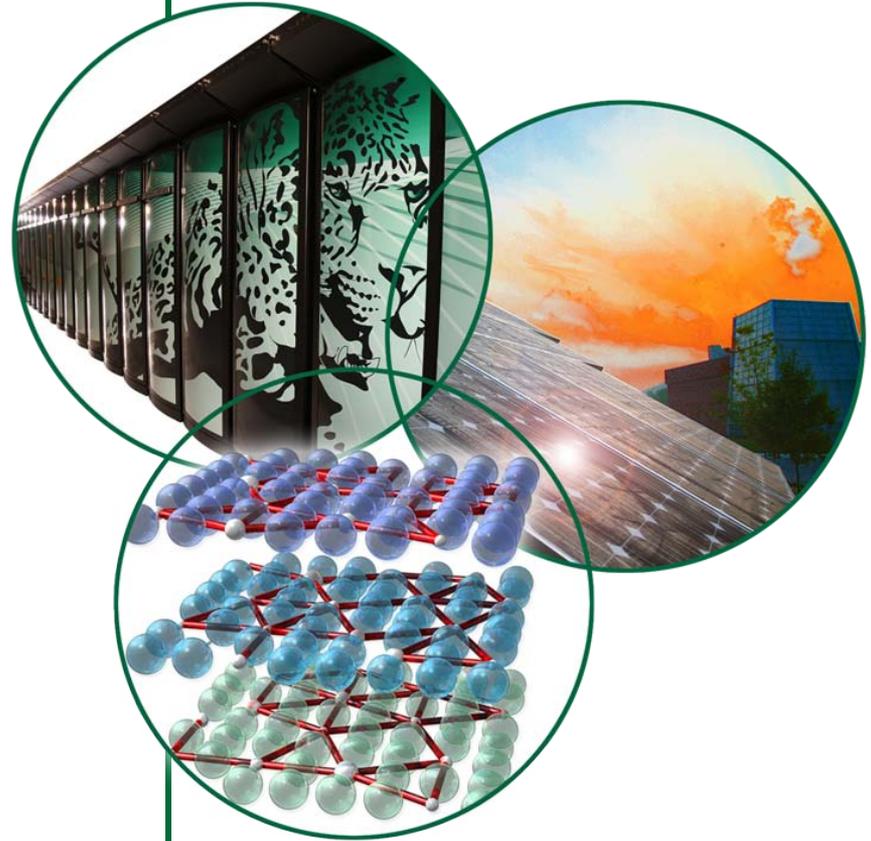


Preventing Cascading Event(s): A Distributed Cyber-Physical Approach



Josef De Vaughn Allen, PhD

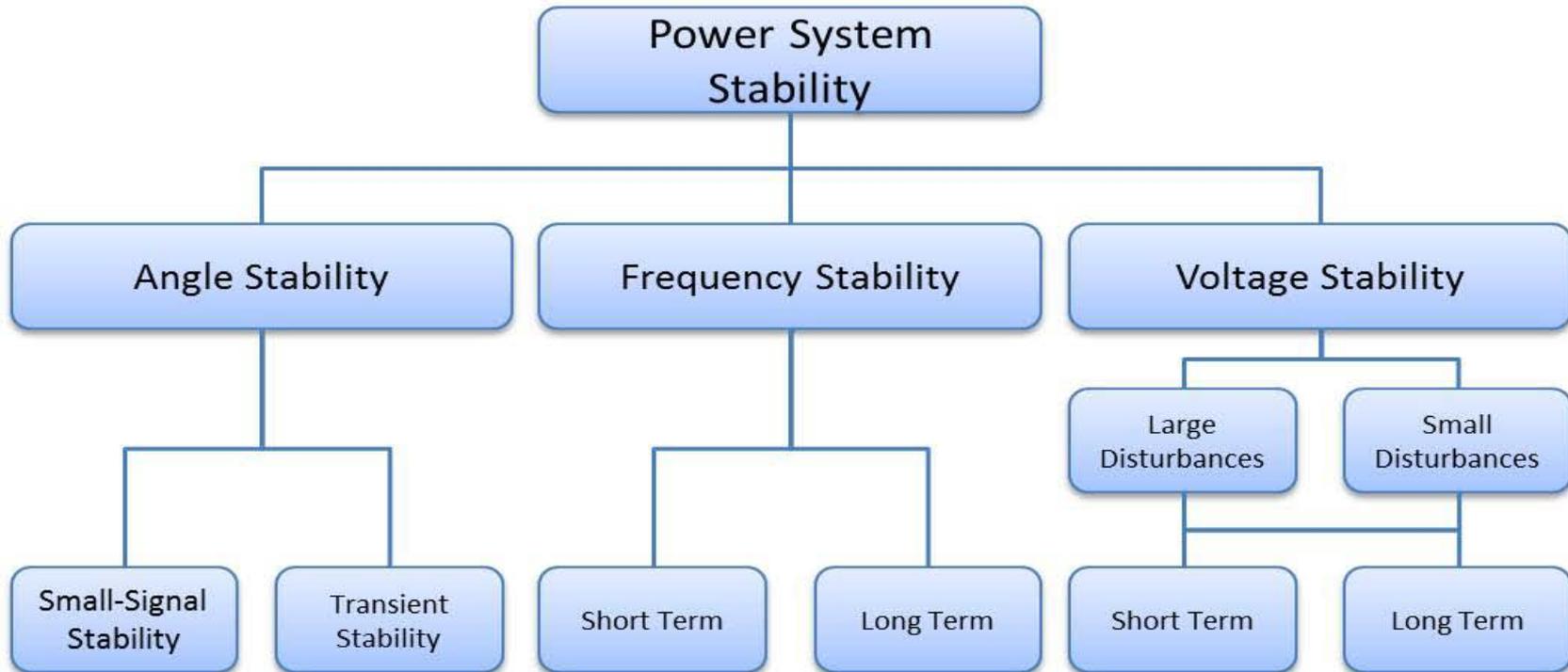
INFOSEC Professional

The Problem

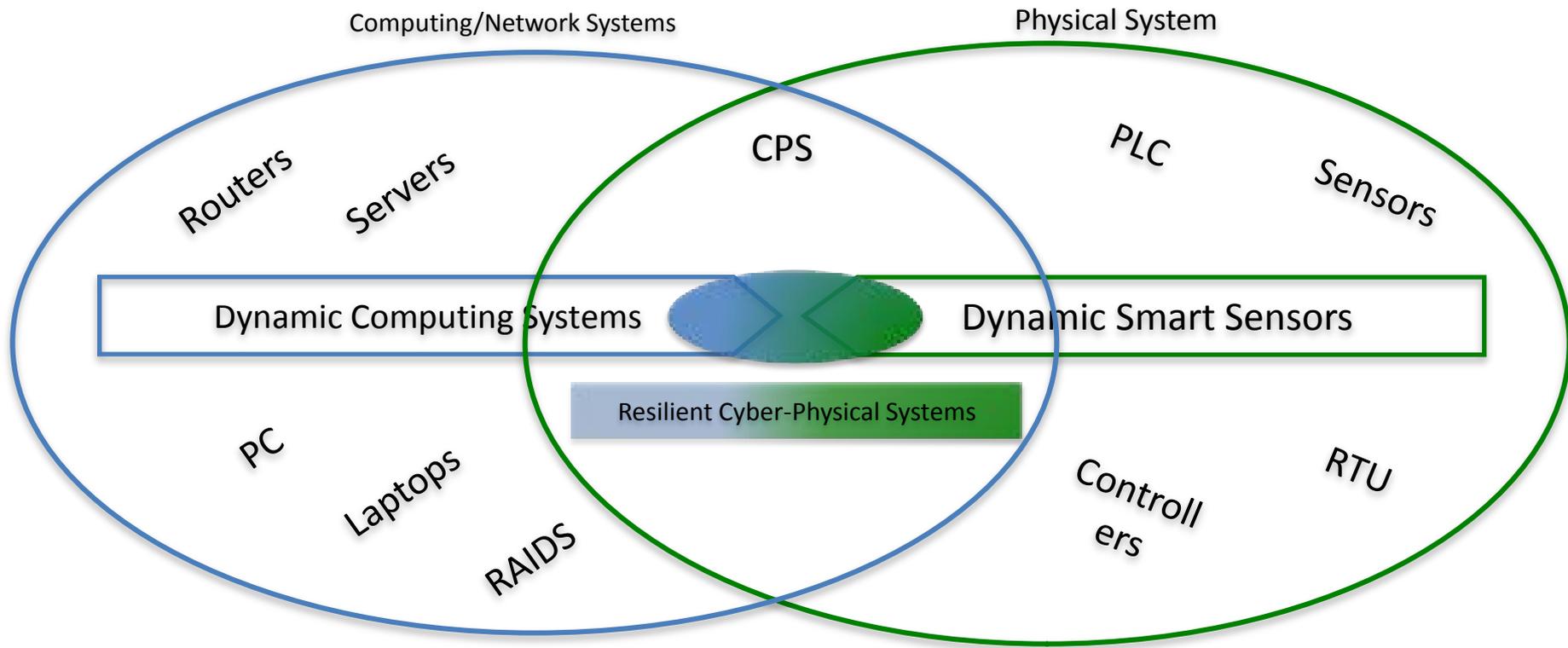
- CIP for of the grid is vulnerable to well-coordinated synchronized attacks
- Time for effective countermeasures to prevent synchronized attack is on the order of ten(s) of power cycles
- Control operators may not have sufficient time to react to such an attack
- Communications and networks to prevent synchronized attacks are not currently robust enough or well understood
- Protective Systems are currently local vice being semi-global
- Global ramifications of Cyber Events are not factored nor fully understood for the Electric Delivery System
 - What may harm one area may be minimal to another zone
- Network Architectures are proprietary per utility, asset owner and/or energy producer
- Sophisticated malware has proven to be successful in penetrating our defenses

How do we respond after getting punched in the face?

Cyber Events



Resilient Cyber-Physical Systems (CPS)



Mission Statement

We propose to define, model and build a “*Cyber-Physical Security Systems to Prevent Cascading Events*” for power systems by making cyber-purposeful attacks on the electric delivery systems less relevant by utilizing and amalgamating static and dynamic data/measurements such that they will be actionable in real time in order to provide resilience to the Grid.

Motivation

- Wide Area Monitoring Systems, WAMS, are being implemented
 - NASPINET, WESCO
 - Perfect Citizen, NSA
- Securing the grid against cyber and physical attacks is our top priority
- Due to the grid's structure, small coordinated attacks can cause disproportional amounts of damage.
- The timeframe to react in these circumstances is on the order of 400ms, therefore we need an automated system.

We Need a Wide Area Actionable System (WAAS)

Mission

- Ensure the reliability of the Electrical Grid during an attack
- Make Cyber and Physical Attacks less Relevant
- Make vulnerabilities less relevant through challenging system operation assumptions
- Maintain operations to some degree of fidelity after an attack
- We must show Resilience and Be Resilient!
- Provide end-to-end solutions for cyber-secure resilient systems

After an attack we must take defensive counter measures such that the mission can continue

Entry Ways

- Current Electric Grid Vulnerabilities
 - Transmission Lines
 - Transmission Substations
 - Distribution Lines
 - Protective Relays
 - SCADA
 - Humans
 - Distribution Substations



Typically unmanned and vulnerable to physical and/or cyber attack

Attack Vectors

- Terrorist/COIN could simultaneously attack unmanned Transmission and distribution assets. Negates the need for sophisticated Cyber Attacks
- Network
 - Hacker remotely monitored VPN connection between two control centers
 - Florida State University Center for Advanced Power Systems FSU/CAPS
- Phishing Malware
 - Users mistakenly download malicious software through email-attachment or website
 - Trustworthy Cyber Infrastructure for the Power Grid "TCIPG"
- Worm
 - Stuxnet, could spread at a high secured site remote site. As described by many there are many ways for Stuxnet to infect a system.
 - Byres Security Incorporated/SCADAHacker

We can and will get hacked! However the payload is typically directed to our
Cyber-Physical Power Assets

Synchronized Attack

- Why

- The Electric Grid is primarily and currently a **Synchronous System** that has a center frequency of 60hz with +/- 0.05hz of Tolerance
- Large Frequency deviation beyond between 0.5hz and 4hz will start Islanding
 - At around 59.3Hz load shedding will occur

- How

- Using aforementioned techniques the Terrorist/COIN is able to store data from several zones.
- Entity sits and waits for all pertinent data to be collected and then perpetrates and **Timed and fairly synchronous attack**

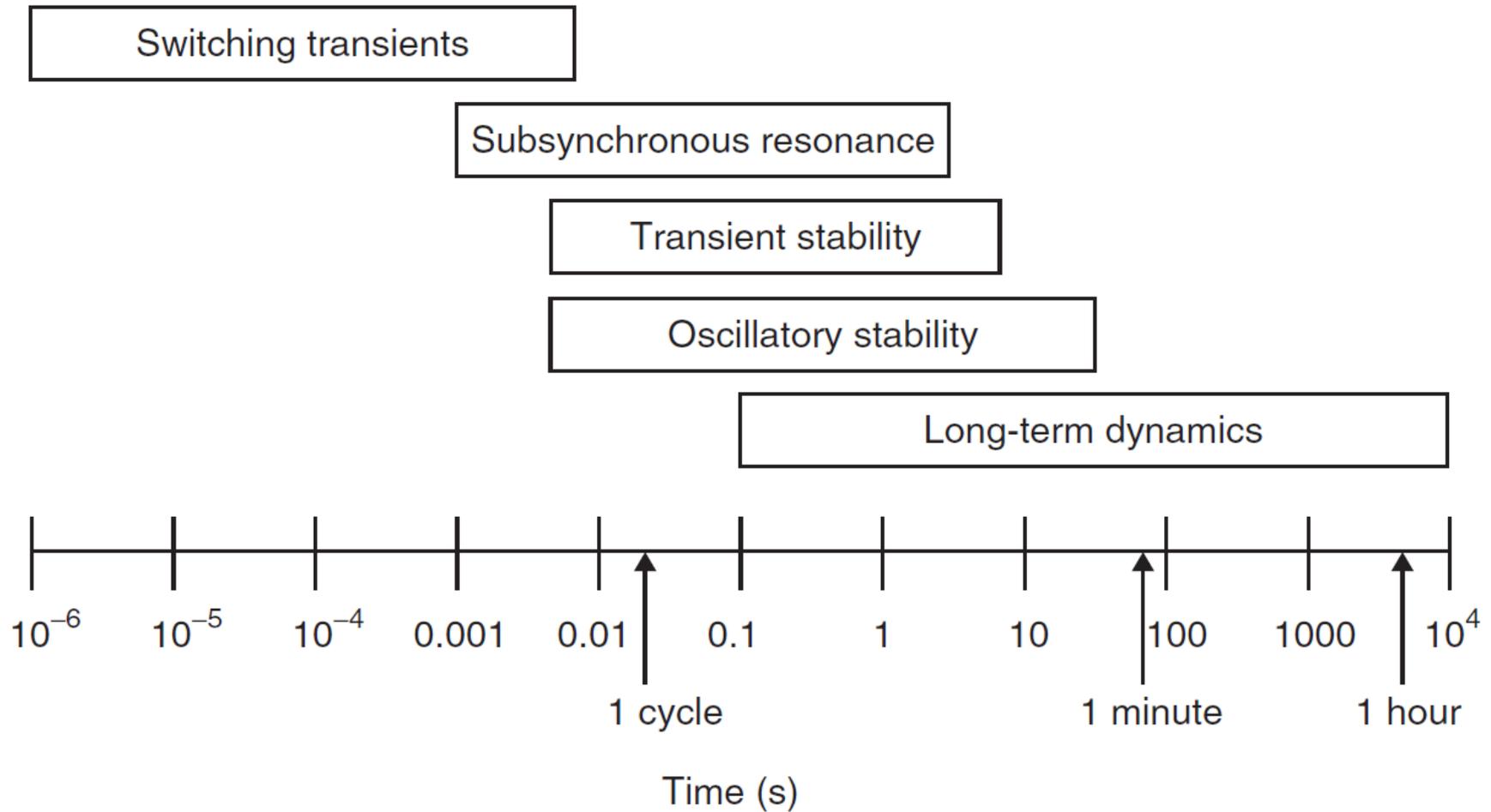
- Consequences

- Due to the speed and precision of the attack N-1, N-2, EMS plans are rendered in-effective

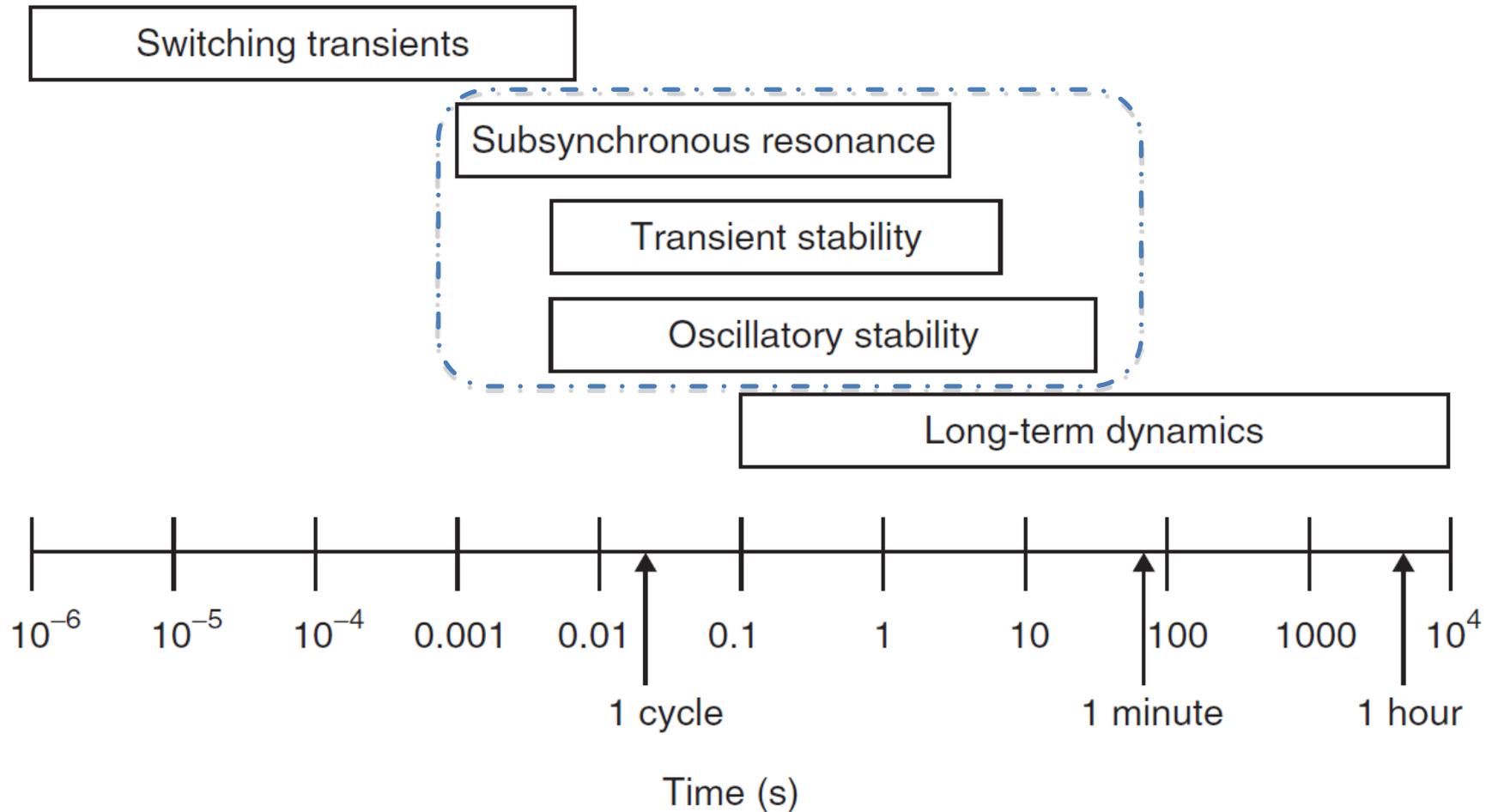
All Are Physics

- Some basic physics of power
 - Electricity travels at $1 / \sqrt{LC} \approx 3 \times 10^8$ m/s
 - Here L and C are the inductance (proportional to the line's permeability) and capacitance (proportional to the line's permittivity) of (overhead) transmission lines
 - Underground cables have a lower speed
 - For electricity with frequency of 60 Hz, for overhead lines, the wavelength is roughly 3100 miles
- Why is it physically possible
 - Instability due to faults induced by attacks happens within around 25 power cycles (about 400 ms)
 - Due largely to stored energy in generators

Timescale of Power System Dynamic Phenomena



Timescale of Power System Dynamic Phenomena





Mathematical Approach

- Time-Domain (T-D) is not sufficient for WAAS
- Direct Methods are not well studied
- We will need to have an amalgamation of the two.
- We propose a polyhedron approximation

Mathematical Modeling

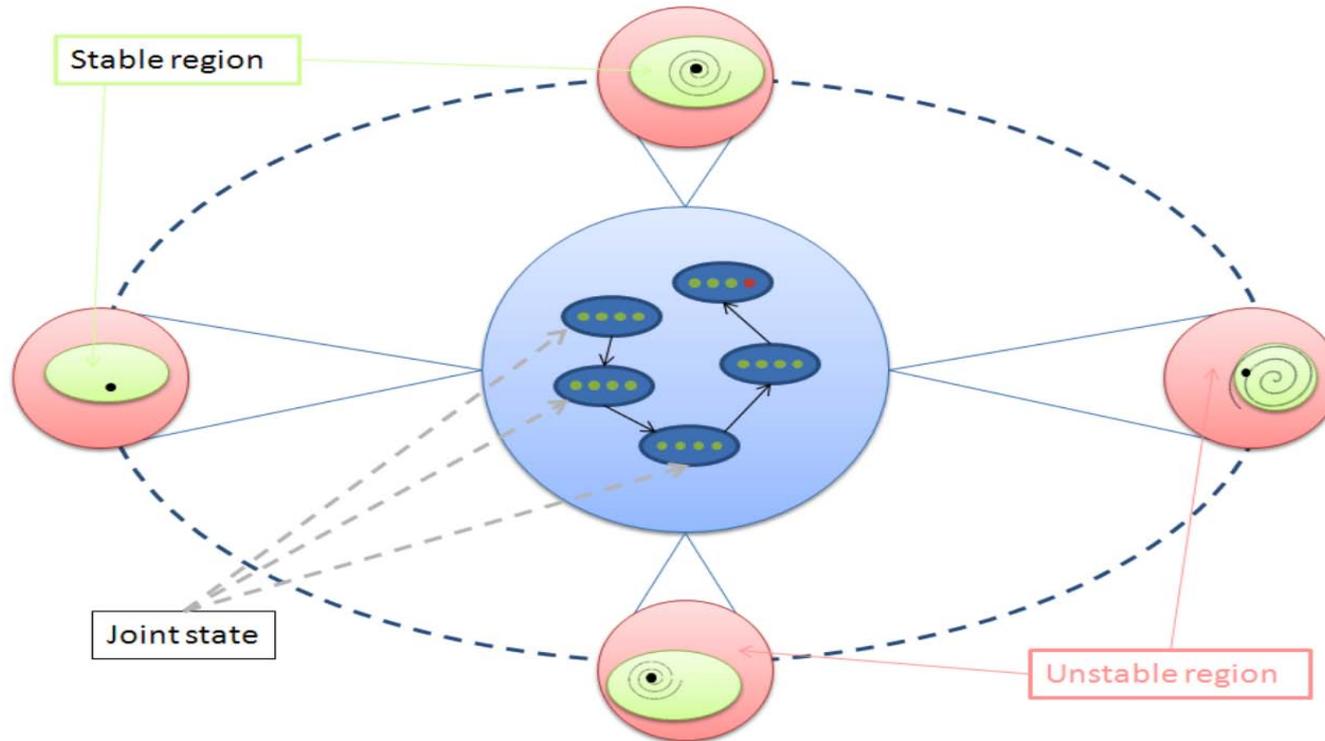
- A power system as a single entity consists of generators, loads, and a transmission system
 - A generator can be described by a model with associated parameters (rotor angle, speed, inertia coefficient, mechanical power and electric power)
 - A load can be described by its admittance, voltage, and current
 - A transmission line can be described by its parameters, voltage, current, and phase angle
 - Mathematically, it can be described by a manifold of high dimensional space with all the physical constraints satisfied

$$\dot{x} = f(x, y, p) \quad (\text{Dynamic modeling})$$

$$0 = g(x, y, p) \quad (\text{Algebraic constraints})$$

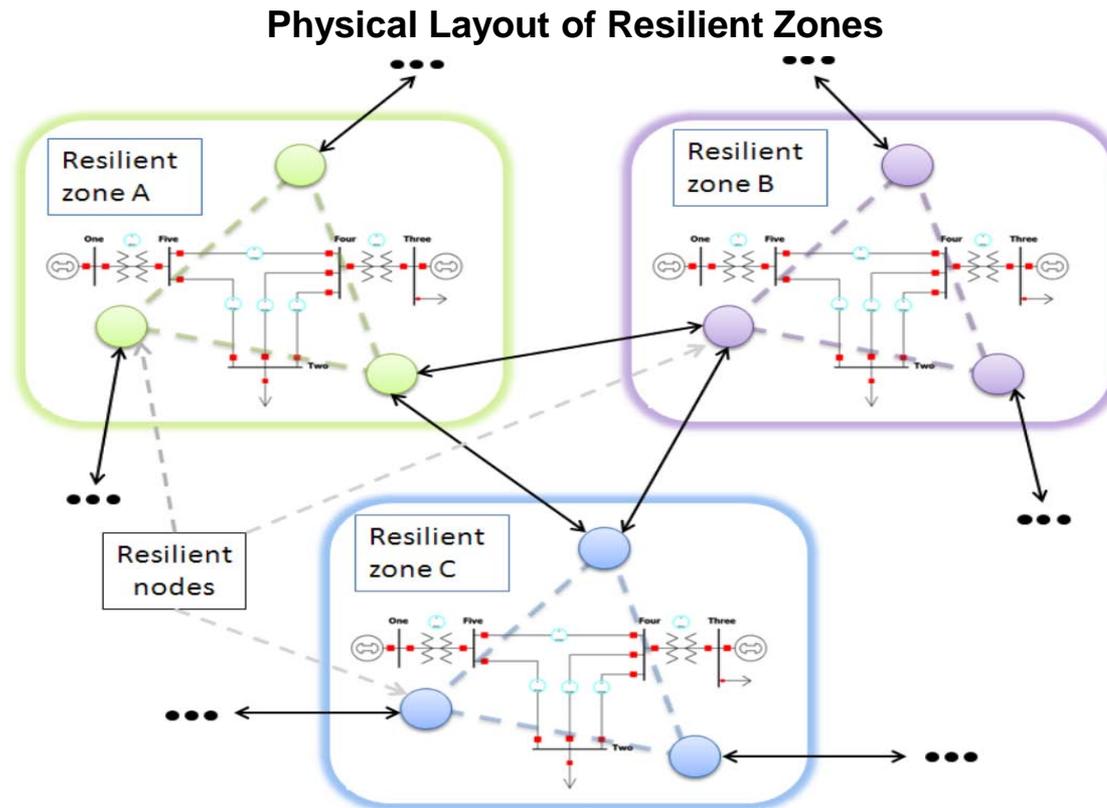
Mathematical Manifold Approach

Illustration of Joint State and Decomposition of Zone Manifolds



As the state of a power system is determined by state variables (that determine the dynamic aspects of power systems (such as generators)), all the possible states form a manifold and the evolution of the power system can be described as a path on the manifold. By decomposing the manifold into relatively independent zones, we can model submanifolds and the minimal interactions among them.

Mathematical Approach



Here zones can be defined in several ways. One way is a graph-cut method. By modeling the grid as a weighted connected graph, where the weight between two nodes is the amount of energy being transferred, we can create clusters by minimizing the inter-cluster energy transfer. In other words, we would like each zone to be as independent as possible to reduce the probability of failure propagation. They can also be defined using the established control zones.

Components of a resilient power grid control

- To achieve resilience, we need to do
 - Data acquisition (measurements taken at strategic locations) (T_{mea} , under 20ms)
 - Communication to resilient control nodes (T_s , around 50ms can be achieved)
 - Power system status estimation and control actions to counter attack if detected (T_{dec})
 - Execution of control actions ($T_s + T_{dev}$ (time for devices to execute, around 70ms))

$$T = T_{mea} + T_s + T_{dec} + T_s + T_{dev} = T_{dec} + 190ms$$

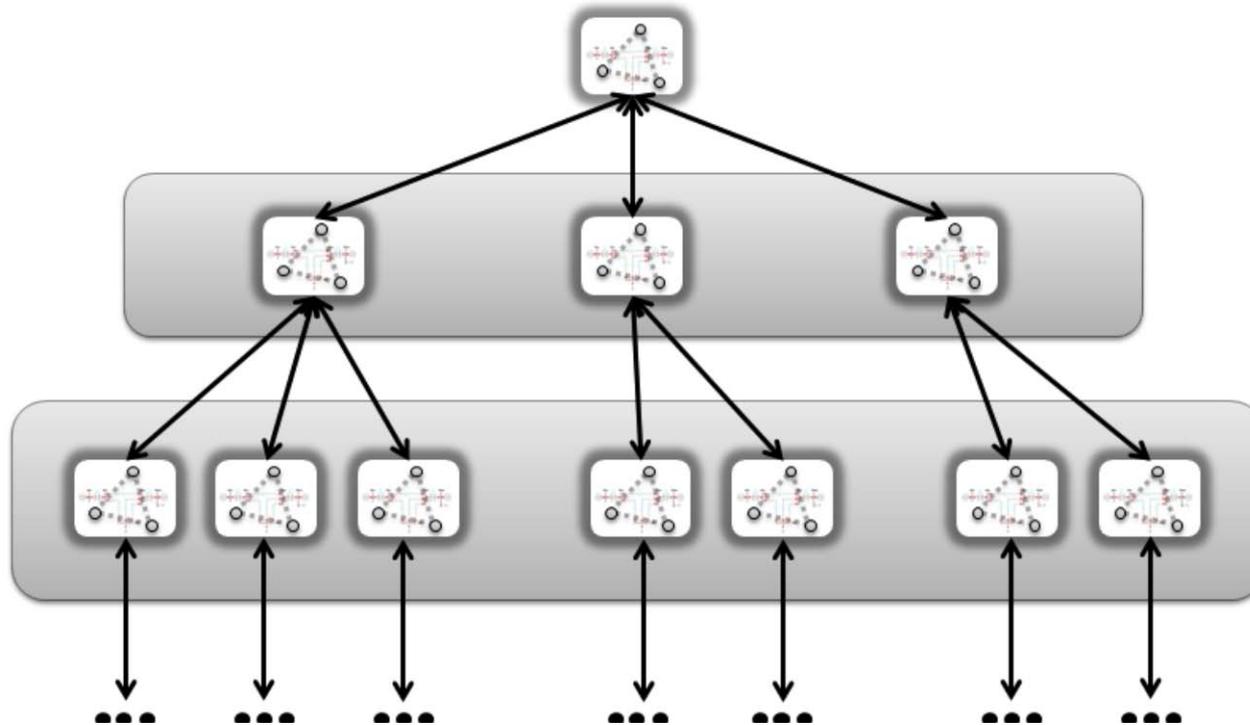
- The entire process must be done before it is too late

Distributed resilience control algorithm

- We will model the power system as resilience zones, which are submanifolds connected by links to neighboring resilience zones
 - The model of a resilience zone consists of the states of its generators, loads, and transmission components
 - One or more resilience nodes are inserted to the resilience zone
 - Communication infrastructure with ultra low latency is built between measurement units and resilience nodes
 - Resilience nodes are also connected with resilience nodes neighboring zones (according to border gateway or other proper protocol)

Communication

Communication Tree for a Resilient Zone for Blocking Cascading Events



The entire interconnect forms a hierarchy of resilient zones.

Each resilient zone has a leader that is responsible for aggregating the zone information to the outside world, receiving zone updates from its peers, and distributing the outside zone updates to devices within its zone.

Resilience node

- A fundamental issue is that resilience control actions must be computed and executed before the system becomes unstable
 - A time-dependent simplified model of the zone will be built using available measurements and generator and system states
 - The model will be used to estimate the time and margin of the system's stability
 - Due to the time constraints, time-domain methods are computationally not feasible
 - We are studying a Single Machine Equivalent (SIME) approach, a hybrid direct and time-domain method
 - Other methods will be studied

After an attack we must take defensive counter measures such that the mission can continue

Challenges that must be overcome

- We need accurate models
- Zones will be different
- System must be semi-global to global
 - Special Protection System (SPS) vice Protective System (PS)
- How do we deal with the enormous amounts of data from WAMS
- What/How many communications protocols should be used
 - IEEE 1451, IEC 61850
 - UDP, IPV6
 - LTE, WiMAX

Implementation issues

- Communication infrastructure must support communication with ultra low latency
 - Resilience zone partition needs to be optimized relative to the communication structure, communication protocol, and power system structure
 - Latency less than 50ms is achievable with optimized protocol and hardware support
 - NASPInet specifications appear to be sufficient
- Candidate resilient Cyber-Physical Control elements/actions can be evaluated in parallel
 - There is no dependency among candidate resilient control actions, that is, the SIME model and the updated resilience margin can be computed in parallel
- As SIME and resilience control actions can be computed within 100ms, attacks with 300ms critical time can be handled

Achieving resilience

- For each resilience zone, the associated SIME model is used to compute the critical clearing time
 - If the zone and neighboring zones are normal, then nothing needs to be done and communicate its status to neighboring zones
 - If there is an attack detected, compute the critical machines (the generators that will be out of control) and then control actions based on neighboring zones
 - Control actions will depend on available power system support, including load redistribution
 - Candidate actions will be evaluated using updated SIME models and resilience margin
 - Note that fast communication between neighboring resilience zones is essential to stop cascading events that could otherwise propagate

We will build a Cyber-Physical Control Elements/Systems

Research issues

- As there is no existing study on modeling and handling synchronized attacks, extensive simulation of "real world models" and emulation need to be studied
 - A key issue is the hard time constrain imposed by the power, power transfer delays as well as communication delays must be modeled accurately
 - Emulation must be done in order to evaluate the feasibility of the proposed approach
- Clearly the distributed SIME and other methods need to be implemented and compared
- We are performing a pilot study regarding a systematic evaluation of the approach

We will build a Cyber-Physical Control Elements/Systems

References and Related Work

- C. M. Davis et al., "SCADA Cyber Security Testbed Development,".
- Jim Y. Cai, Zhenyu Huang, John Hauer, and Ken Martin, "Current Status and Experience of WAMS Implementation in North America," in Transmission and Distribution Conference and Exhibition: Asia and Pacific, Dalian, 2005, pp. 1-7.
- Yusheng Xue, "Some Viewpoint and Experiences on Wide Area Measurement Systems and Wide Area Control Systems," in Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, 2006, pp. 1-6.
- D. Maynor and R. and Graham, "SCADA Security and Terrorism: We're Not Crying Wolf."
- May R Permann and Kenneth Rohde, "Cyber Assessment Methods for SCADA Security," in The 15th Annual joint ISA POWID/EPRI Controls and Instrumentation Conference, 2005.
- David M. Nicol, Charles M. Davis, and Tom Overbye, "A Testbed for Power System Security Evaluation," International Journal of Information and Computer Society, pp. 114-131, 2009.
- J. Tang et al., "The CAPS Power System Security Testbed," in CRIS, Third International Conference on Critical Infrastructures, Alexandria, 2006.
- "Standard CIP-002-4," 2009.
- Eric Byres, Andrew Ginter, and Joel Langill, "How Stuxnet Spreads - A Study of Infection Paths in Best Practice Systems," 2011.
- Duncan Glover, Mulukutla Sarma, Tomas Overbye, "Power System Analysis and Design," 5th Edition, 2011.

References and Related Work

- References

- D. Chang, S. Hines, P. West, G. Tyson, and D. Whalley, “**Program Differentiation**” in the Journal of Circuits, Systems, and Computers, accepted March 2011
- X. Liu, A. Srivastava, and D. L. Wang, “Intrinsic generalization analysis of low dimensional representations,” *Neural Networks*, vol. 16, no. 5/6, pp. 537--545, 2003.
- S. C. Zhu and X. Liu, “Learning in Gibbsian fields: How accurate and how fast can it be?” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 1001--1006, 2002.
- F. Wang, F. Gong, C. Sargor, K. Goseva-Popstojanova, K. S. Trivedi and F. Jou, “**SITAR: A Scalable Intrusion Tolerant Architecture for Distributed Services**”, 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, West Point, New York, June 2001
- João Filipe Ferreira, Jorge Lobo, Jorge Dias. Journal of Real Time Image Processing (2010) **Bayesian real-time perception algorithms on GPU**
- D. Powell and R. Stroud, “Conceptual model and architecture of MAFTIA,” MAFTIA Deliverable D21, 2003.
- N. F. Neves and P. Verissimo, “Complete Specifications of APIs and Protocols for the MAFTIA middleware,” MAFTIA Deliverable D9, 2002.
- M. Dacier (editor), “Design of an Intrusion-Tolerant Intrusion Detection System,” MAFTIA Deliverable D10, 2002.
- M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398-461, 2002.
- J. Levy, H. Saidi, and T. Uribe, “Combining monitors for runtime system verification,” *Electronic Notes in Theoretical Computer Science*, vol. 70, no. 4, 2002.
- Berger, S.; Cáceres, R.; Goldman, K. A.; Perez, R.; Sailer, R. & van Doorn, L. vTPM: Virtualizing the Trusted Platform Module USENIXSS’ 06: Proceedings of the 15th conference on USENIX Security Symposium, USENIX Association, 2006, 2121
- Sadeghi, A.; Scheibel, M.; Stübke, C. & Wolf, M. Play it once again, Sam Enforcing Stateful Licenses on Open Platforms Second Workshop on Advances in Trusted Computing (WATC ’06 Fall), 2006
- Xue, Y., Some Viewpoints and Experiences on Wide Area Measurement Systems and Wide Area Control Systems, 2008 IEEE Journal
- C. Arguayo, J. Reed, Detecting Unauthorized Software Execution in SDR Using Power Fingerprinting, MILCOM 2010
- T. Messerges, E. Dabbish, R. Sloan, “Examining Smart-Card Security under the Threat of Power Analysis Attacks”, *IEEE Transactions on Computers*, Vol 51, No. 4, April 2002

- Related Work

- Very recently there were several noticeable efforts toward intrusion tolerant systems
 - DARPA OASIS (Organically Assured and Survivable Information Systems, <http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8932>)
 - Supported a number of projects on a number of topics related to intrusion tolerant systems
 - DIT (Dependable Intrusion Tolerance, <http://www.csl.sri.com/projects/dit/>)
 - Aimed to develop an intrusion tolerant prototype, in particular, an intrusion tolerant web server
 - MAFTIA (Malicious- and Accidental-Fault Tolerance for Internet Applications) (<http://spiderman-2.laas.fr/TSF/cabernet/maftia/>)
 - It developed a middleware-based intrusion tolerance system using fault-tolerant computing, and computer security techniques
 - ReSIST (Resilience for Survivability in IST) (<http://www.resist-noe.org/>)
 - It explored several areas that can lead to intrusion tolerance

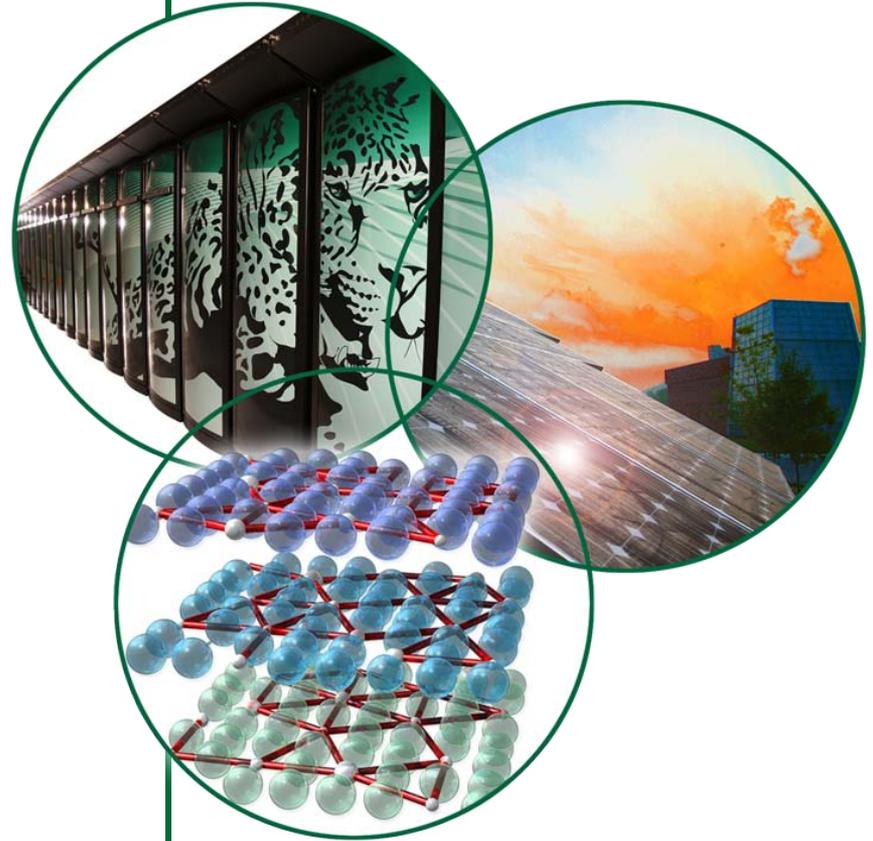
Team

- Oak Ridge National Laboratory
 - Josef D. Allen
 - Travis Smith
 - Joshua Lawrence⁺
 - Sereyvathana Ty⁺
- Florida State University
 - Xiuwen Liu
 - Xin Yuan
 - Ivan Lorenzo
- GE Research
 - Arthur “Chip” Cotton
- Harris Corporation
 - Travis Berrier

⁺ORNL Grid Innovation Leadership Fellows

Cross Discipline Team is Essential for Success!!

Guidance



Guidance

- We want to make sure that our direction makes sense.
- Please give feed back!!
- Presenters:
- Josef D. Allen
 - Email: allenjd@ornl.gov

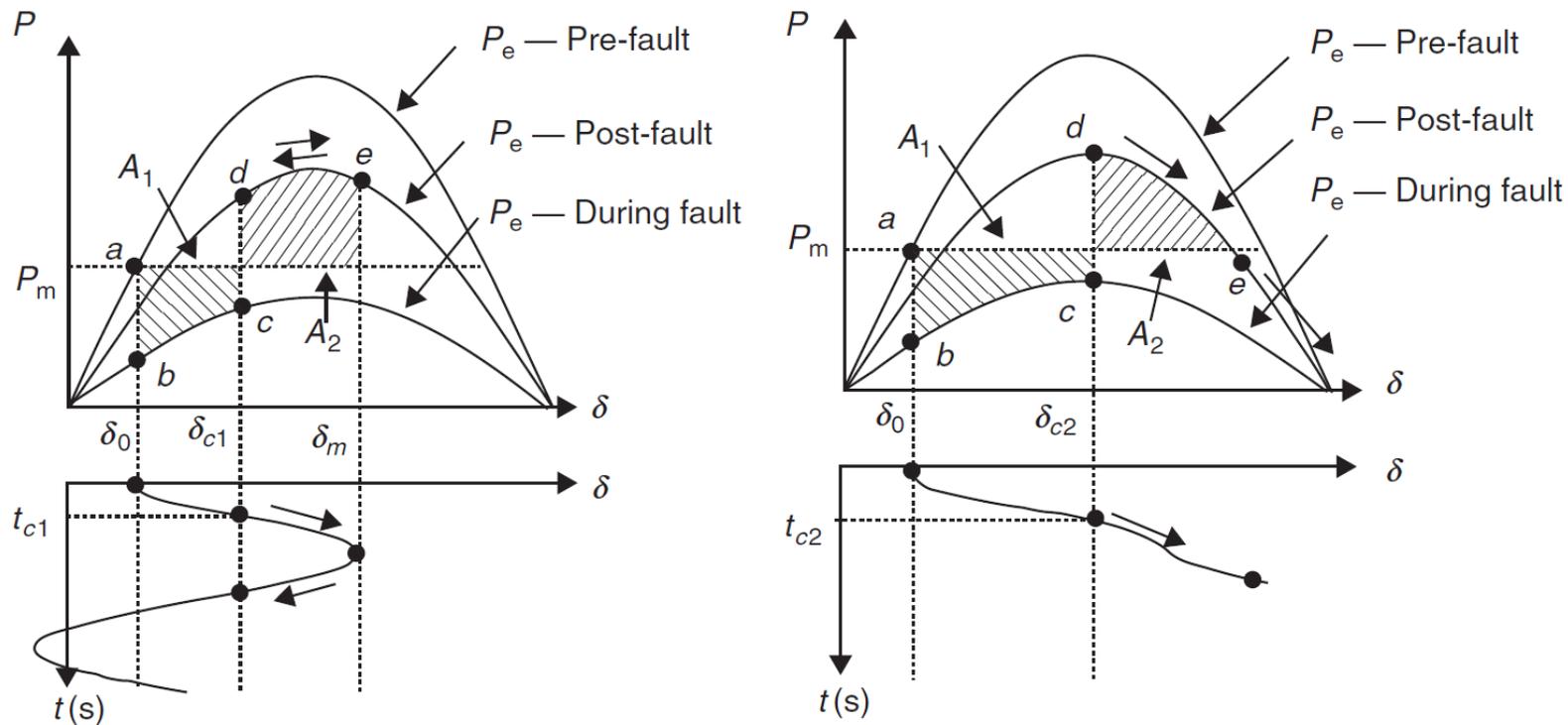
Thank You



Back Up

Distributed SIME method

- SIME uses the equal area criterion that allows the estimation of the stable margin accurately and efficiently
 - Based on a one-machine infinite bus model (OMIB) system



- Illustrations from “Power system stability and control” (editor, L. L. Grigsby, editor, CRC Press, 2007)