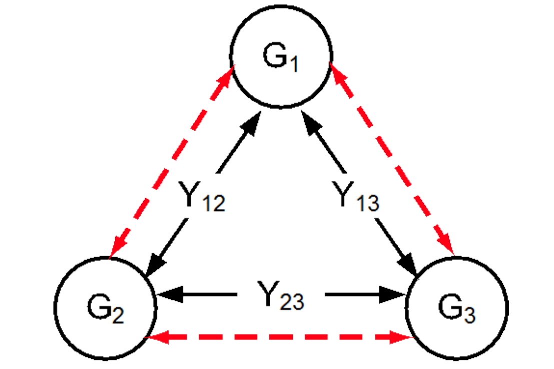

"Lead" Agent of Cluster 2
"Lead" Agent of Cluster 1
"Lead" Agent of Cluster 3
DOS
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN
RN

Multiple Flocks



Adaptability to DoS

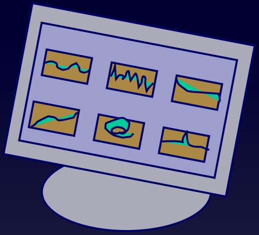


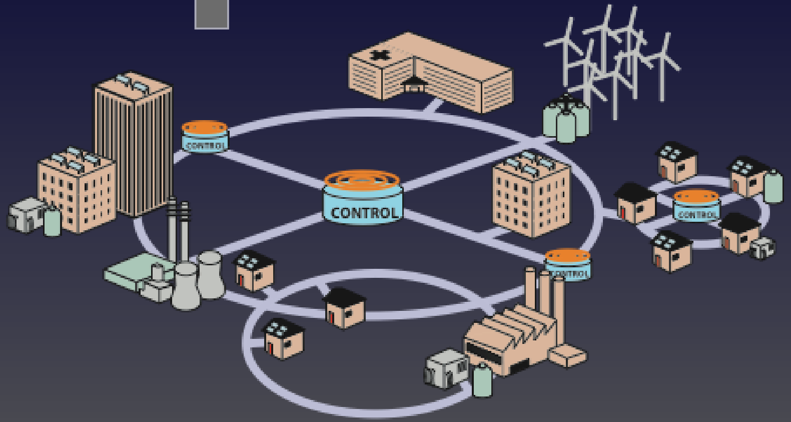


$$\dot{\boldsymbol{\omega}} = f(\boldsymbol{\theta}, \boldsymbol{\omega}) + \boldsymbol{u}$$

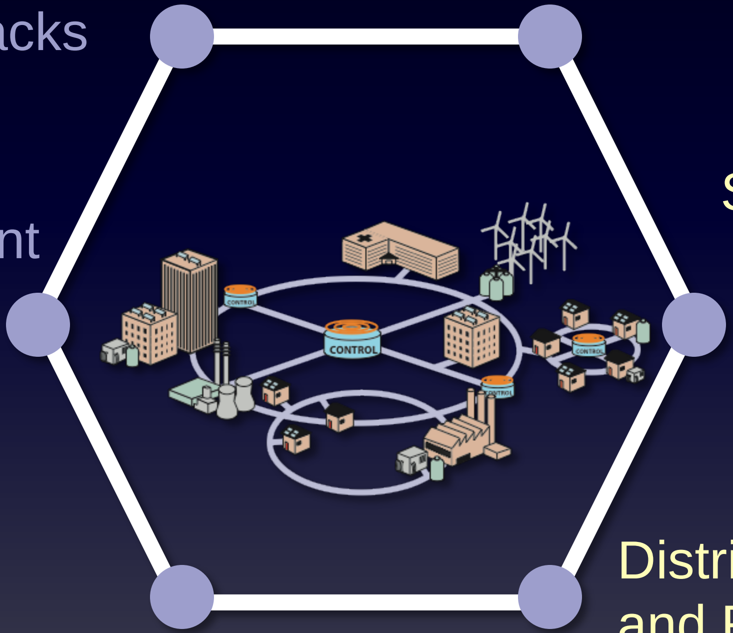
Outcomes

- Distributed control strategies for self-healing.
- Strategies to harness energy storage systems.
- Robust routing strategies.





Ongoing Research Thrusts



Coordinated Variable-Structure Switching Attacks

Cyber-Physical Co-Simulation

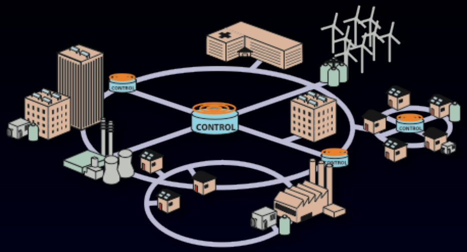
Flocking-Based Multi-agent Power System Protection

Secure Demand Response and Dispatch

Self-Organizing Microgrid Networks

Distributed Control and Resilience of Smart Grid

Final Remarks



- The electric power grid has enormous impact on society. Its improvement will greatly benefit public welfare.
- Smart grid represents a rich and challenging case study to craft CPS analysis and synthesis tools.
- Validation of CPS principles on the smart grid will enable translations to other systems.

Transferability to Other Cyber-Physical Systems

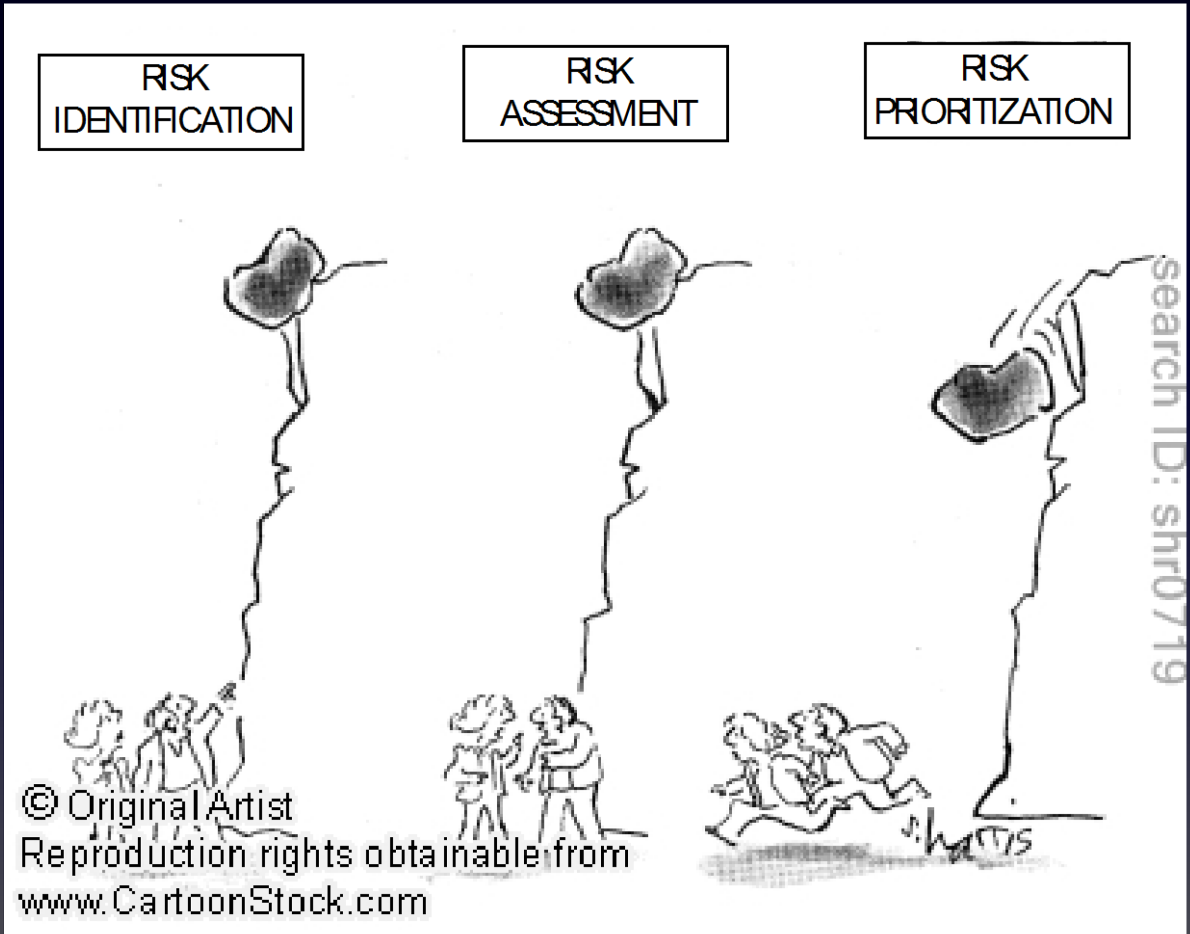
- Autonomous transportation systems
- Medical monitoring
- Distributed robotics
- Industrial control systems

... smart city

Future Directions

- Apply principles of cyber-physical resilient design to a variety of new contexts
- Include models of human decision-making
- Investigate the use of social networking in influencing cyber-physical systems and their security

Closing Senitment



Contact

Dr. Deepa Kundur

Professor

Department of Electrical & Computer Engineering

University of Toronto

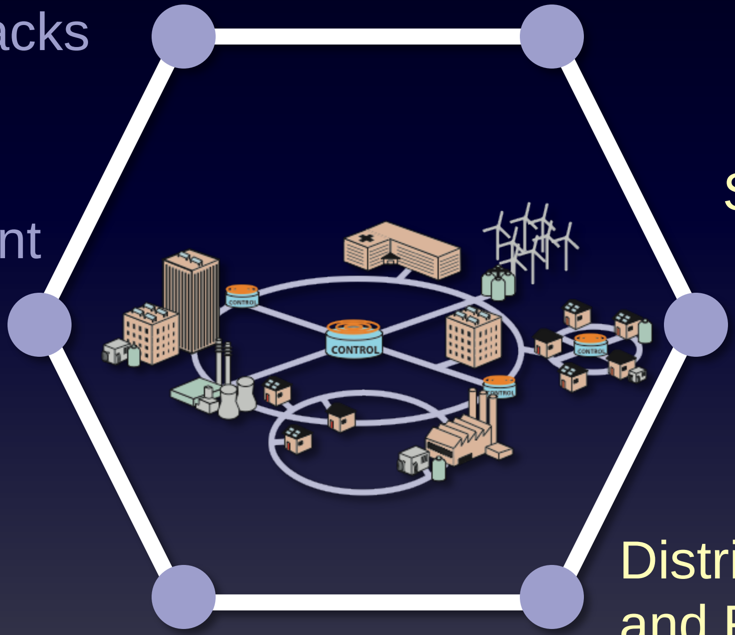
dkundur@comm.utoronto.ca

http://www.comm.utoronto.ca/~dkundur/

Questions?

Acknowledgements:
Joint work with
Jin Wei
Abdallah Farraj
Eman Hammad
Pirathayini Srikantha
Mellitus Ezeme
Joseph Dongchan Lee
Jinjing Zhao
Karen Butler-Purry

Ongoing Research Thrusts



Coordinated Variable-Structure Switching Attacks

Cyber-Physical Co-Simulation

Flocking-Based Multi-agent Power System Protection

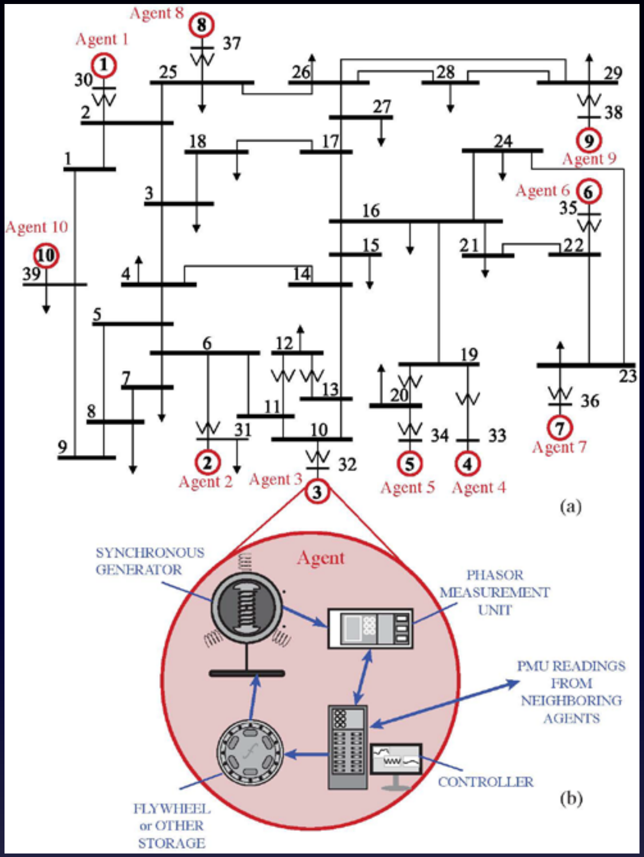
Secure Demand Response and Dispatch

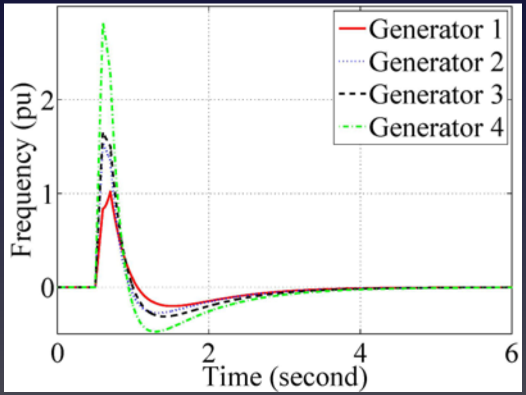
Self-Organizing Microgrid Networks

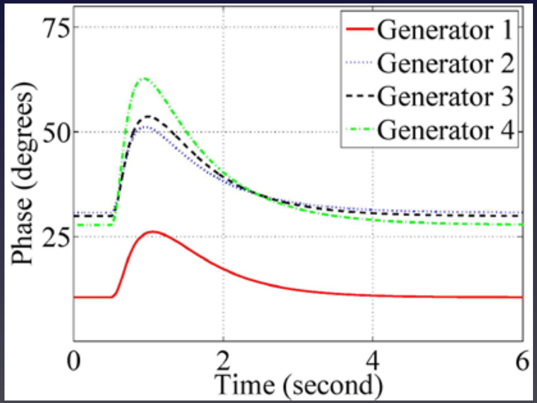
Distributed Control and Resilience of Smart Grid

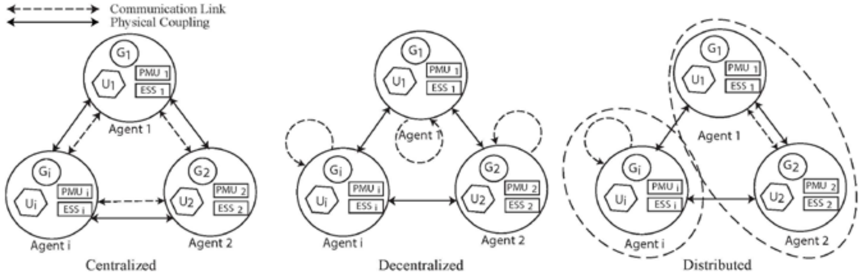
Distributed Control and Resilience of Smart Grid

- **Problem:** Enhance resilience of power systems in the face of severe faults, reconfiguration attacks and time delays from denial-of-service attacks.
- **Challenges:** Providing sufficient time to detect and appropriately react to an attack.
- **Approach:** Utilize storage devices to inject artificial inertia into the grid.
- **Impact:** Provide system operators more time to isolate and react to disturbances.



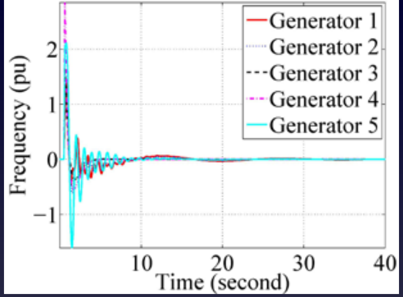




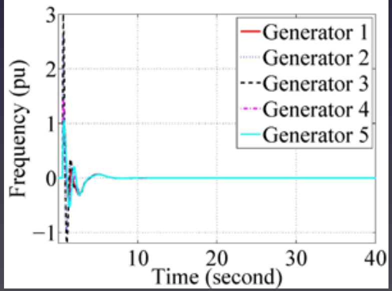


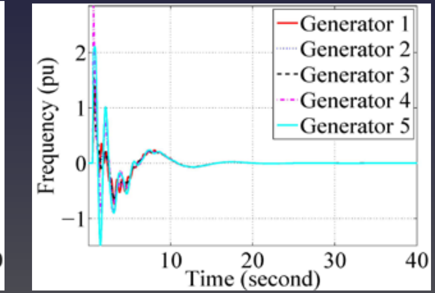
Control Architectures

- **Problem:** Efficient and cyber-secure resilient control.
- **Challenges:** Efficiency, stability time, cyber and cyber-physical attacks, complexity.
- **Approach:** Centralized/decentralized, distributed and hierarchical control architectures.
- **Impact:** Control architectures that are capable to actively respond to cyber attacks and cyber-physical disturbances.



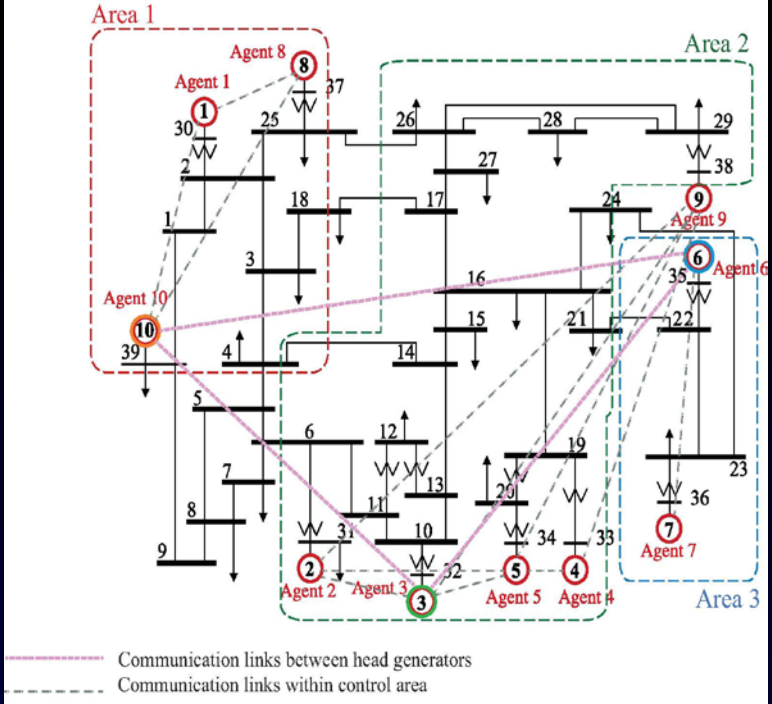
- *Demonstrate the performance of different control architectures against cyber/physical and cyber attacks.*
- *Results shown for low complexity parametric feedback linearization control utilizing storage.*

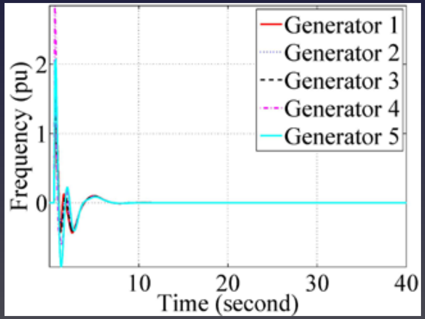


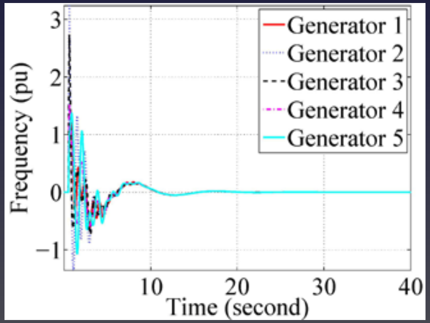


Control Area Design

- Problem: Optimize the performance of distributed control schemes by harnessing cyber-physical coupling.
- Challenges: Efficiency, stability time, cyber and cyber-physical attacks, complexity.
- Approach: Spectral graph theory.
- Impact: Design control areas with best performance of different control architectures.

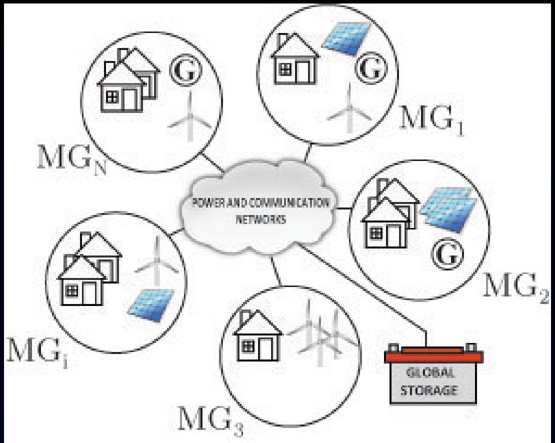




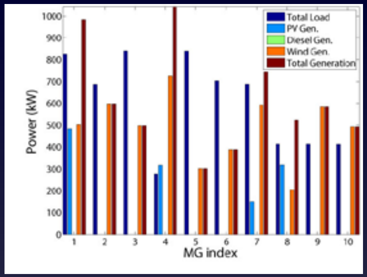


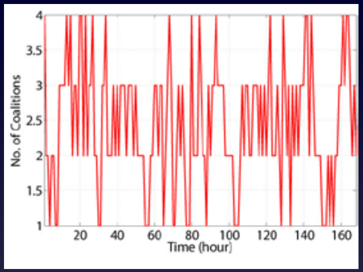
- *Demonstrate the control area design effect on the performance of various control architectures.*
- *Exploratory analysis based on the New England 39 Bus system, need to verify on IEEE 140 bus system.*

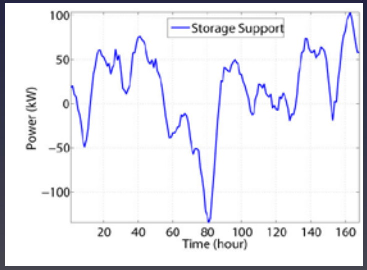
Microgrid Networks (MGNs)

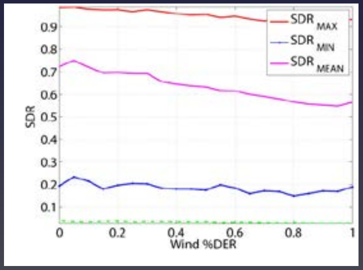


- Problem: Alternative Power Delivery.
- Challenges: Renewable resources, autonomous sustainable operation, cyber-security, resilience.
- Approach: Cooperative game theory.
- Impact: Results in resilient sustainable communities with best utilization of renewable and intermittent resources.







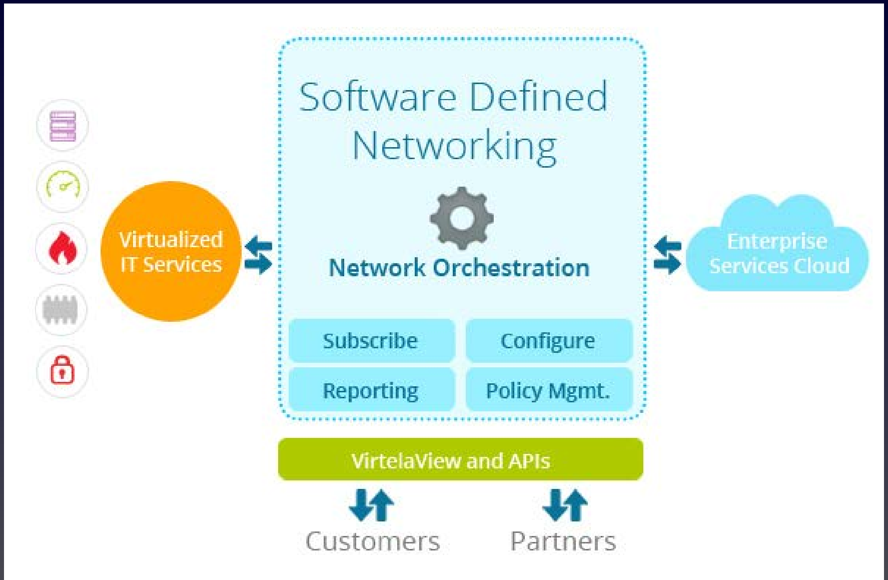


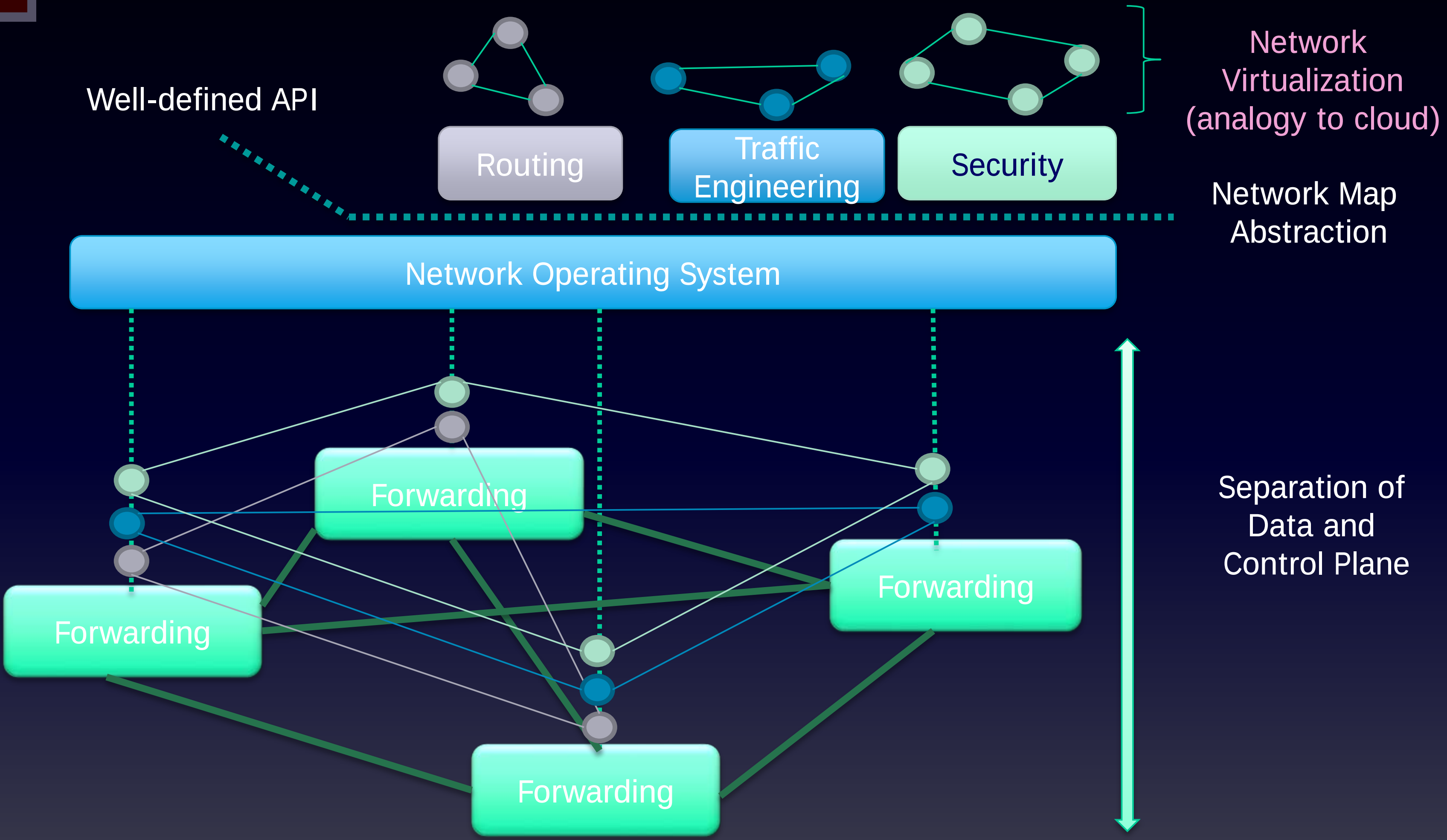
- *Demonstrate the benefits of employing cooperative model for off-Grid microgrid networks, specially for high penetration levels of renewable DERs.*
- *Provide insights into the dynamics and security of cooperation, dependency on the storage, and capacity limits of the storage needed for different penetration levels and different wind generation percentages.*

Security in SDN for Smart Grid

- Problem: Adaptive state-dependent routing protocol that balances between security and performance.
- Challenges: Traditional routers (using BGP, OSPF) cannot select forwarding paths dynamically; varying link vulnerability level.
- Approach: Software defined networking (SDN).
- Impact: Improved security that accounts for diversity of smart grid communication infrastructure.

- Decoupling of control and data planes.
- Dynamic, manageable, cost-effective, and adaptable architecture.
- Logically centralized control to facilitate threat monitoring across network.
- Granular, dynamic and adjustable policy management account for varying threats.
- Flexible path management to achieve rapid containment and isolation of intrusions.





Well-defined API

Routing

Traffic Engineering

Security

Network Virtualization (analogy to cloud)

Network Map Abstraction

Network Operating System

Forwarding

Forwarding

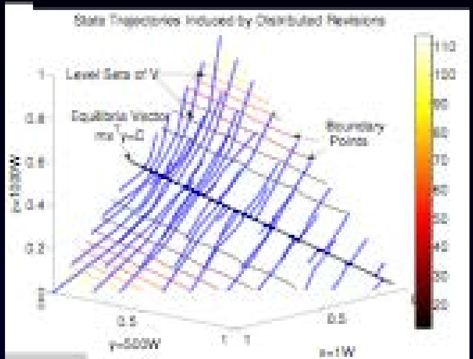
Forwarding

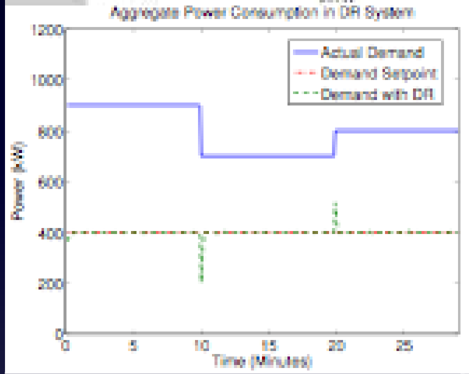
Forwarding

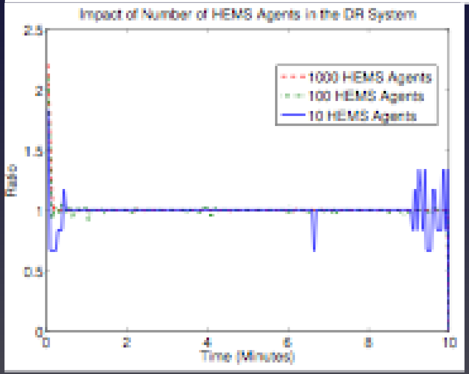
Separation of Data and Control Plane

Secure Demand Response

- Distributed demand response (DR) schemes can manage power consumption in a secure (no single point of failure), robust (agents can adapt to attacks) and real-time manner
  - Our recent work:
    - A Novel Evolutionary Game Theoretic Approach to Real-Time Distributed Demand Response
- Problem: DR schemes rely on aggregates taken on a vast amount of consumption data that are typically obtained from smart meters
- Challenges: Need to process vast amount of data at small timescales and protect highly revealing smart meter data
- Approach: Leverage cloud services and homomorphic encryption techniques (aggregation of cipher text)
- Impact: Cloud provides scalable resources. No need to decrypt data on the cloud (cloud providers will not have access to data). Allows for secure communication and storage.

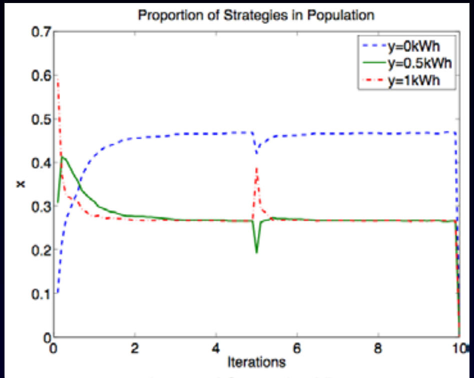


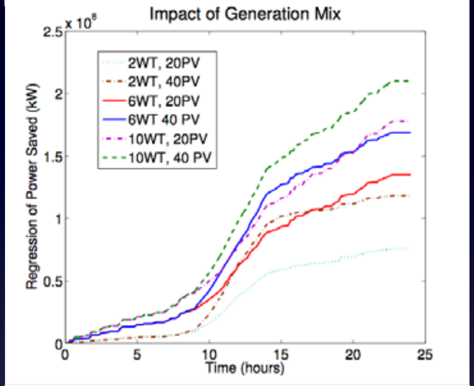


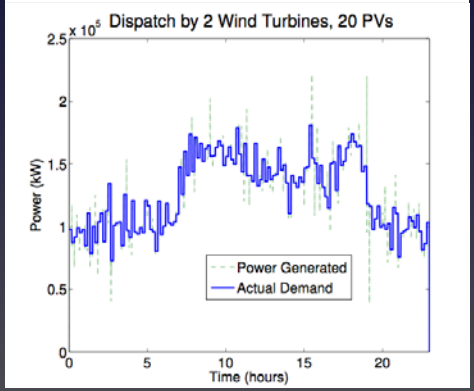


Secure Renewable Dispatch

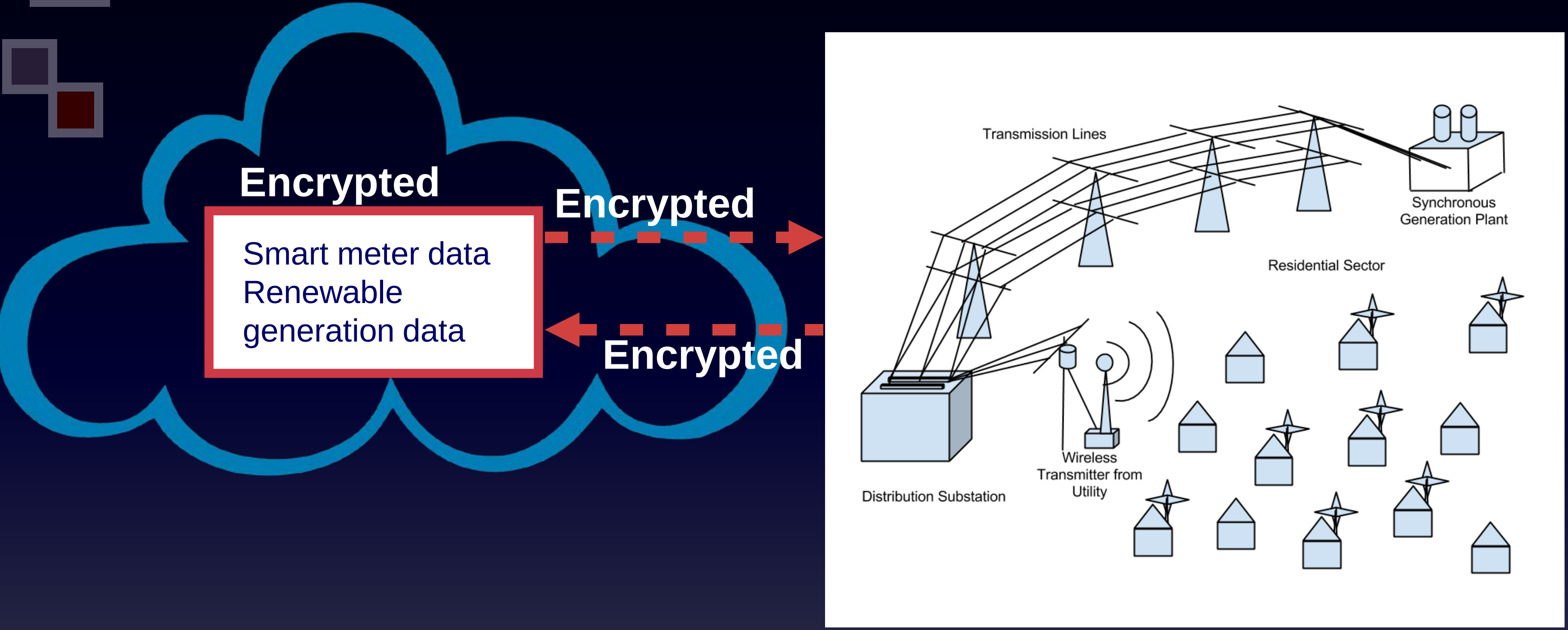
- Distributed dispatch schemes can manage power generation of a large number of small scale generation sources (reduce dependency on the grid)
  - Our recent work:
    - Distributed Optimization of Dispatch in Sustainable Generation Systems via Dual Decomposition
    - Distributed Sustainable Generation Dispatch via Evolutionary Games
    - Dispatch of Sustainable Generation Sources via Bifurcation Controls
- Problem: Similar to DR, dispatch schemes rely on aggregates taken on a vast amount of generation and consumption data
- Challenges: Need to process vast amount of data at small timescales and protect highly revealing smart meter data
- Approach: Leverage cloud services and homomorphic encryption techniques (aggregation of cipher text)
- Impact: Cloud provides scalable resources. No need to decrypt data on the cloud (cloud providers will not have access to data). Allows for secure communication and storage.







Cloud and Homomorphic Encryption



Encrypted

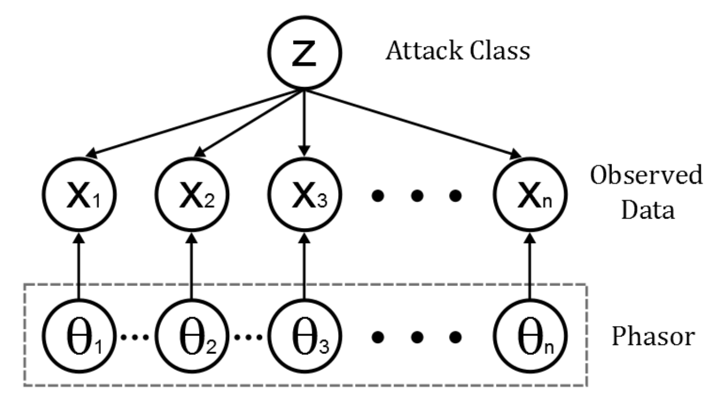
Smart meter data
Renewable
generation data

Encrypted

Encrypted

False Data Detection using Machine Learning

- Problem: Detection of false data injection in PMU measurements.
- Challenges: Difficult to detect if opponent has access to multiple PMU data, Finding model to distinguish bad data from normal operation.
- Approach: Unsupervised machine learning; expectation maximization (EM) algorithm.
- Impact: Enables filtering of potentially corrupt data; system operators will have confidence levels of state estimates.



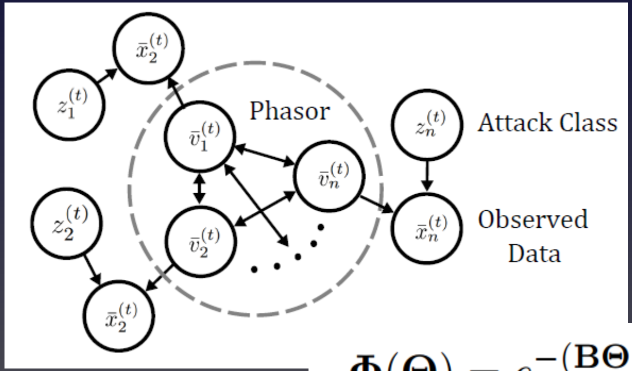
False Data Detection using Machine Learning

Methodology

1. Compute probability of observation.
2. Compute the expectation, and iteratively update the probability of attack to maximize the expectation.

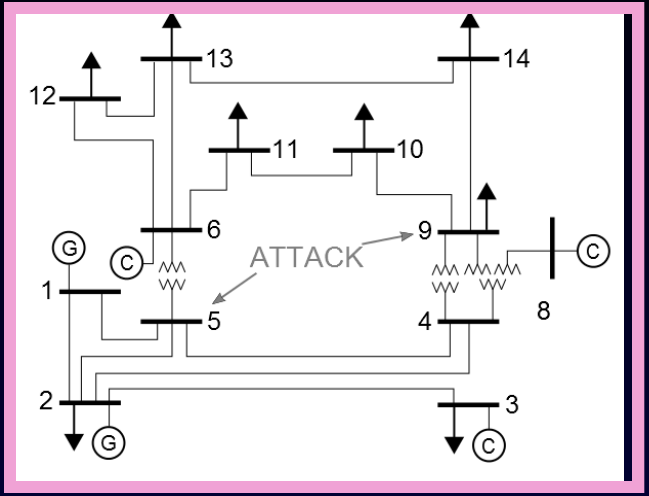
$$E[z_i|x_i,\theta_i^{(t)}] = \frac{\pi_i(\theta_{i,max}-\theta_{i,min})^{-1}}{\pi_i(\theta_{i,max}-\theta_{i,min})^{-1}+(1-\pi_i)\mathcal{N}(x_i|\theta_i,\sigma_i^2)} \quad (14)$$

$$\pi_i^* = \sum_{k=1}^{m} p(z_i|x_i,\gamma_i)\,, \quad \theta_i^{k,*} = \frac{b_i^k + (1-E[z_i^k|x_i^k,\theta_i^{k,(t)}])\frac{x_i^k}{\sigma_i^{k\,2}}}{2a_i^k + \frac{(1-E[z_i^k|x_i^k,\theta_i^{k,(t)}])}{\sigma_i^{k\,2}}} \quad (15{,}16)$$

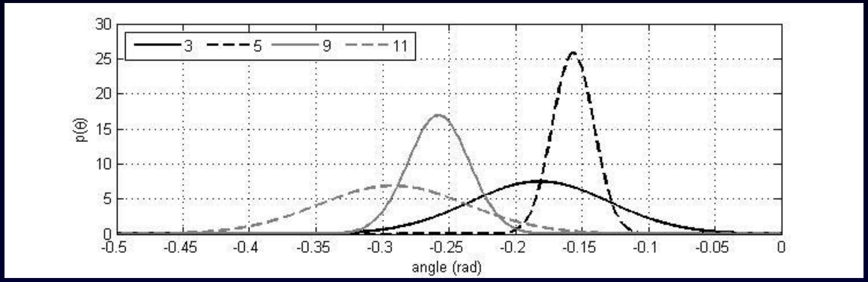


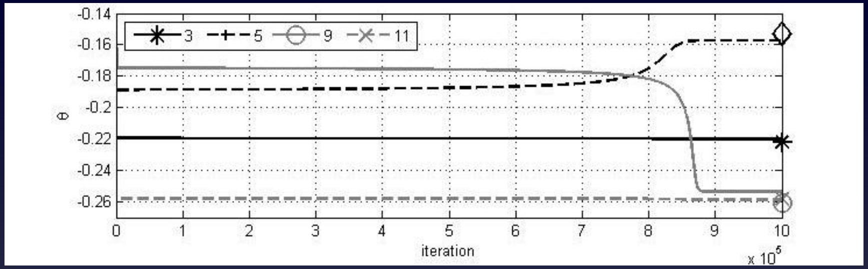
Use governing physics for MAP detection prior function.

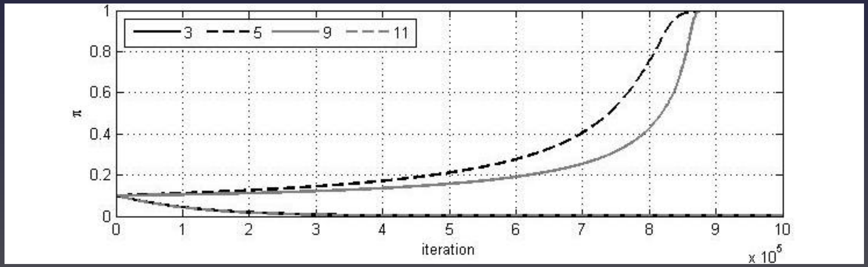
$$\Phi(\Theta) = e^{-(\mathbf{B}\Theta-\mathbf{P}_{inj})^{\intercal}\Sigma_{\Phi}^{-1}(\mathbf{B}\Theta-\mathbf{P}_{inj})}$$


13
14
12
11
10
6
9
ATTACK
G
C
1
5
4
8
C
2
3
G
C

Results


3
5
9
11
p(θ)
30
25
20
15
10
5
0
-0.5
-0.45
-0.4
-0.35
-0.3
-0.25
-0.2
-0.15
-0.1
-0.05
0
angle (rad)

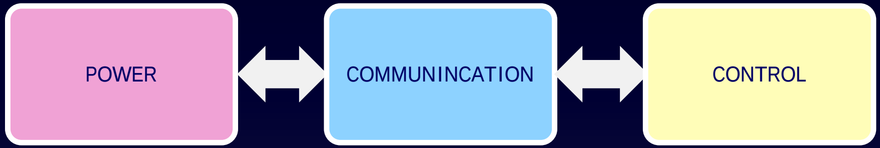

3
5
9
11
θ
-0.14
-0.16
-0.18
-0.2
-0.22
-0.24
-0.26
0
1
2
3
4
5
6
7
8
9
10
iteration
x 10^5


3
5
9
11
π
1
0.8
0.6
0.4
0.2
0
0
1
2
3
4
5
6
7
8
9
10
iteration
x 10^5

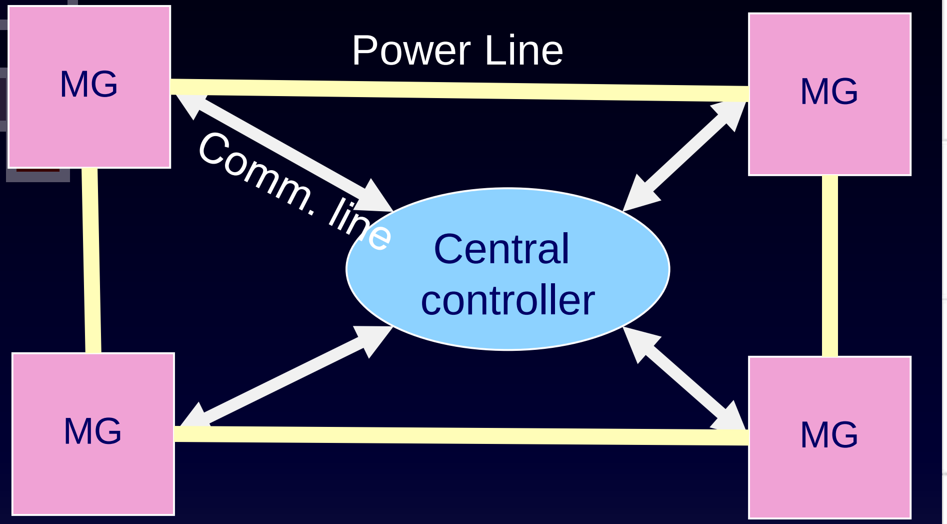
Cyber-Physical Co-Simulator

- Problem: Smart grid co-simulator development to model power-information-control dependences to better understand emerging system vulnerabilities.
- Challenges: Synchronizing federated simulators, effective co-simulator data exchange, reduction of accumulated errors.
- Approach: PSCAD, OMNeT++ and MATLAB with C/C++ programming as binding medium.
- Impact: Facilitates study of impacts of cyber attacks on power systems.

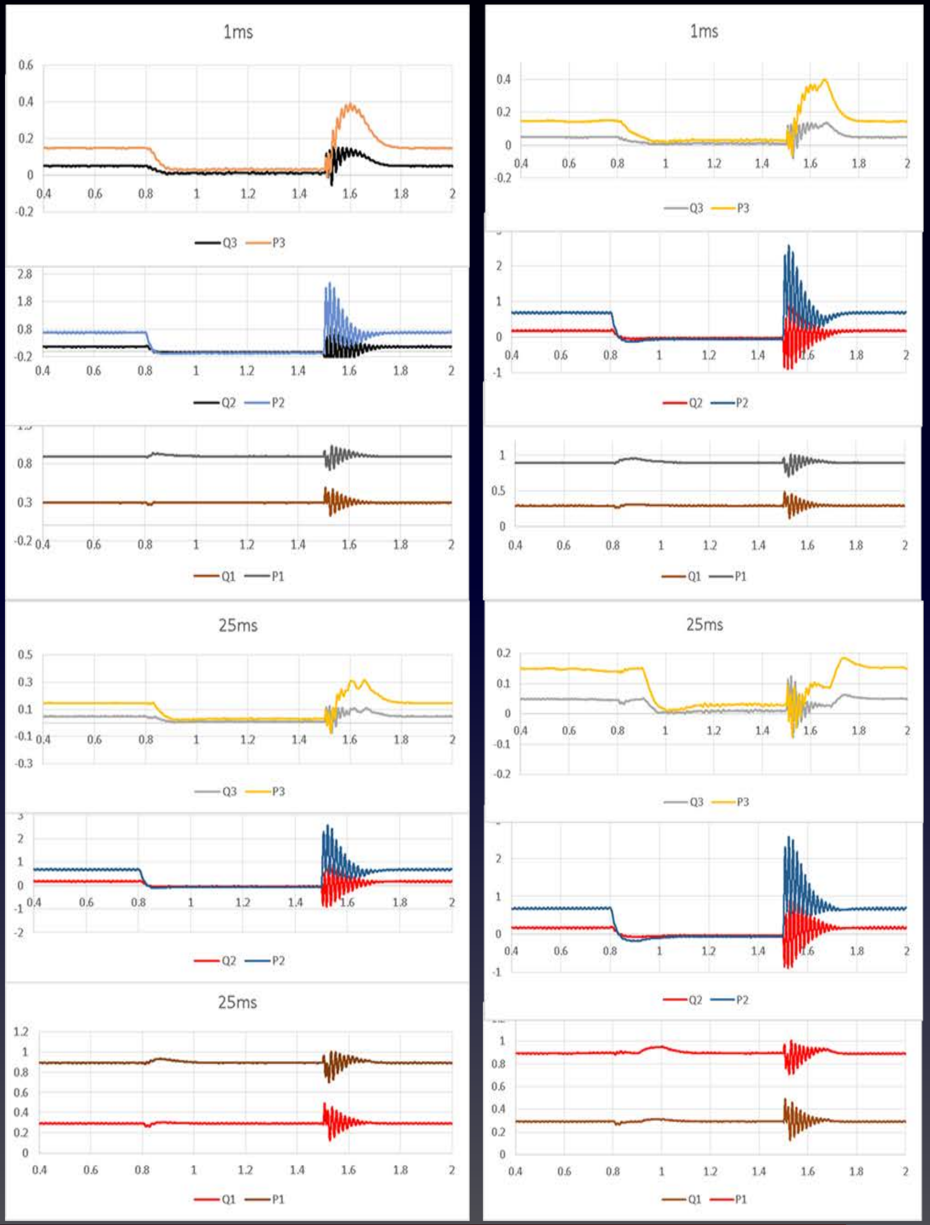
Federation of simulators that runs concurrently or serially to achieve a given objective



- Transient Analysis
- State estimation
- Voltage stability
- Small signal stability
- Post mortem analysis



Distributed/Hierarchical Control of cluster of microgrids


1ms
Q3
P3
Q2
P2
Q1
P1
1ms
Q3
P3
Q2
P2
Q1
P1
25ms
Q3
P3
Q2
P2
25ms
Q1
P1
25ms
Q3
P3
Q2
P2
Q1
P1