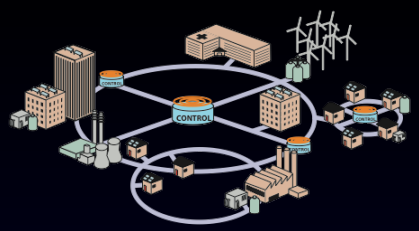


Cyber-Physical Security for the Smart Grid

Deepa Kundur
Texas A&M University
(Joint work with Shan Liu, Takis Zourntos and Karen Butler-Purry)

SeMANTIC Research Group

Dr. Deepa Kundur

- Cyber security of the electric smart grid
  - Cyber security impact analysis
  - Modeling and analysis of cyber-physical system dependencies
  - Robust topology design
- Security and privacy of sensor and social networks
  - Secure wireless connectivity and routing
  - Design of ad hoc surveillance networks in attack-prone and uncertain environments
  - Distributed encryption
- Information forensics
  - Information leakage acr

CYBER SECURITY

Power System Automation Lab

Dr. Karen L. Butler-Purry

- On-line Monitoring, Condition Assessment, and Management of Power Distribution Systems
  - Prognosis of aging power systems
  - Protection of distribution systems with distributed generators
  - Active management of MicroGrid and stand alone power systems
  - Power management and damage control of shipboard power systems
  - System modeling and simulation for terrestrial and military

ge-scale power systems, including
and hardware in the loop (HIL)

POWER SYSTEMS

15

Parasol Smarter computing. Texas A&M University

Dr. Takis Zourntos

- Control theory and applications
  - Linear and nonlinear adaptive and robust control
  - Nonlinear dynamical systems
  - Digital control
  - Applications in power and electromechanical systems
- Robotics
  - Autonomous agents, multi-agent systems
  - Algorithms and system integration for lightweight robots
  - Application of multi-agent techniques to smart grid systems
  - Human-robot interaction
- Integrated circuits
  - Analog, digital and mixed-signal microelectronics
  - Signal processing, data conversion and instrumentation

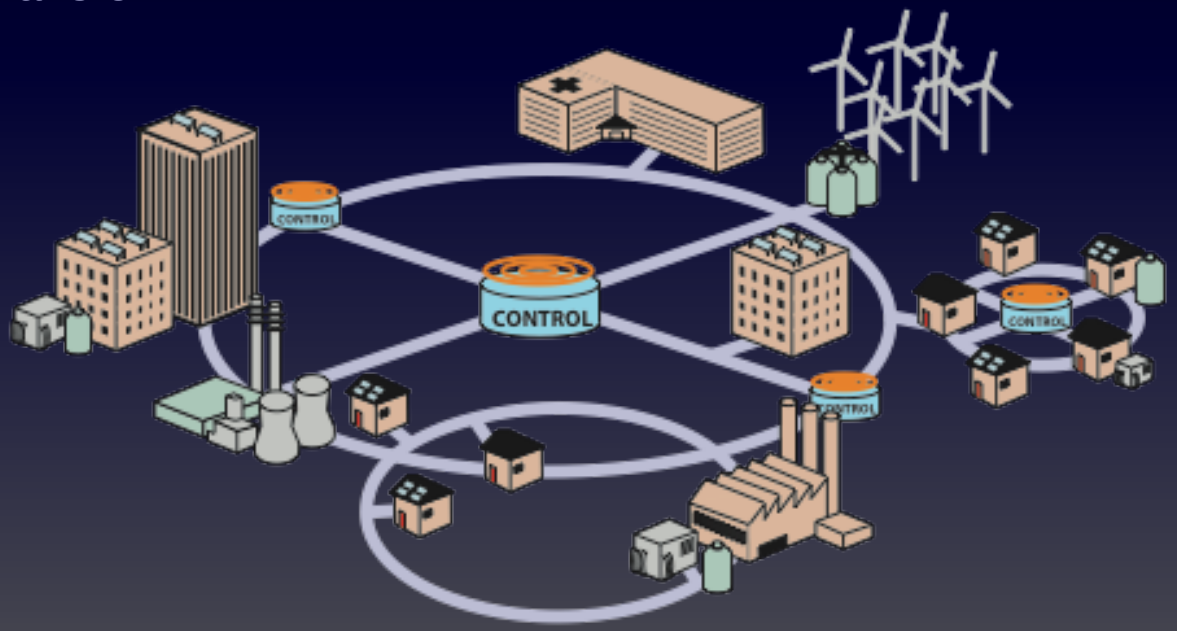
DYNAMICAL SYSTEMS

17

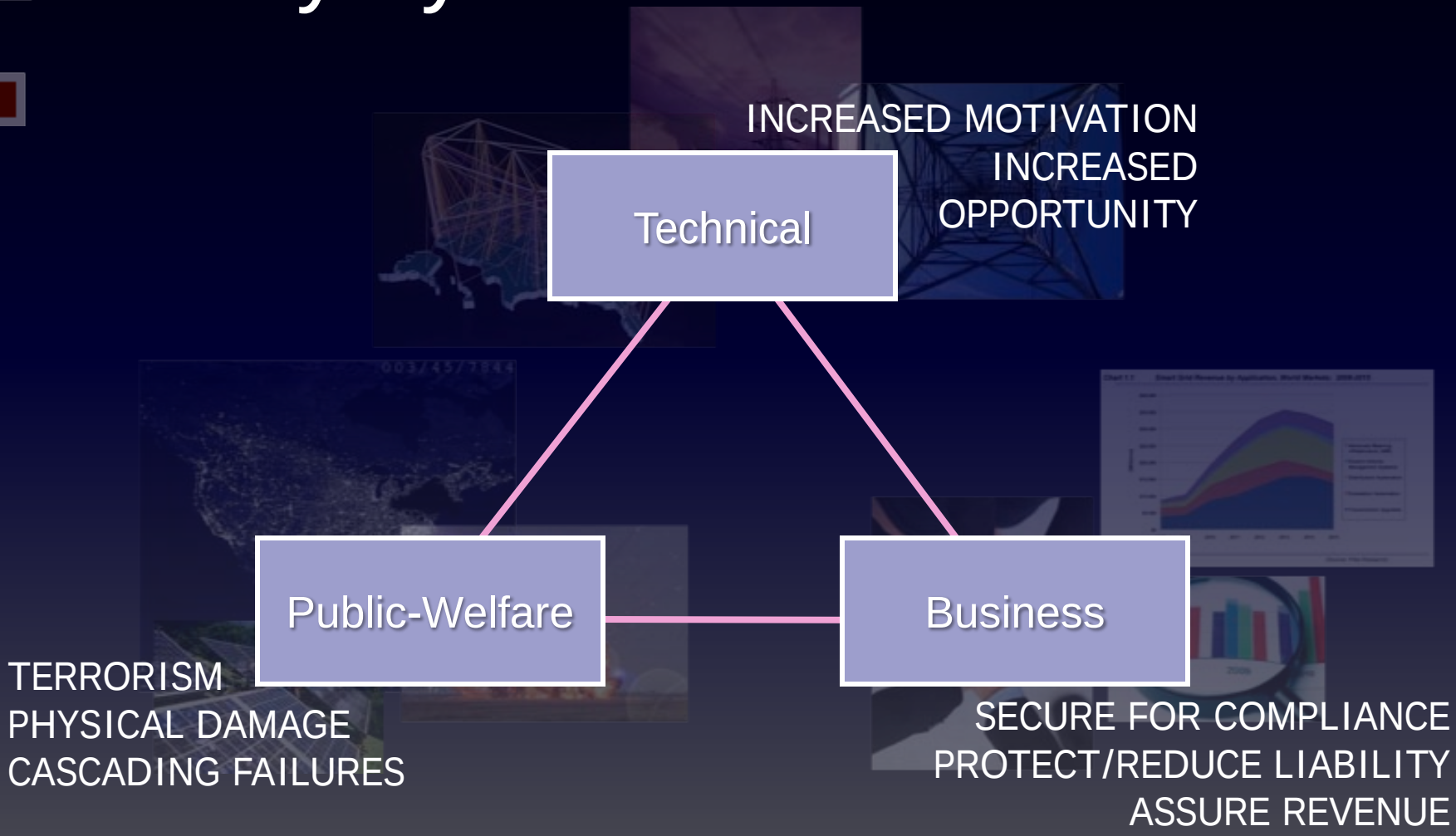
A Smarter Grid

MARRIAGE OF INFORMATION TECHNOLOGY WITH THE EXISTING ELECTRICITY NETWORK

Bidirectional information transfer!
Bidirectional energy transfer!



Why Cyber Protect the Grid?



What has history taught us?

- 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

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?

Of Interest to the EPU Community

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

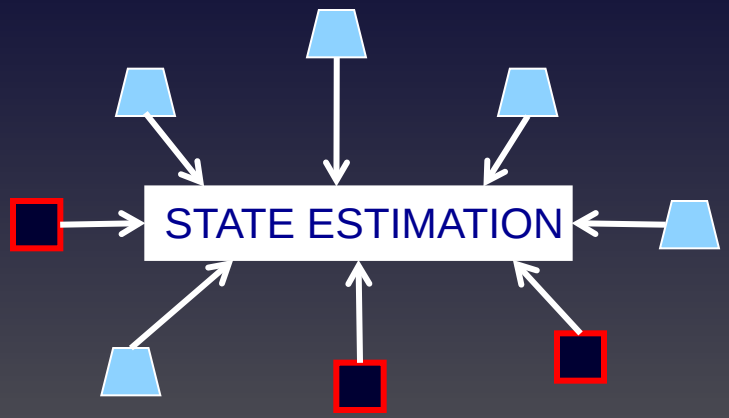
Design Mantra

"*Cyber assets are targets of cyber attacks.*"

- Cyber assets:
  - Any data, device or component of the environment that supports information-related activities
  - E.g., IEDs, PLCs, RTUs, PMUs, PDCs, SCADA, AMI, communication infrastructure ...

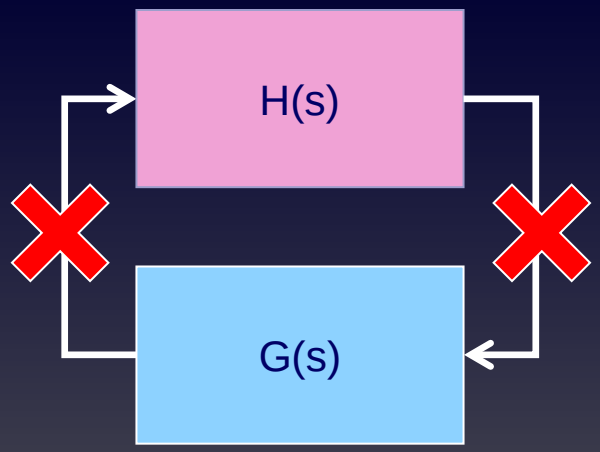
False Data Injection Attacks

- Liu et al. (2009)
- Corruption of measurements:
  - $z_a = z + a$, for $a = Hc$ and constraints on a
- Figures of merit:
  - Likelihood of finding a
  - Impact = $||x_a - x||$



Denial-of-Service Attacks

- How do you make decisions with lack of or delayed information?



Risk

- Risk = Likelihood x Impact
- Risk = $P_{Threats}$ x $P_{Vulnerabilities}$ x Impact

THREATS

NATURALLY OCCURRING

UNTRAINED PERSONNEL

MALICIOUS INSIDER

LONE ACTORS

ORGANIZED CRIME

TERRORISM

NATION-STATES

VLUNERABILITIES

COMMUNICATIONS

INTERNET

GRID COMPLEXITY

SYST

EXIT

EMS

NEW DEVICES

IMPACT AREAS

GENERATION SENSORS

GENERATION ACTUATORS

XMISSION SENSORS

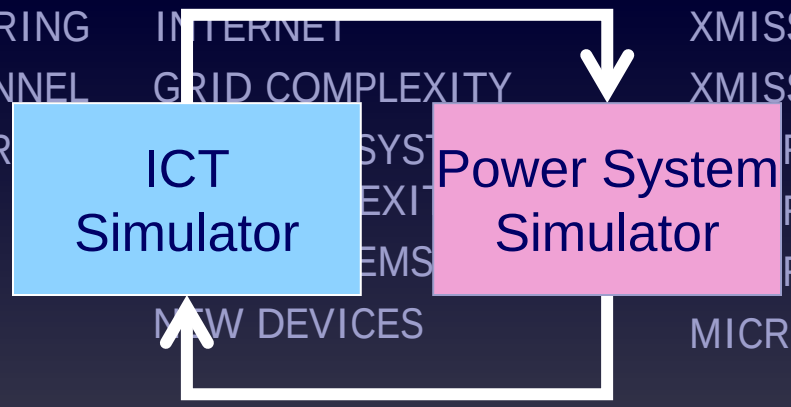
XMISSION ACTUATORS

RIB SENSORS

RIB ACTUATORS

RIB GNERATION

MICROGRIDS



Emerging Design Mantra

"*Cyber-physical assets are targets of cyber-physical attacks*."

- Cyber-physical assets:
  - Any component of the environment that supports energy-related activities
  - E.g., IEDs, PLCs, RTUs, PMUs, PDCs, SCADA, AMI, communication infrastructure, energy sources, transformers, transmission lines, buses, loads

Cyber-Physical Vulnerabilities

- Cyber assets can be direct targets of cyber and physical attacks.
- Physical assets can be direct targets of physical attack and indirect targets of cyber attack.

Cyber-Physical Attacks

- Evolving definitions:
  - A coordinated set of cyber and physical attacks on cyber-physical assets with the goal of maximizing physical disruption
    - E.g., combination of transmission line fault with state estimation modification
  - A cyber attack employed on a cyber asset with the goal of disruptive impacts to the physical assets
    - E.g., control signal modification to reconfigure power system to an emergency state

Emerging Grand challenge: Modeling

Modeling Wish List

- Tight coupling of cyber and physical components:
  - time-scale integration, vulnerability analysis
- Formalism using powerful mathematical constructs
- Flexible granularity of modeling detail to tune complexity
- ‘What if’ analysis possible.

Dynamical Systems

✓ Formalism
 Variable granularity
 'What if' analysis

How can you model cyber and physical entities within a common framework?

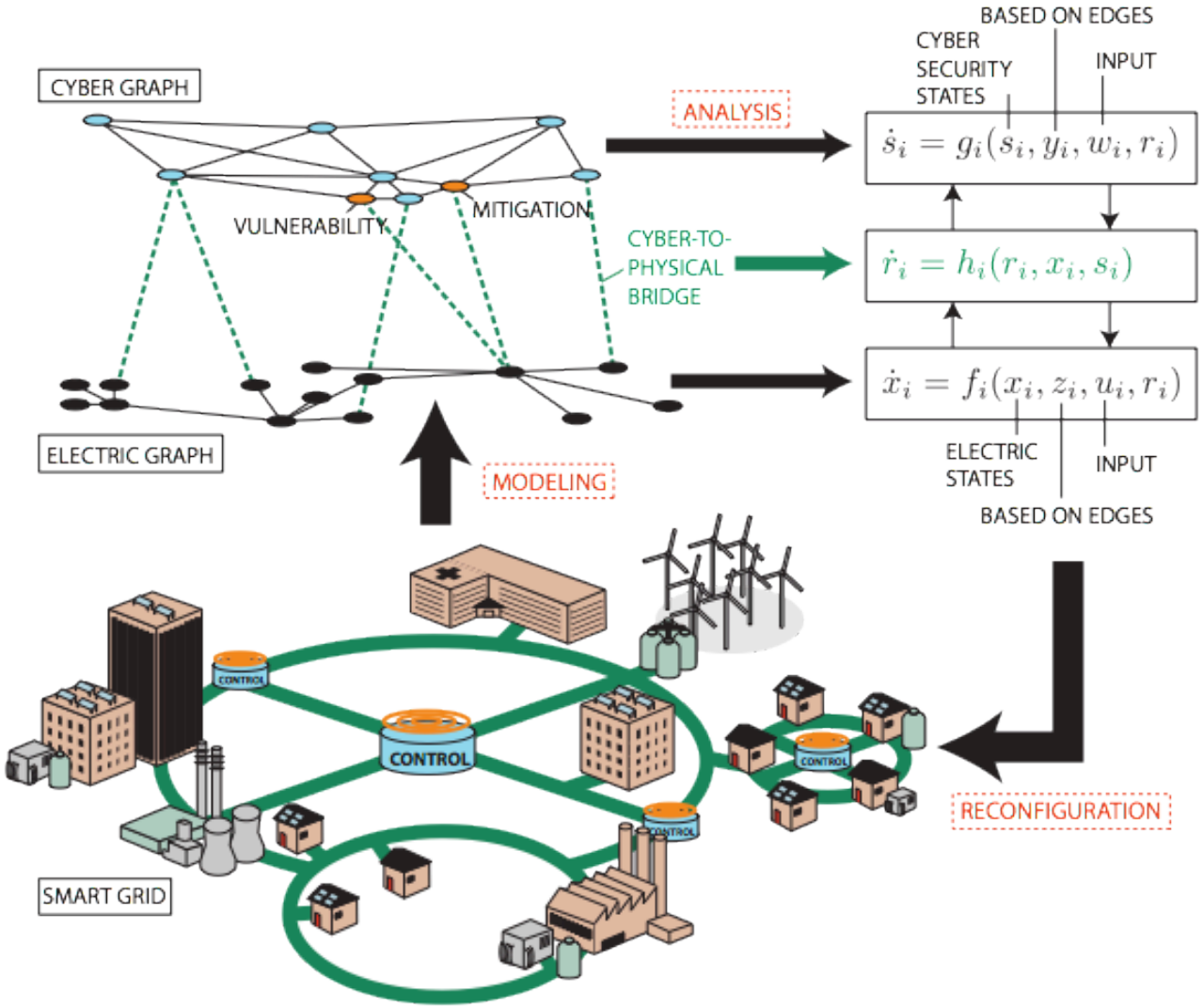
Dynamical Systems

- Describes time evolution of state vector:

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

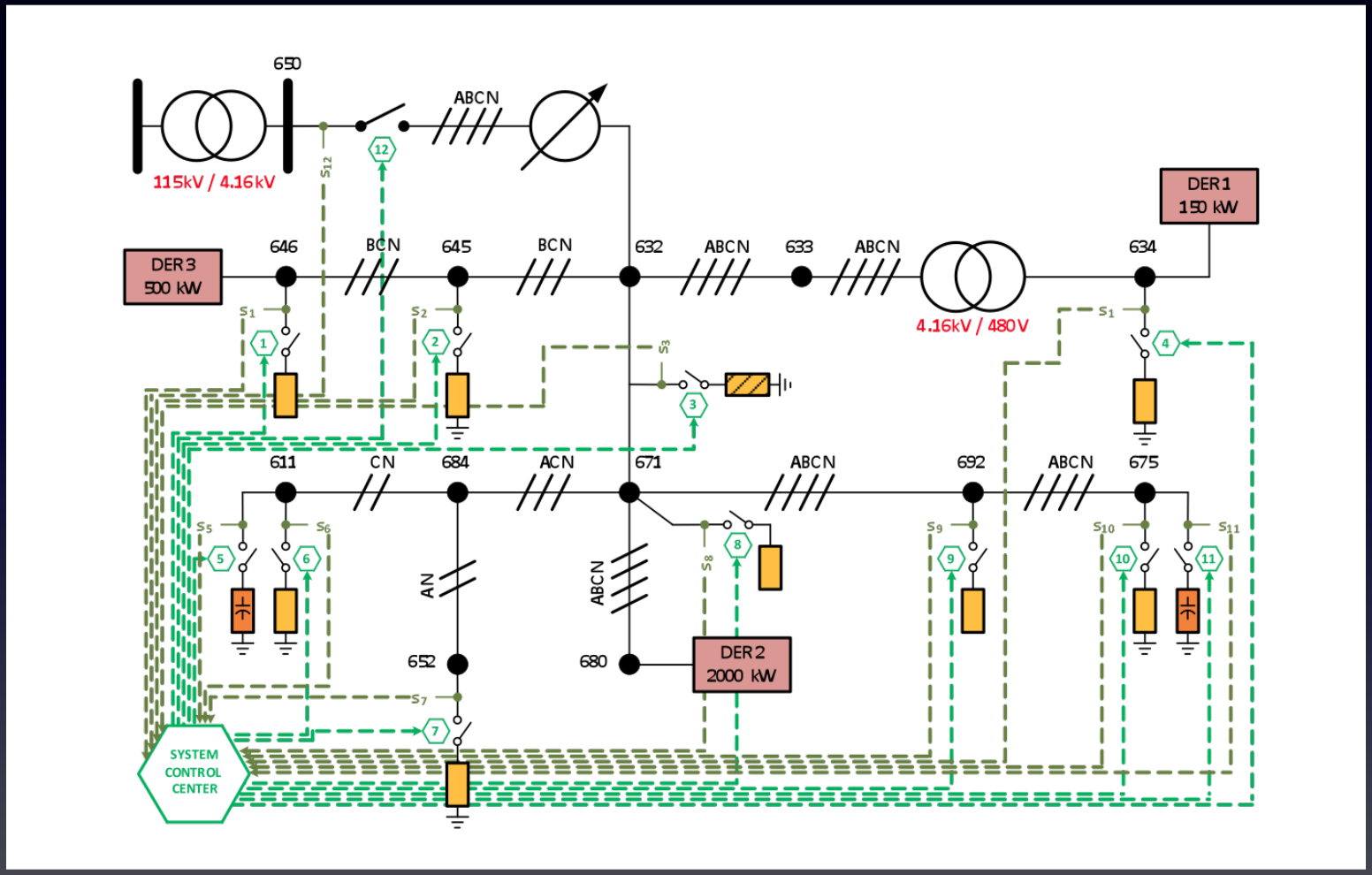
$$y = g(x, u)$$

- Models physics of power systems effectively

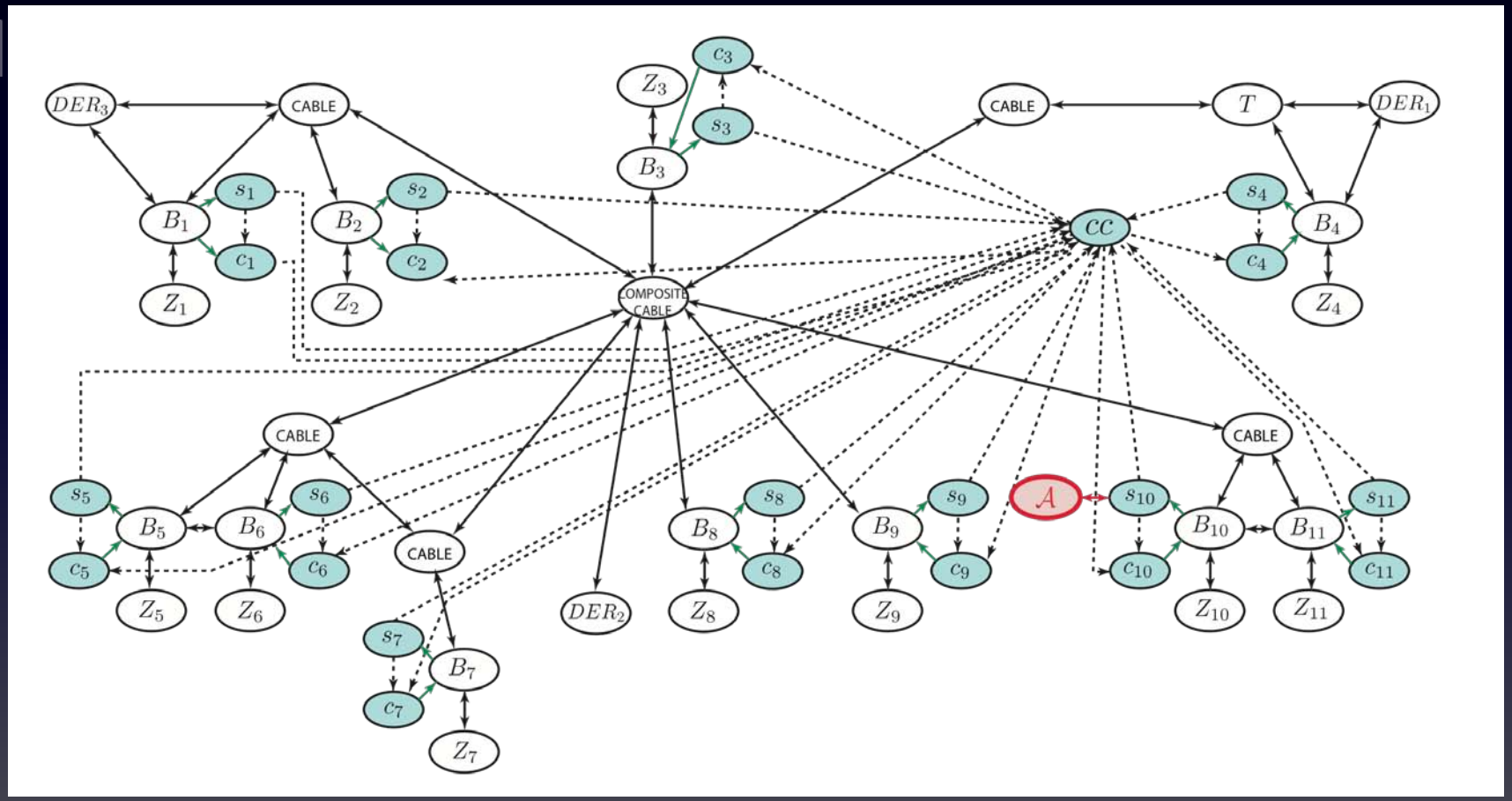


CAPTION: OVERVIEW OF CYBER SECURITY ANALYSIS FRAMEWORK

13 Node System



Graph Model


DER_3
CABLE
Z_3
c_3
s_3
B_3
CABLE
T
DER_1
s_1
B_1
c_1
Z_1
s_2
B_2
c_2
Z_2
CC
s_4
B_4
c_4
Z_4
COMPOSITE CABLE
CABLE
s_5
B_5
c_5
Z_5
s_6
B_6
c_6
Z_6
CABLE
s_7
B_7
c_7
Z_7
DER_2
s_8
B_8
c_8
Z_8
s_9
B_9
c_9
Z_9
$\mathcal{A}$
s_{10}
B_{10}
c_{10}
Z_{10}
CABLE
s_{11}
B_{11}
c_{11}
Z_{11}

Of Interest to the Power Community

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

Cyber-Physical Attacks

- Evolving definitions:
  - A coordinated set of cyber and physical attacks on cyber-physical assets with the goal of maximizing physical disruption
    - E.g., combination of transmission line fault with state estimation modification
  - A cyber attack employed on a cyber asset with the goal of disruptive impacts to the physical assets
    - E.g., control signal modification to reconfigure power system to an emergency state

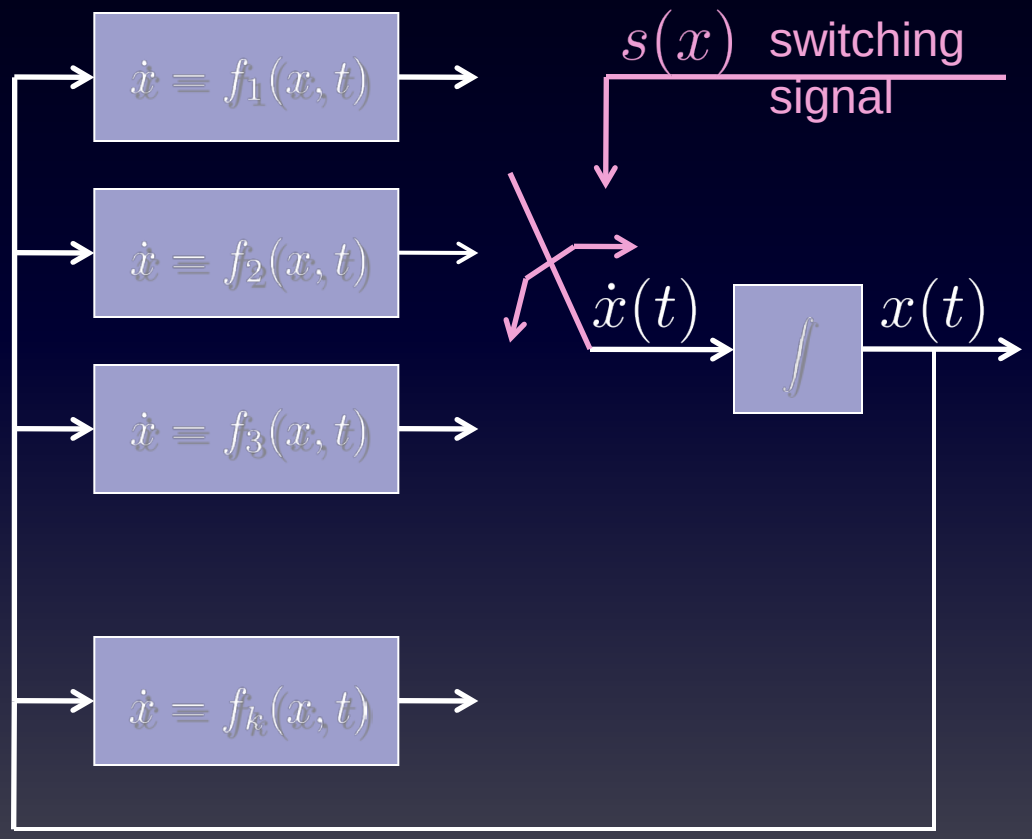
Coordinated Switching Attacks

- Smart grid envisions remote access of circuit breakers and switches
- Breaker control signals are corrupted
- Exploits physical vulnerabilities from reconfiguration

Coordinated Switching Attacks

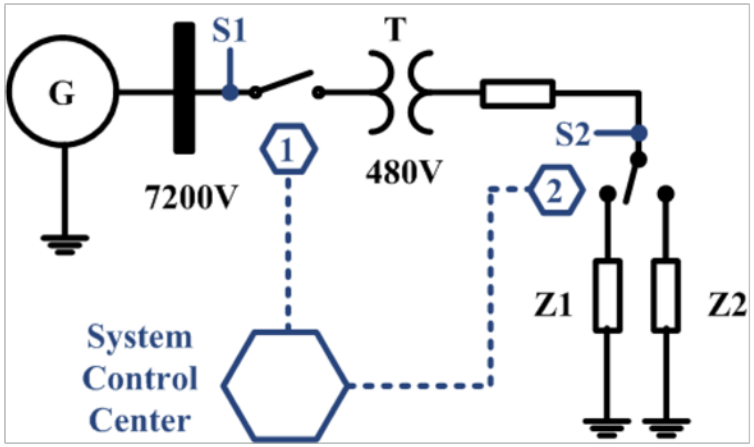
- Goal: physical disruption through rotor angle instability
- Exploit local state info to define a disruptive cyber control switching sequence
- Model the cyber-physical system as a type of hybrid dynamic system:
  - Exhibit both continuous and discrete behaviors

Variable Structure System



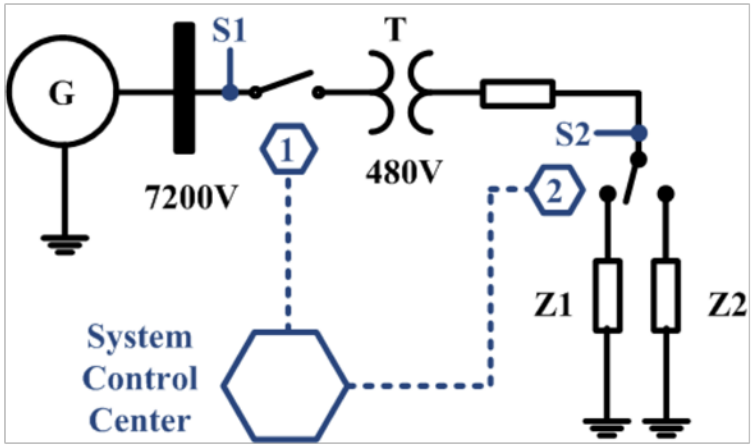
Variable Structure System

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

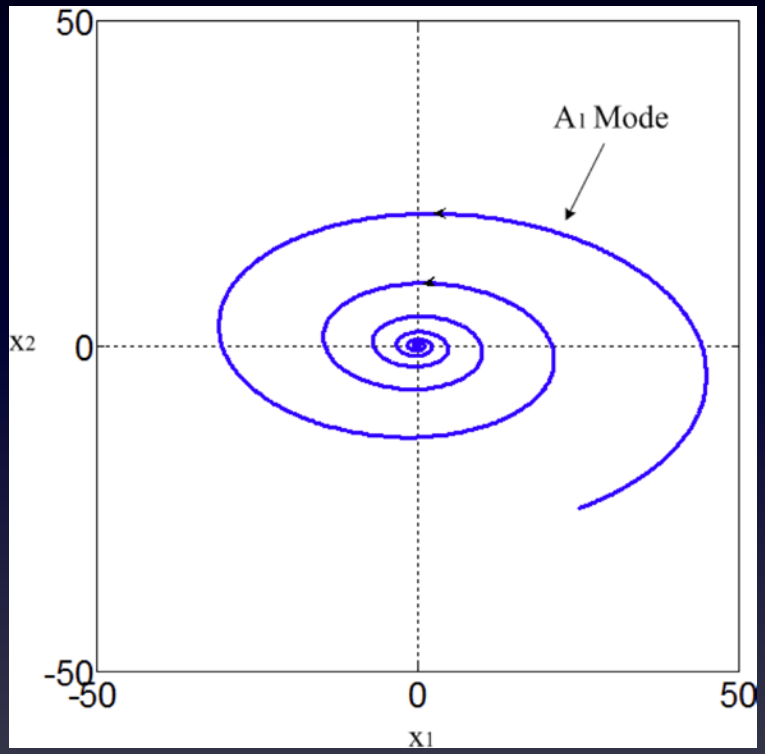


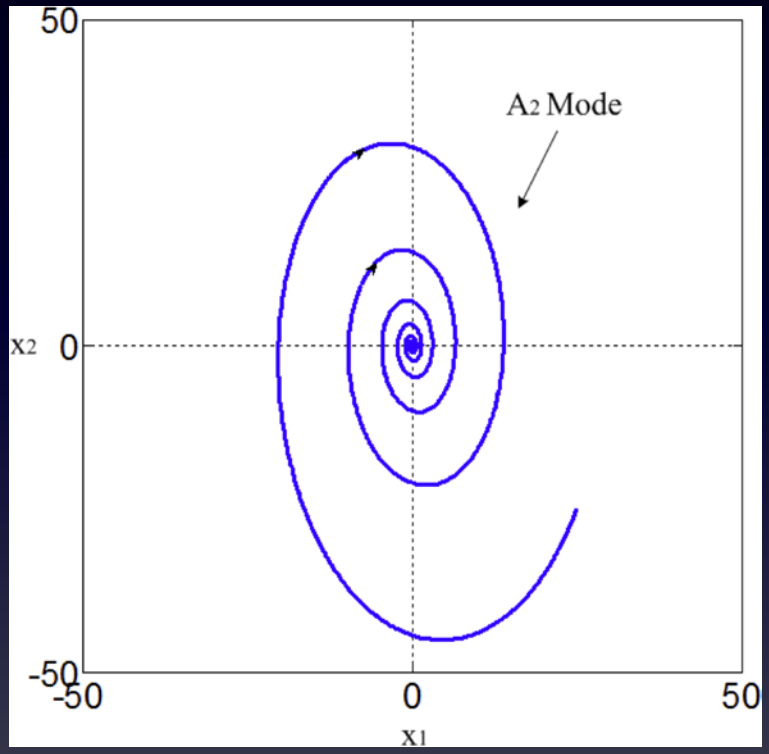
Variable Structure System

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



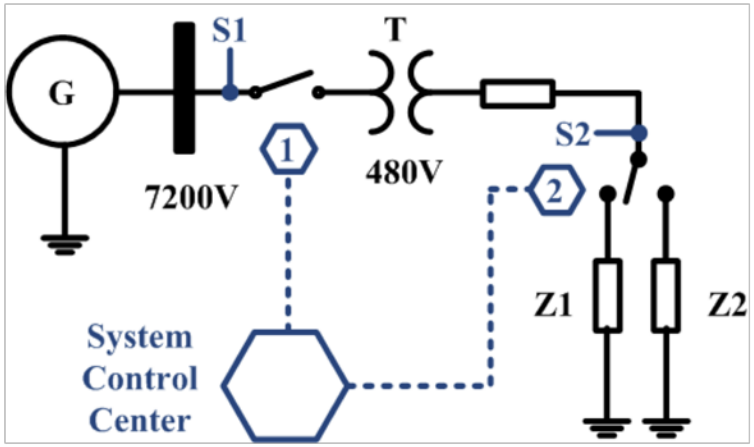
Static Switch Phase Portraits





Variable Structure System

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



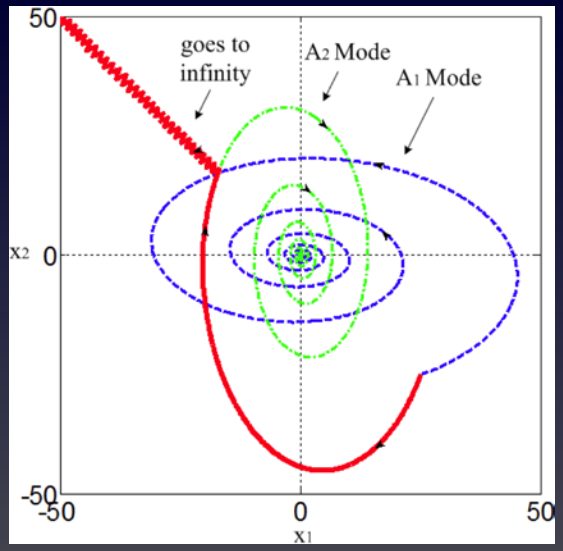
$$s(x) = x_1 + x_2$$

OR

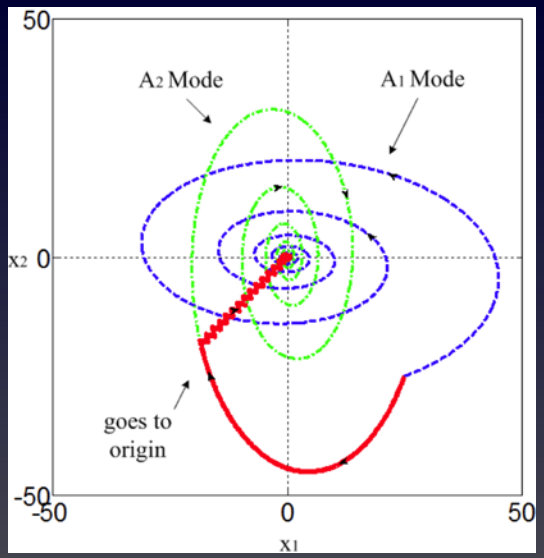
$$s(x) = -x_1 + x_2$$

Variable Structure System

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



$s(x) = x_1 + x_2$



$s(x) = -x_1 + x_2$

The Sliding Mode

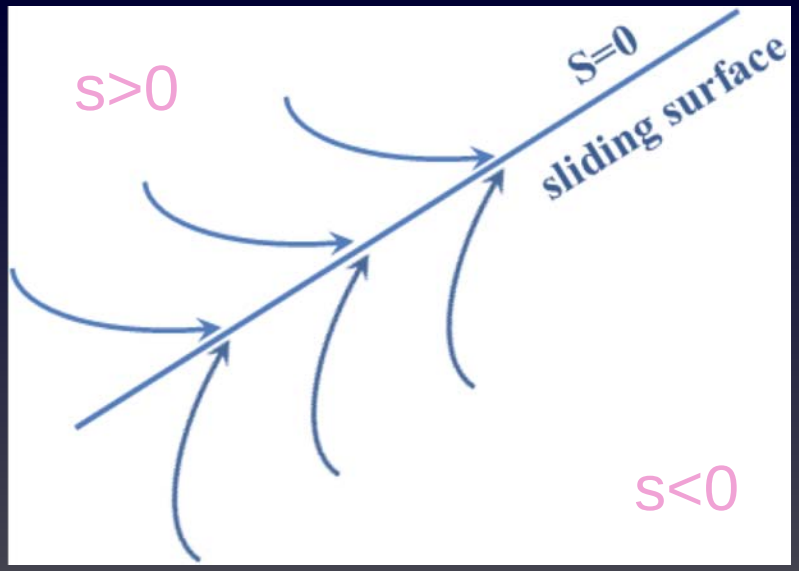
- "Emergent" property from switching that has characteristics different from individual subsystems
- Motion of state trajectory along a chosen line/plane/surface

Existence of Sliding Mode

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

$$\boxed{s\dot{s} < 0}$$

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



Attack Construction

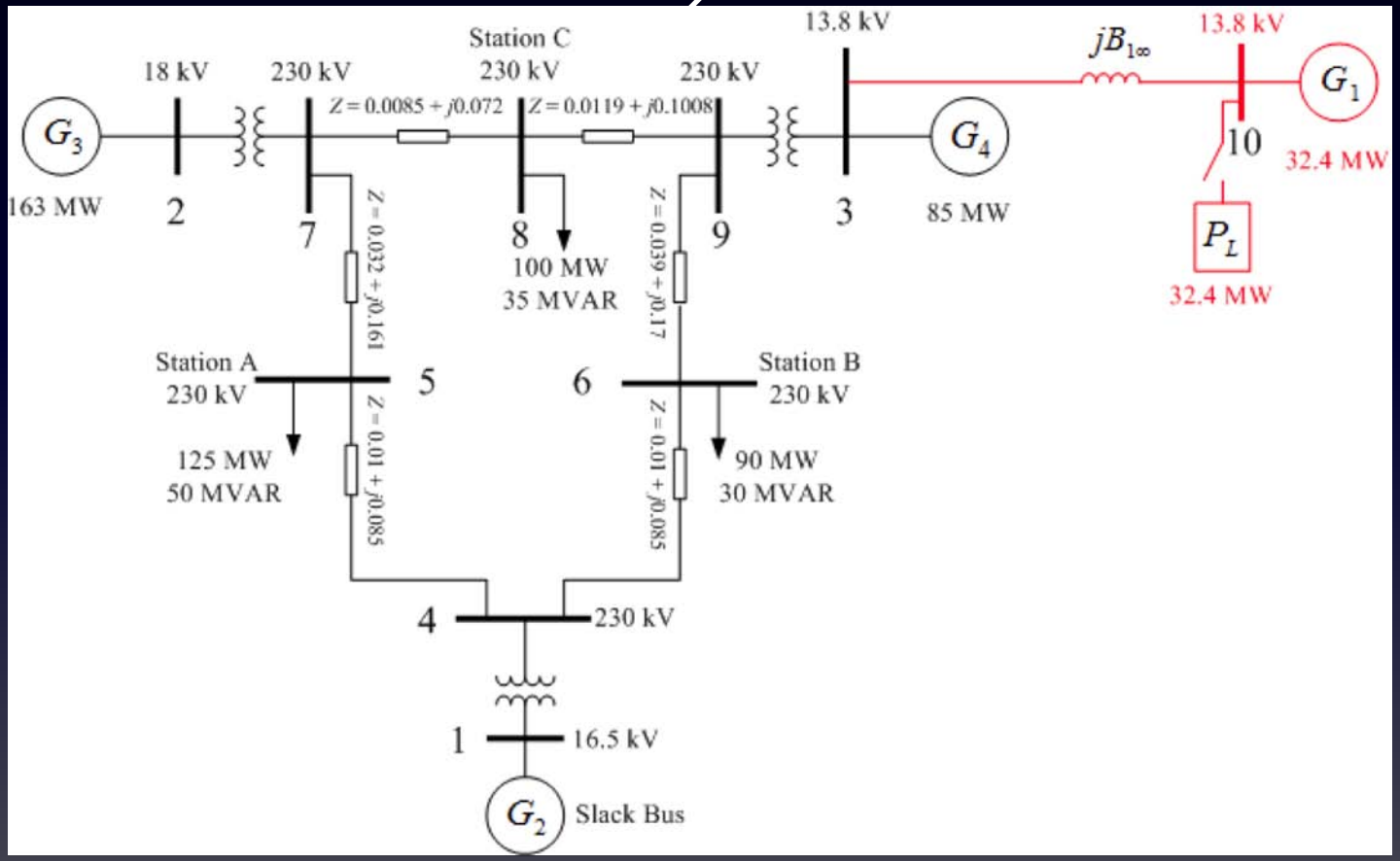
1. Represent smart system as variable structure system whereby s(x) is general.

2. Determine existence of and identify class of sliding modes.

3. Assign identified sliding surface for attack.

WECC System

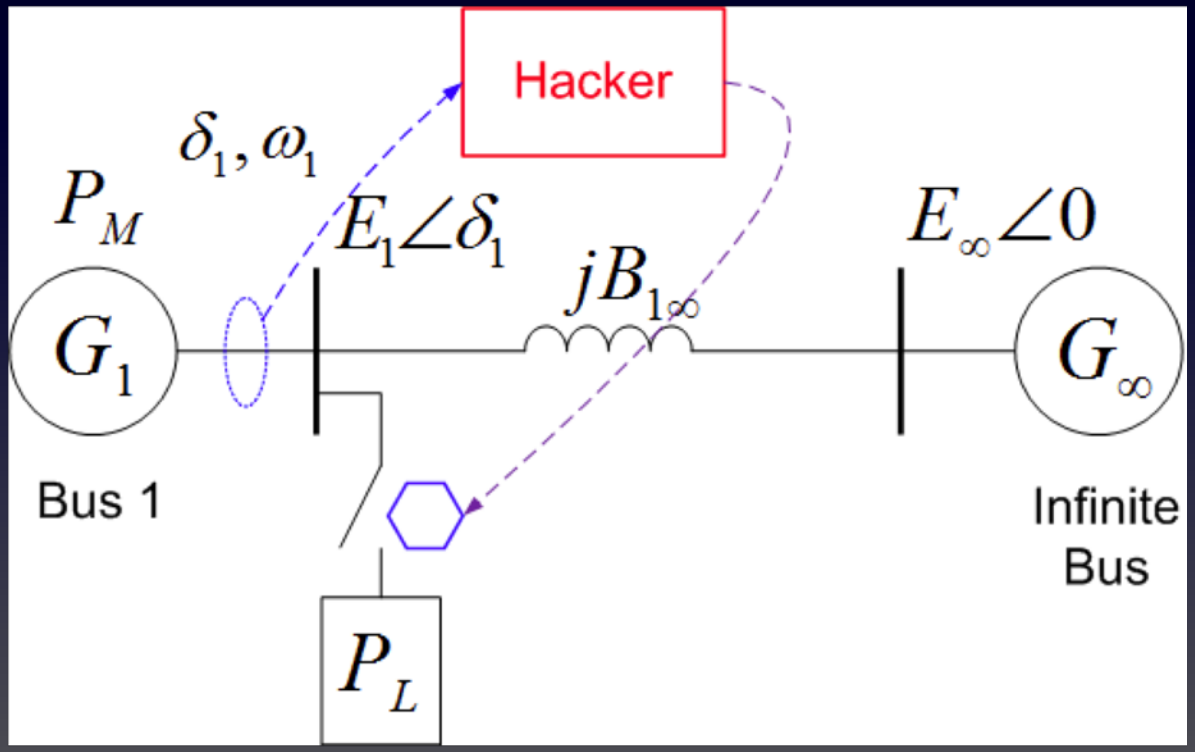
Western Electricity Coordinating Council, 3 machine, 9-bus system



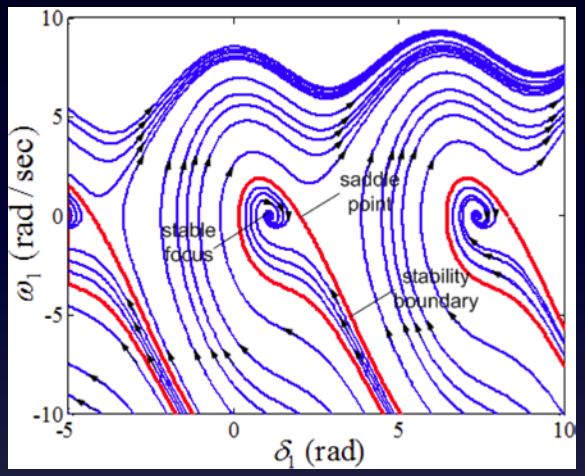
Step 1: Modeling

$$A_1 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = -10 \sin \delta_1 - \omega_1 \end{cases} \quad \text{if } P_L \text{ connected}$$

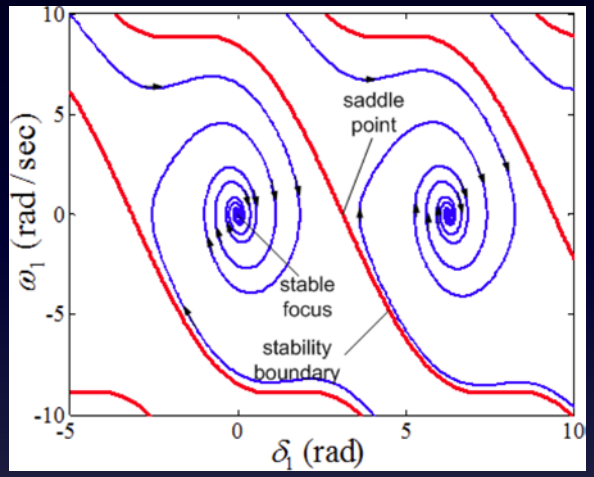
$$A_2 : \begin{cases} \dot{\delta}_1 = \omega_1 \\ \dot{\omega}_1 = 9 - 10 \sin \delta_1 - \omega_1 \end{cases} \quad \text{if } P_L \text{ not connected}$$



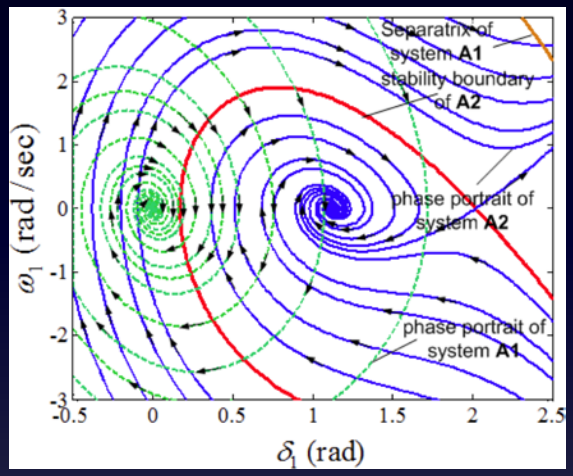
Step 2: Existence of Sliding Mode



Phase Portrait of A_1

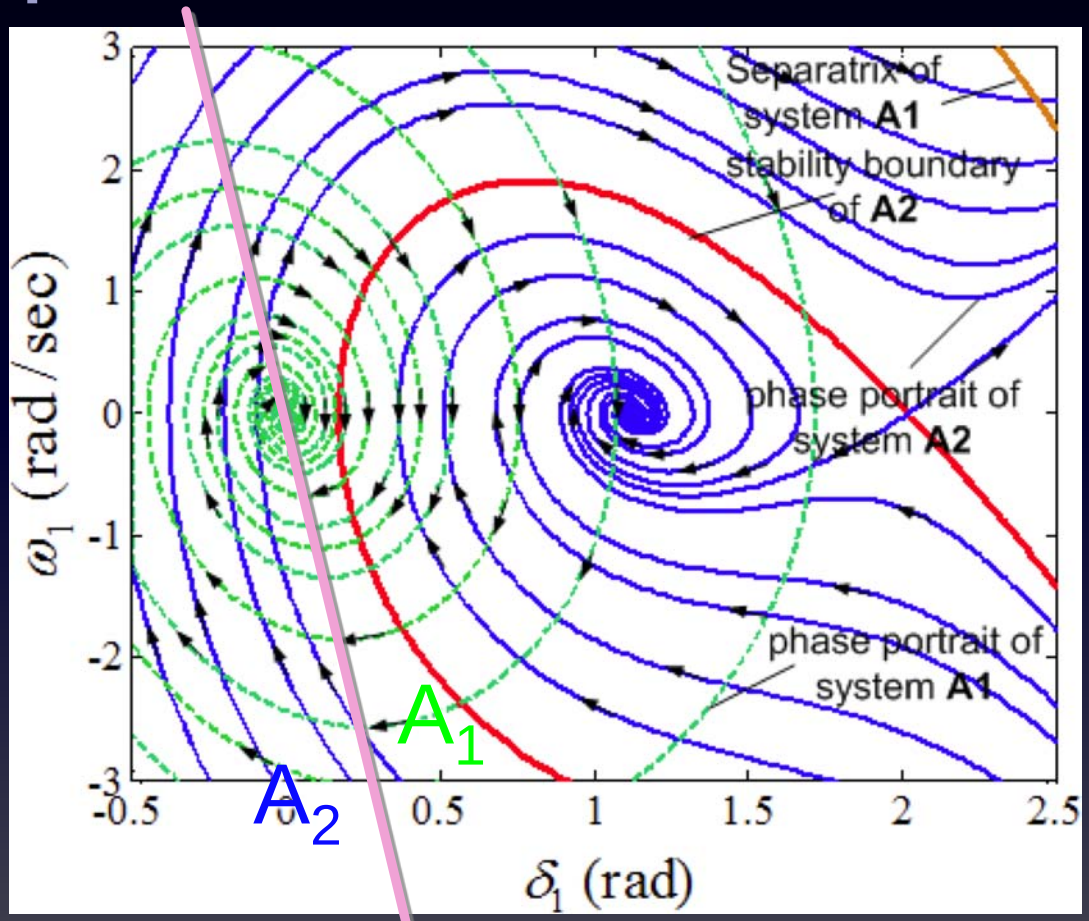


Phase Portrait of A_2



Overlapping Close-up

Step 2: Existence of Sliding Mode



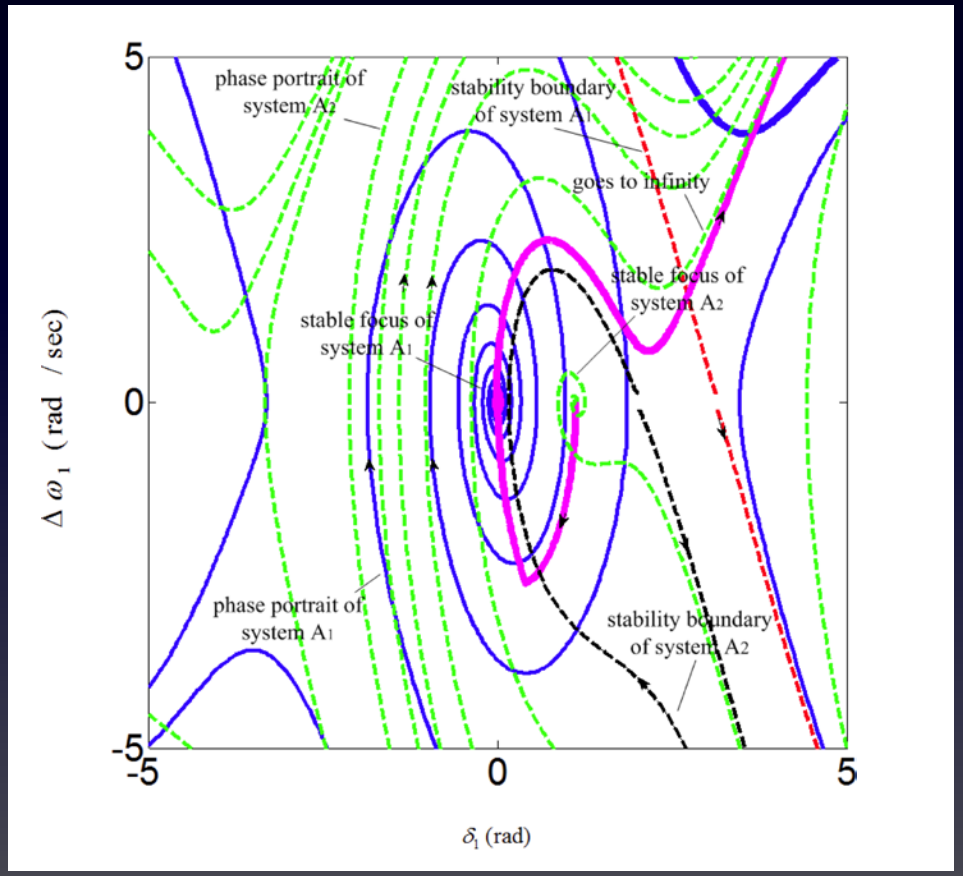
$s = 6\delta_1 + \omega_1$

VALID SLIDING SURFACE

Step 3: Assign s(x) for attack

$$\boxed{s = 6\delta_1 + \omega_1}$$

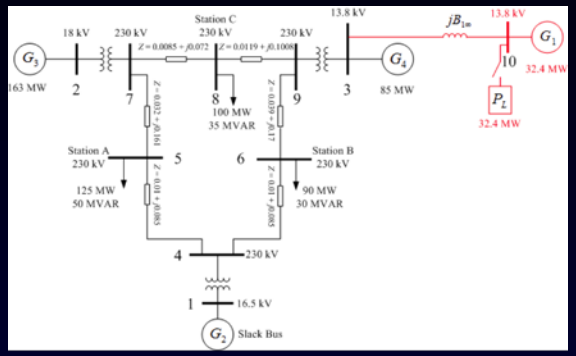
Attack Simulation on SMIB Model



Switching applied From 0 s to 2.5 s.

Attack Simulation on WECC

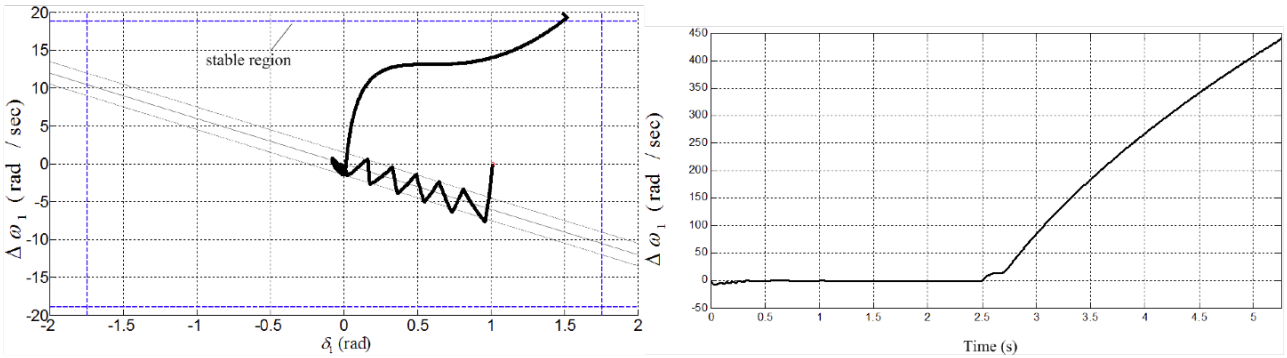
- PSCAD Simulations



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

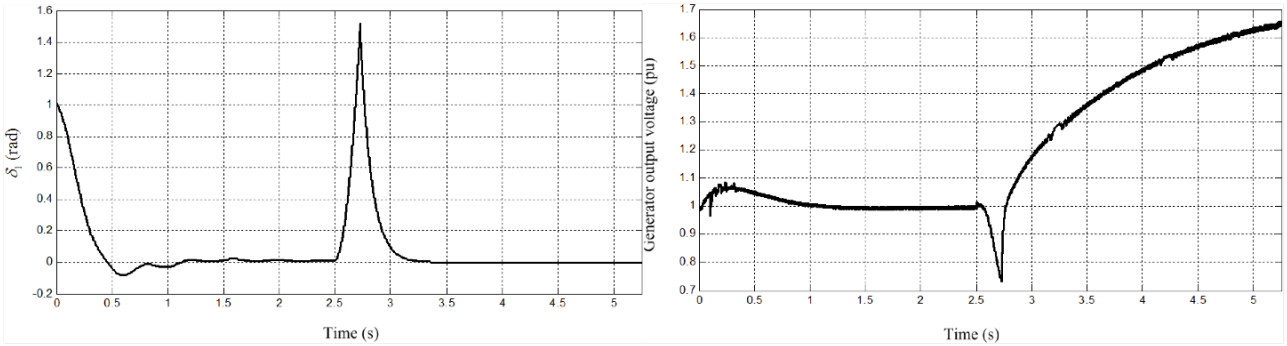
Name	Parameter	Gen 3	Gen 4
Rated RMS Line-Line Volatge	V_{gl-l}	18.0 kV	13.8 kV
Active Power	P_g	163 MW	85MW
Power Factor	p_{fg}	0.8	0.8
Frequency	f	60 Hz	60 Hz
Direct axis unsaturated reactance	Xd	0.8958	1.3125
D axis unsaturated transient reactance	Xd'	0.1198	0.1813
D axis open circuit unsaturated 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

Attack Simulation on WECC



(a) System state trajectory.

(b) G_1 deviation from nominal frequency.



(c) G_1 phase angle.

(d) G_1 output voltage.

Final Remarks

- Coordinated variable structure switching attacks represent a new class of attacks aimed specifically to disrupt power system operation.
- Hybrid dynamical system models are effective tools in vulnerability analysis.

Where should we go from here?

- Develop common problem formulations within community
  - Exciting area, but still ad hoc
- Encourage greater collaboration amongst power system researchers, control theorists and information technology community

Contact

Dr. Deepa Kundur
Associate Professor
Electrical & Computer Engineering
Texas A&M University
dkundur@tamu.edu
http://www.ece.tamu.edu/~deepa/