Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid

D. Kundur, F. Xianyong, S. Liu, T. Zourntos and K.L. Butler-Purry

Presenter: Deepa Kundur

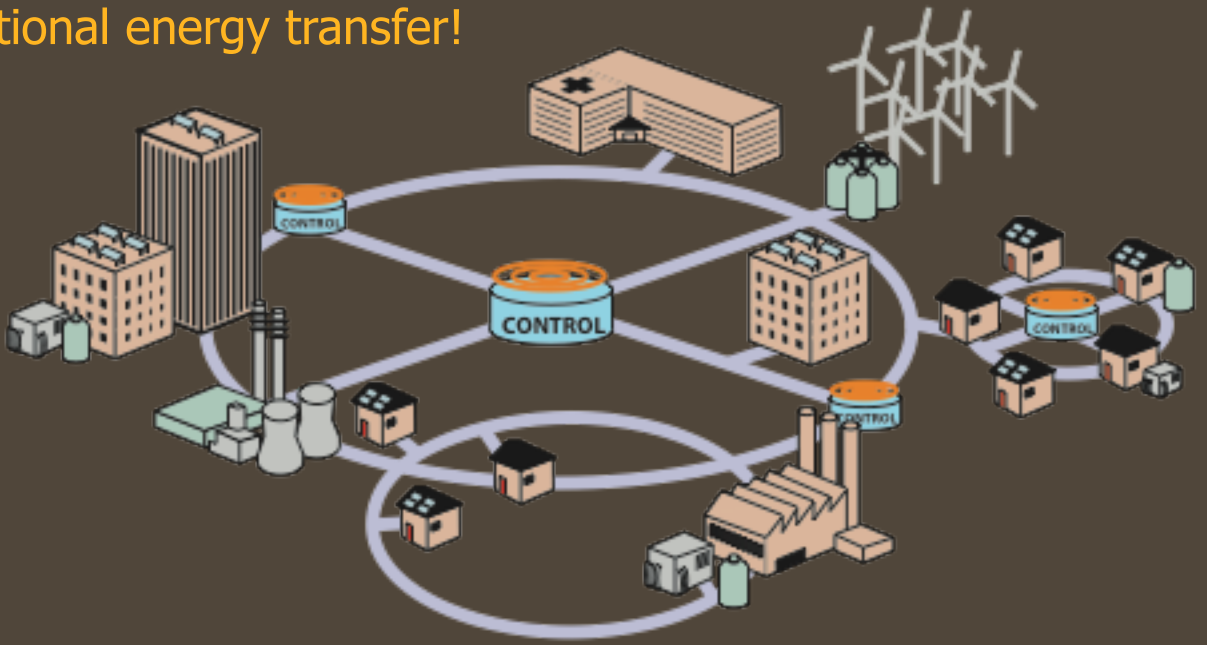
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

A Smarter Grid

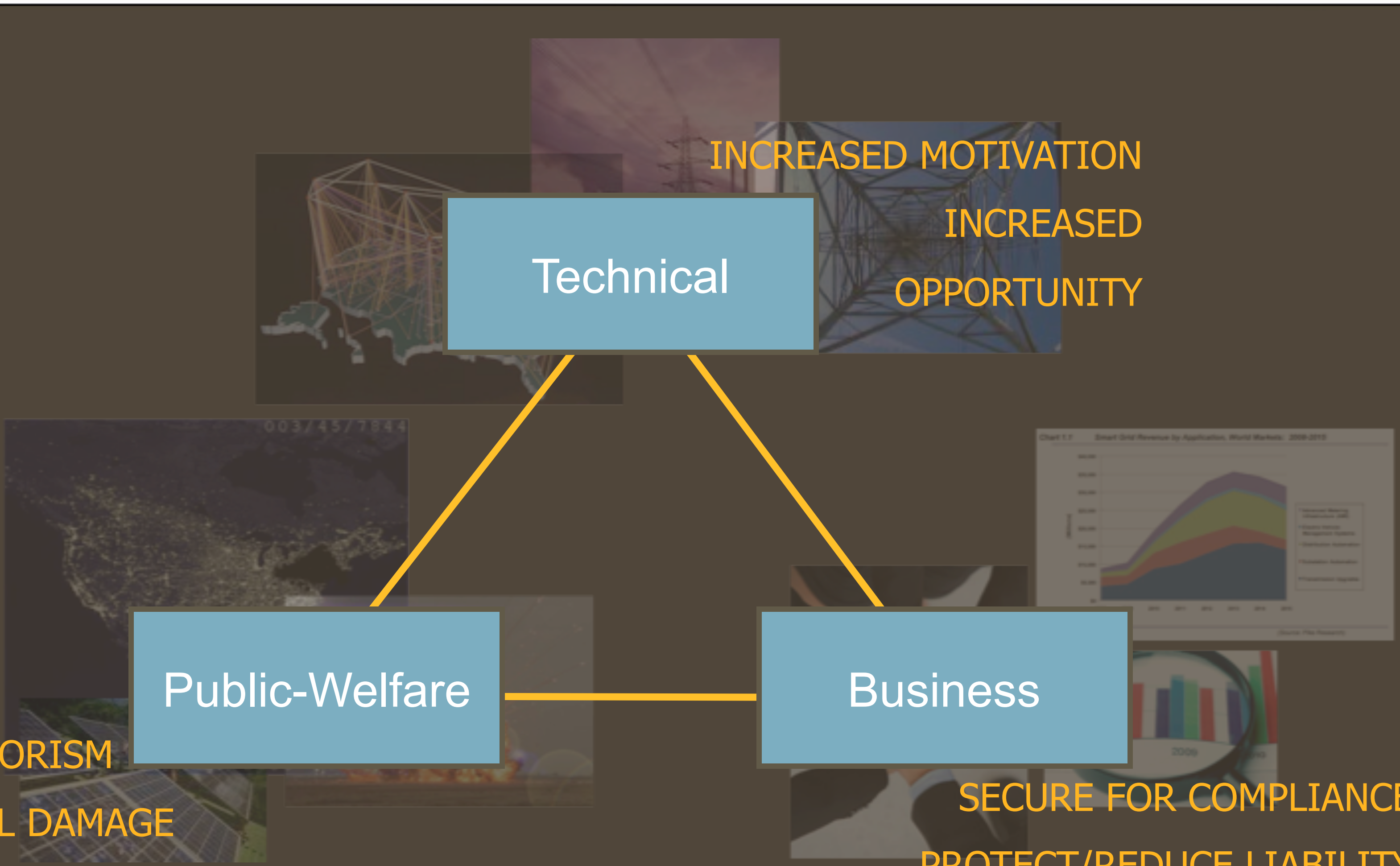
MARRIAGE OF INFORMATION TECHNOLOGY WITH THE EXISTING ELECTRICITY NETWORK

Bidirectional information transfer!

Bidirectional energy transfer!



Why Protection the Grid?



Technical

Public-Welfare

Business

INCREASED MOTIVATION

INCREASED

OPPORTUNITY

TERRORISM

PHYSICAL DAMAGE

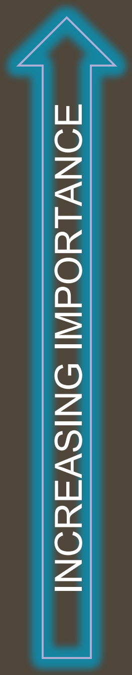
CASCADING FAILURES

SECURE FOR COMPLIANCE

PROTECT/REDUCE LIABILITY

ASSURE REVENUE

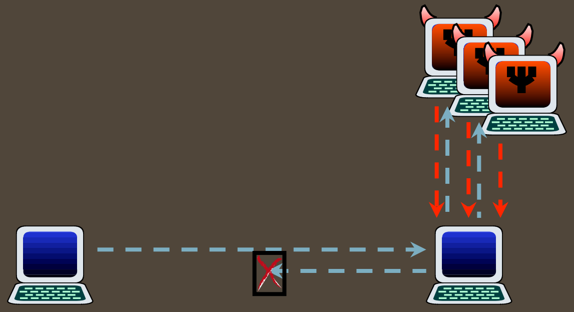
System Security Services


INCREASING IMPORTANCE

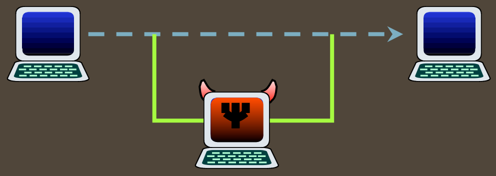
- Availability of info and power services
- Access control of cyber infrastructure
- Authentication of control and sensor data
- Integrity of decision-making data
- Confidentiality of control and sensor data

Of Interest to the Energy Community

- Attacks on timely delivery
  - Denial of information access



- Attacks on information accuracy and reliability
  - Deliberate attack or operator error



System Security Needs

- Risk assessment
- Prevention
- Detection
- Response
- Recovery

CHALLENGES:

COMPLEX INTERDEPENDENCIES

INTEGRATION WITH LEGACY SYSTEMS

REAL-TIME ONLINE

LACK OF SECURITY CULTURE

Risk

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

<u>THREATS</u>

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

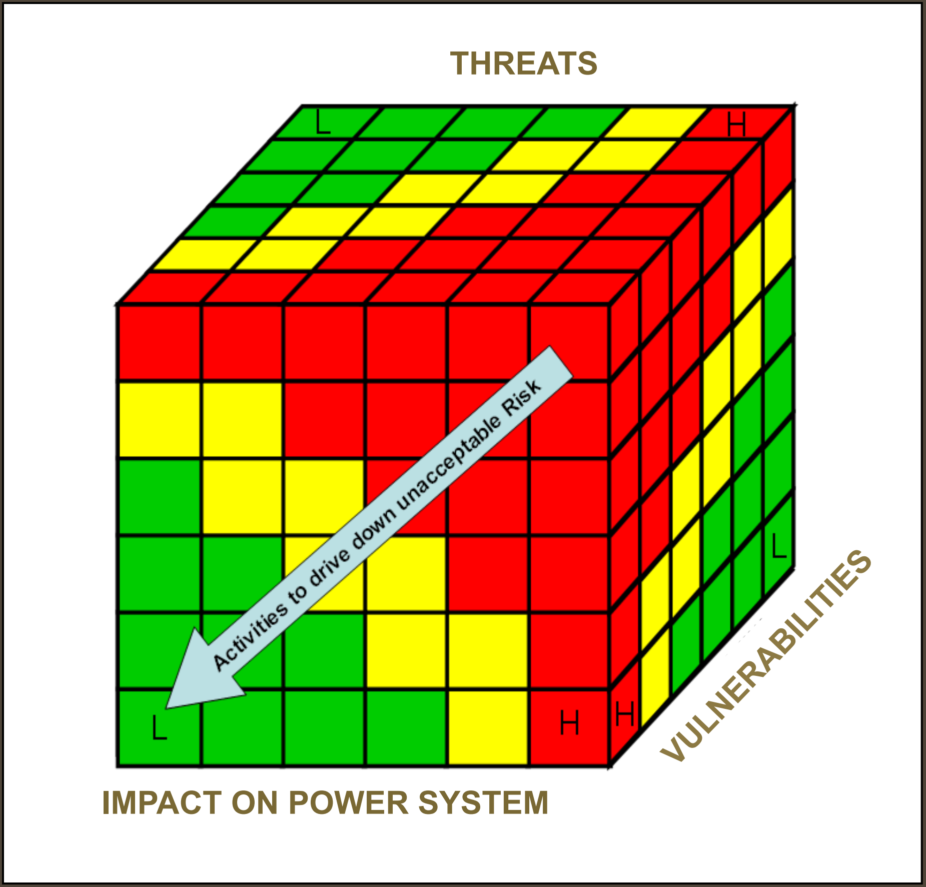
<u>VULNERABILITIES</u>

COMMUNICATIONS
INTERNET
GRID COMPLEXITY
CONTROL SYSTEM COMPLEXITY
NEW SYSTEMS
NEW DEVICES

<u>IMPACT AREAS</u>

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

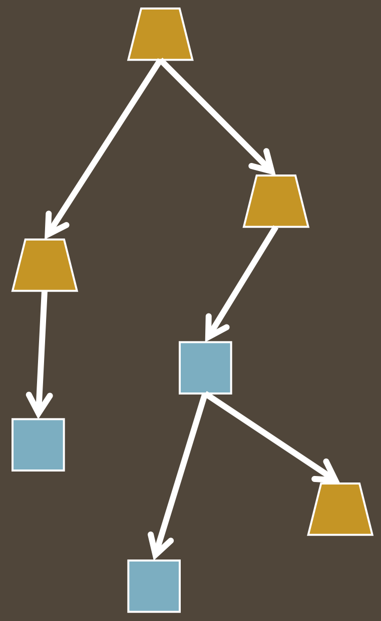
Fundamental R&D Questions

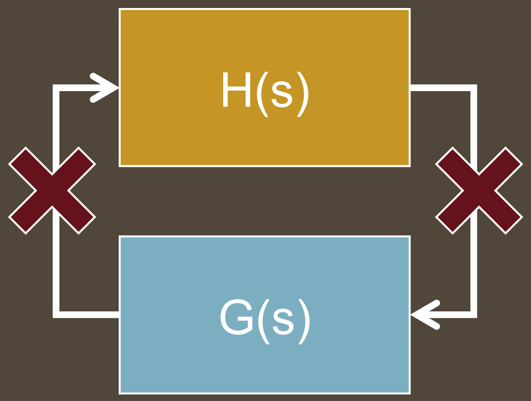
- What are the electrical system impacts of a cyber attack?

- How should security resources be prioritized for the greatest advantage?

- Is the new data/control worth the security risk?

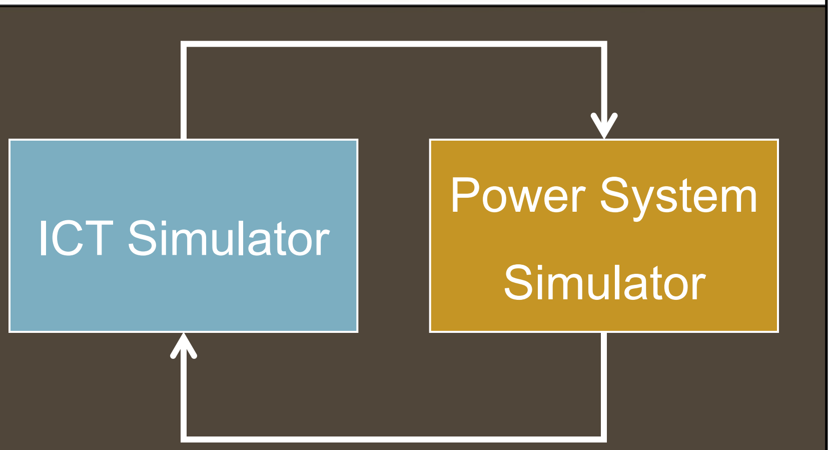
Prior Art





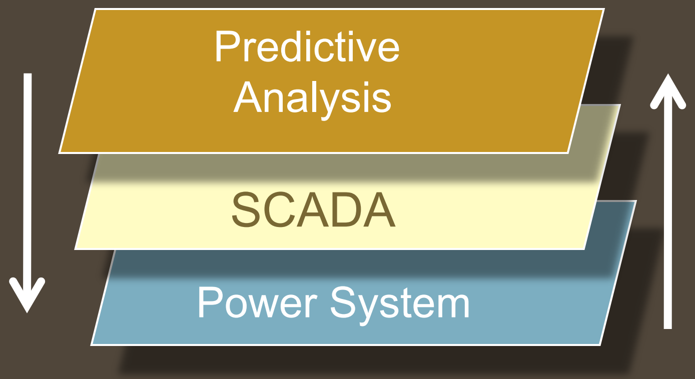
H(s)

G(s)



ICT Simulator

Power System Simulator



Predictive Analysis

SCADA

Power System

Impact Analysis Tool

Wish List

- Tight coupling between cyber and physical components.
- Effective integration of varying cyber-physical time scales to account for attacks on timely delivery
- Accounting of cascading cyber-physical failures to assess critical dependencies

Impact Analysis Tool

Wish List

- Formalism using powerful mathematical constructs
- Flexible granularity of modeling detail to tune complexity
- 'What if' analysis possible

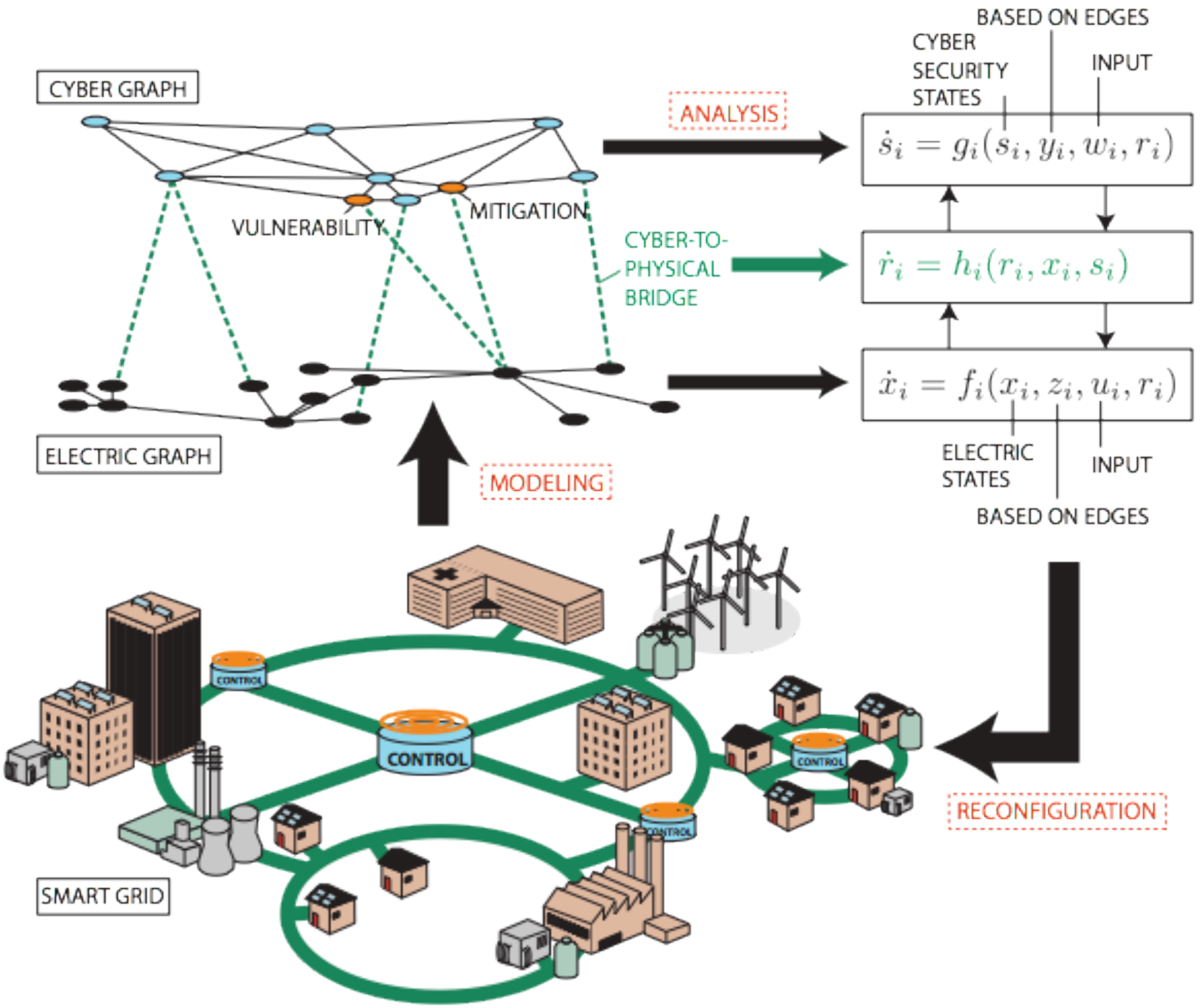
Graphs & Dynamical Systems

Graphs

- Pair wise relations between objects
- Vertices, edges
- Convenient and compact way to show relationships within cyber-physical system

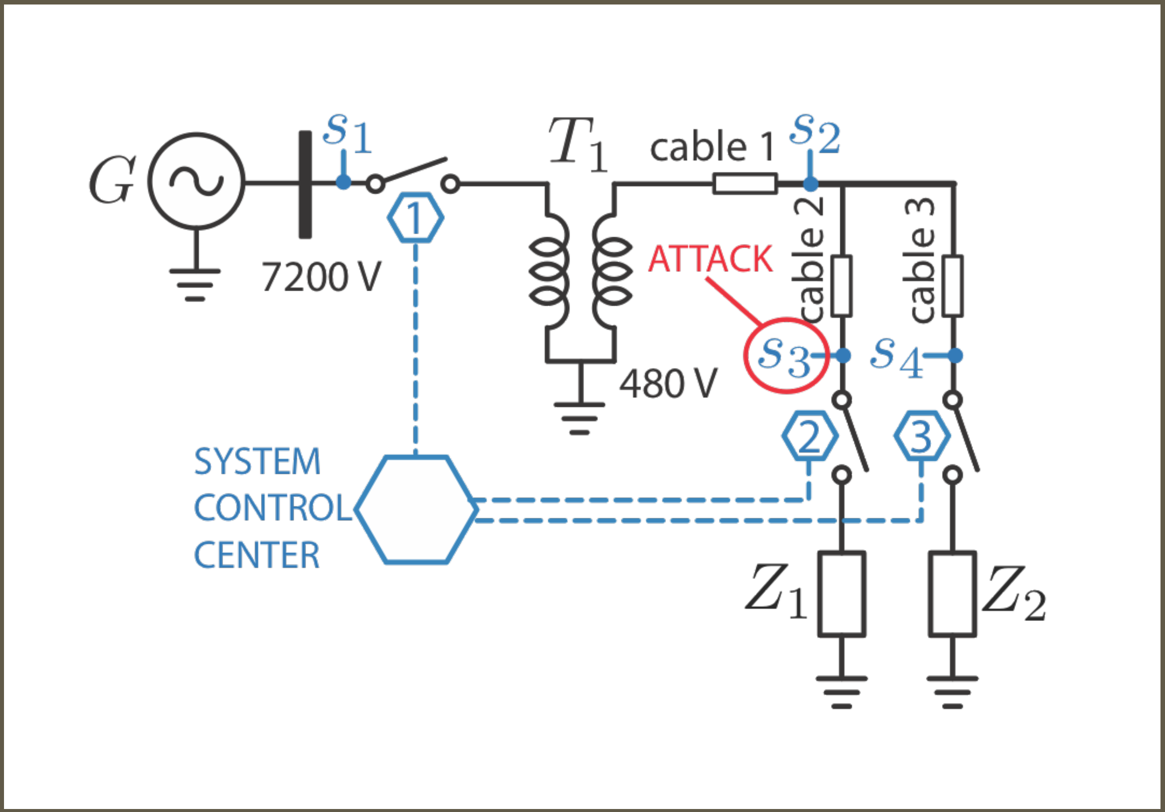
Dynamical Systems

- Describes time evolution of state vector: $$\dot{x} = f(x, u)$$ $$y = g(x, u)$$
- Can account for time-scale separation
- Models physics effectively

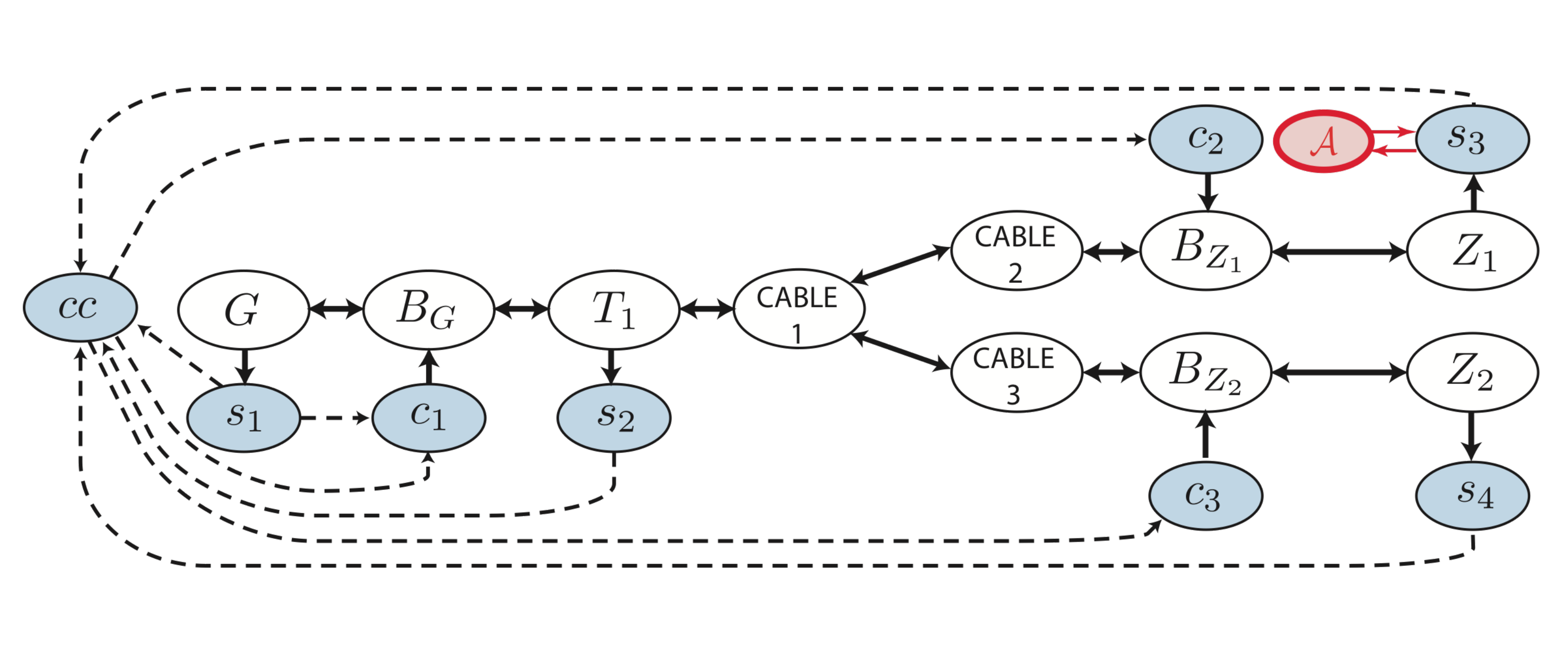


CAPTION: OVERVIEW OF CYBER SECURITY ANALYSIS FRAMEWORK

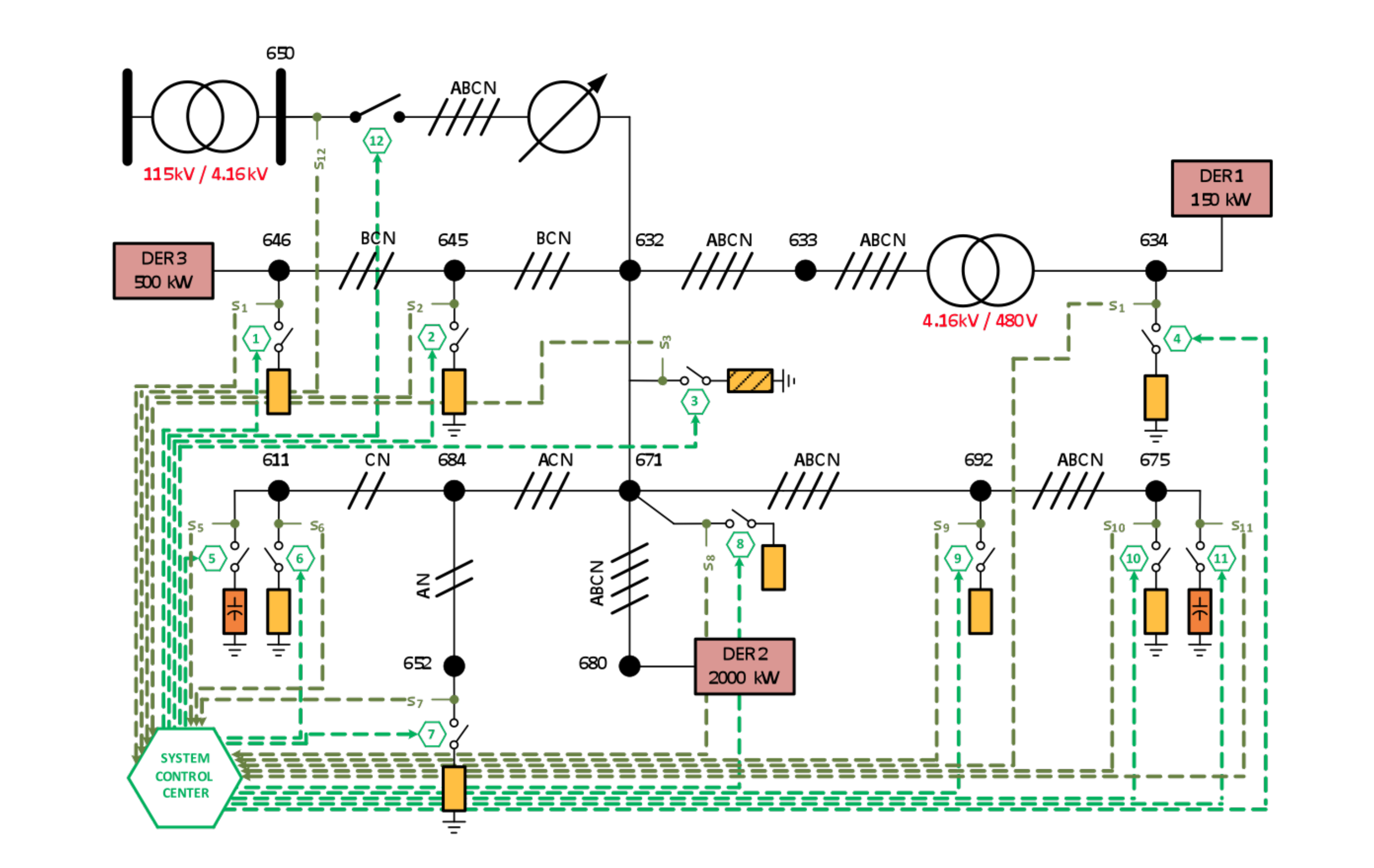
Case Study - Elementary



Graph Model


cc
G
B_G
T_1
CABLE 1
CABLE 2
CABLE 3
B_{Z_1}
B_{Z_2}
Z_1
Z_2
c_1
c_2
c_3
s_1
s_2
s_3
s_4
$\mathcal{A}$

13 Node System



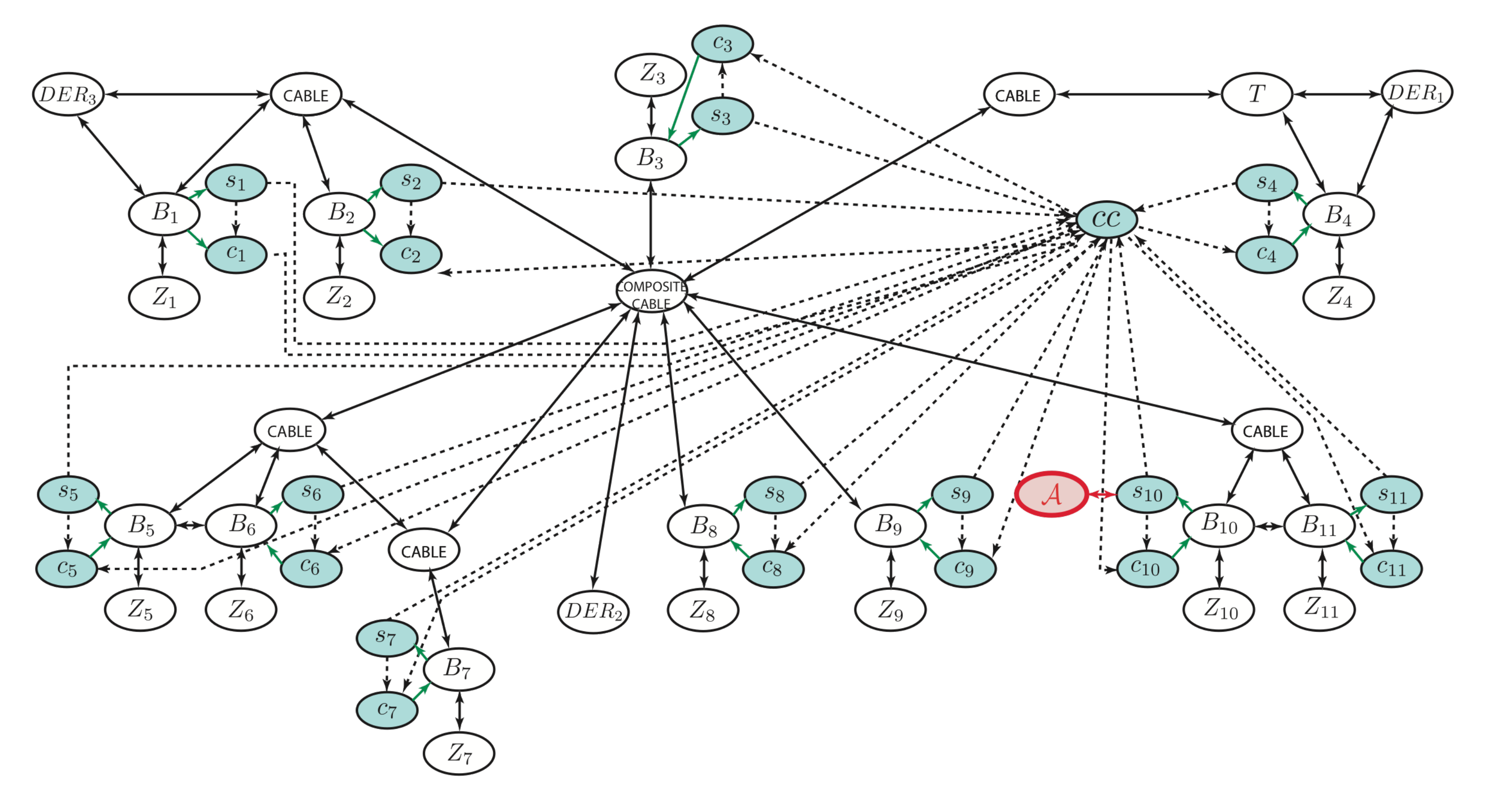
13 Node System

- Based on IEEE 13-node test feeder system
- "Smart" Modifications
  - Measurement device at each node
  - three distributed energy resources (DERs) added
    - DER1 = 150 kW wind power generation unit
    - DER2 = 2000 kW small synch generator
    - DER3 – 500 kW small synch generator
  - Switch added so that system can work in an islanding mode

Load Serving Logic

PRIORITY	NODE	LOAD (kW)	% SYSTEM LOAD
1	671	1155	33.3
2	675	843	24.3
3	632-671	200	5.77
4	692	170	4.92
5	611	170	4.92
6	646	230	6.6
7	645	170	4.9
8	634	400	11.5
9	652	128	3.7

Graph Model


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

General Modeling Challenges

- Two diverse models, one for the electrical grid, the other for the cyber infrastructure must be merged within a unified framework
- Complexity of grid necessitates prioritization of modeling complexity to certain components more than others
- Impact of attack must be appropriately redefined as it affects power delivery not information accuracy or disclosure

Where should we go from here?

- Develop common problem formulations within our community
  - Exciting area, but still ad hoc

- Encourage greater collaboration amongst power system researchers, control theorists and information technology community
  - Excellent area for mathematicians, statisticians, engineers and scientists

References

D. Kundur, F. Xianyong, S. Liu, T. Zourntos and K.L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," *Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm),* Gaithersburg, MD, October 2010.

… and references therein.