What's the big deal with Cybersecurity and Power Systems?

CySER Summer 2023 Workshop

May 30, 2023

Dr. Noel N. Schulz

Edmund O. Schweitzer III Chair in

Power Apparatus and Systems

Chief Scientist Joint Appointment, PNNL

Co-Director, PNNL/WSU Advanced Grid Institute (AGI)

Washington State University Pullman

Noel.Schulz@wsu.edu 509-335-0980 (o)

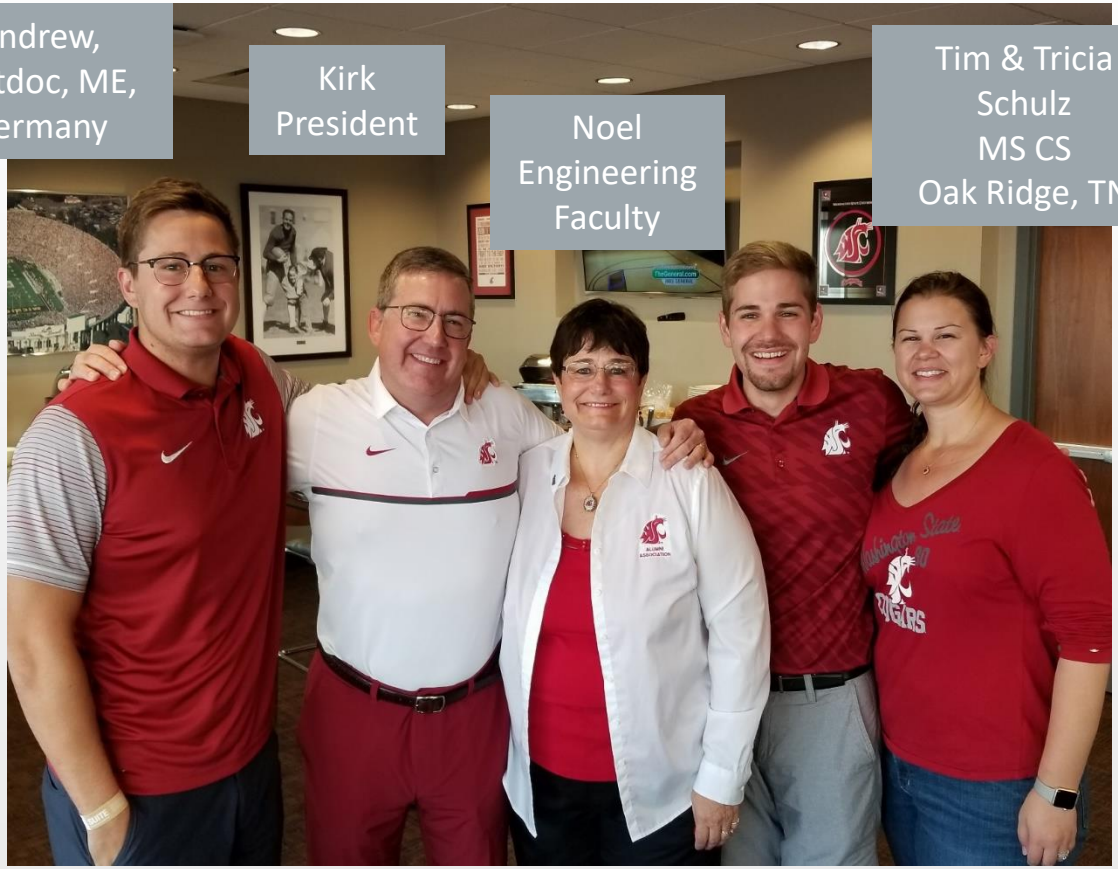
Outline

- My Background
- Power Systems Terminology
  - Smart Grid
  - Resilience
- Intersection of Power Systems and Cybersecurity
- Smart Distribution Power Systems & Microgrids
- Industrial Control Systems and Cybersecurity

My Family

My parents

Dad – EE Professor
Mom – Elementary School Teacher



My Background

- BS and MS, Electrical Engineering
- PhD, EE with CS minor
- Faculty Experience at
  - Virginia Tech
  - University of North Dakota
  - Michigan Tech
  - Mississippi State
  - Kansas State
  - Washington State





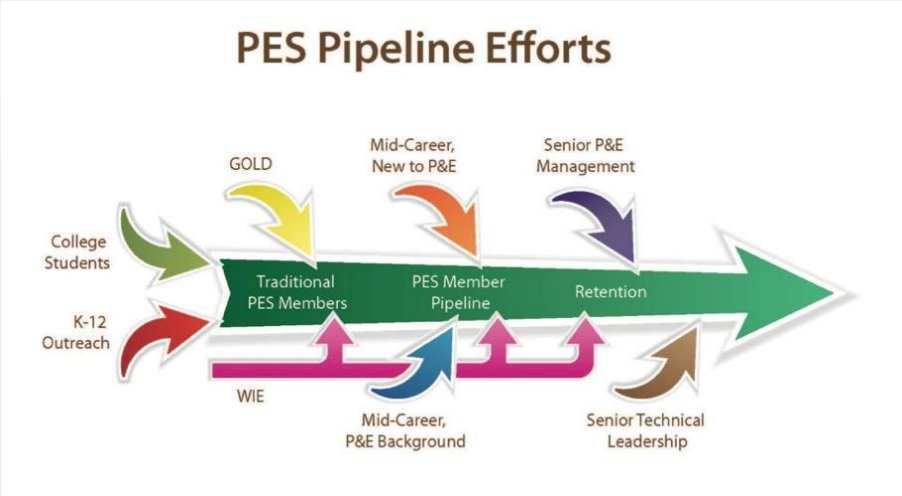



My Research Areas

- Integration of DER into distribution systems including storage and electric vehicles
- Intelligent system applications in power system design, contol and operation
- Outage and Storm Management including smart metering and resilience efforts
- Rural electrification and Microgrids
- Shipboard Power Systems

IEEE Power & Energy Society
President Experiences -2012-2013

- Technical Society within IEEE (over 450,000 members worldwide)
- Over 37,000 members worldwide
- Traveled over 240k air miles over 2 years including 6 continents, interacting with students and engineering professionals from all around the world
- Two initiatives – pipeline support and women in power



Power Systems and Cybersecurity

Power Systems Background

Smart Grids

Microgrids

Power Grid Security

Resilience in Power Systems

What are Smart Grids?

Blackout of 2003

- 50 Million People in US and Canada
- 11 Deaths and $6B cost

- 46 recommendations

https://energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and

Why the changes in electric power in early 2000s?

- Advances in computational capabilities and speeds
- Advances in monitoring and sensors
- Advances in power electronics and interfaces
- Advances in alternative energy

Cybersecurity implications

- Blackout of 2003

Energy Independence and Security Act of 2007

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf

TITLE XIII—SMART GRID

- Sec. 1301. Statement of policy on modernization of electricity grid.
- Sec. 1302. Smart grid system report.
- Sec. 1303. Smart grid advisory committee and smart grid task force.
- Sec. 1304. Smart grid technology research, development, and demonstration.
- Sec. 1305. Smart grid interoperability framework.
- Sec. 1306. Federal matching fund for smart grid investment costs.
- Sec. 1307. State consideration of smart grid.
- Sec. 1308. Study of the effect of private wire laws on the development of combined heat and power facilities.
- Sec. 1309. DOE study of security attributes of smart grid systems.

Smart Grid – According to Energy Independence and Security Act of 2007

It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.

(2) Dynamic optimization of grid operations and resources, with full cyber-security.

(3) Deployment and integration of distributed resources and generation, including renewable resources.

(4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.

(5) Deployment of ''smart'' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.

(6) Integration of ''smart'' appliances and consumer devices.

(7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.

(8) Provision to consumers of timely information and control options.

(9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

(10) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services.

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.

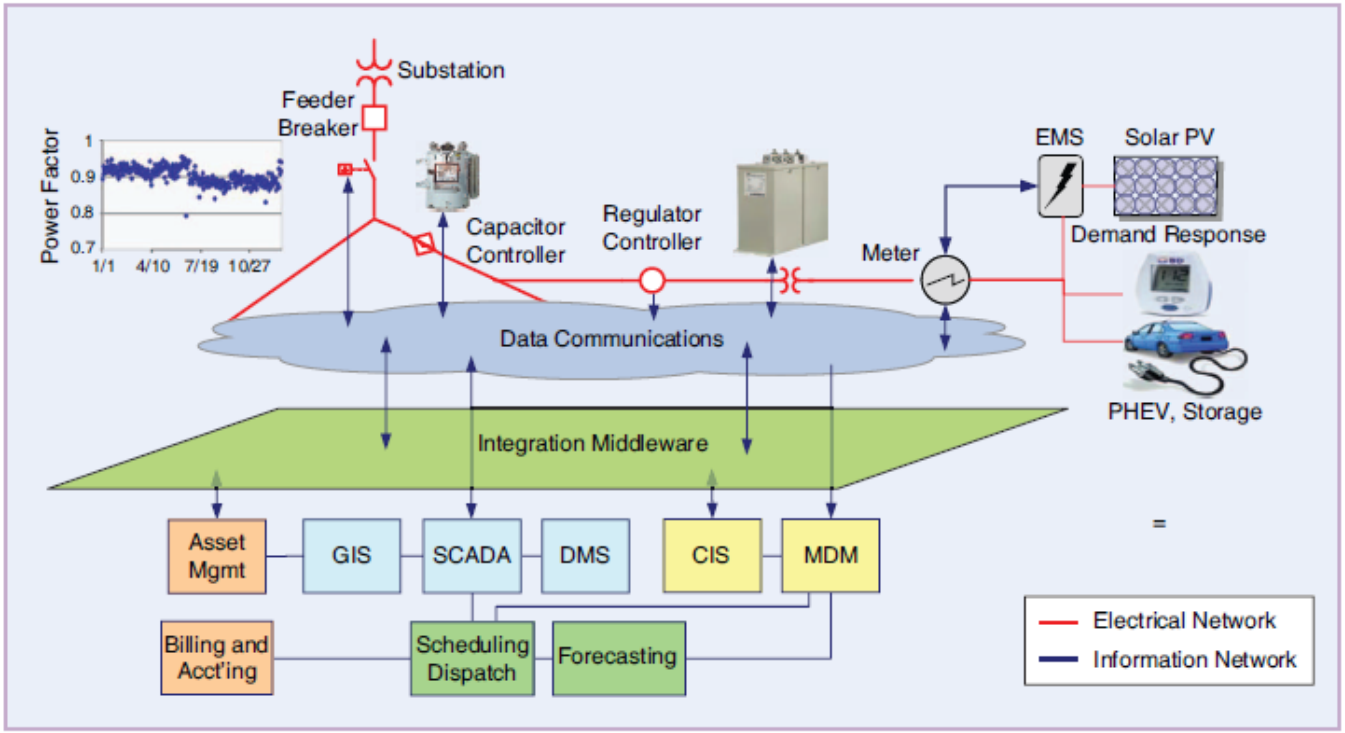


figure 9. Systems required to support the high penetration of distributed resources.

North America Electric Reliability Corporation

CIP 002-011 (Version 5): Overview

NERC CIP CYBER SECURITY STANDARDS Version 5
Ten Standards /43 Requirements

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009	CIP-010	CIP-011
CRITICAL CYBER ASSETS	SECURITY MANAGEMENT CONTROLS	PERSONNEL AND TRAINING	ELECTRONIC SECURITY	PHYSICAL SECURITY	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING AND RESPONSE PLANNING	RECOVERY PLANS FOR BES CYBER ASSETS	CONFIG. CHANGE & VULN. ASSESS.	INFORMATION PROTECTION
1. LOW, MEDIUM, HIGH CRITERIA 2. 15-MONTH REVIEW	1. CYBER SECURITY POLICY FOR HIGH MEDIUM 2. CYBER SECURITY POLICY FOR LOW 3. LEADERSHIP 4. DOCUMENT DELEGATES	1. AWARENESS 2. TRAINING 3. PERSONNEL RISK ASSESSMENT 4. ACCESS 5. ACCESS REVOCATION PROGRAM	1. ELECTRONIC SECURITY PERIMETER 2. REMOTE ACCESS MANAGEMENT	1. PLAN 2. VISTOR CONTROL PLAN 3. MAINTE-NANCE AND TESTING	1. PORTS AND SERVICES 2. SECURITY PATCH MANAGEMENT 3. MALICIOUS CODE PREVENTION 4. SECURITY EVENT MONITORING 5. SYSTEM ACCESS CONTROLS	1. CYBER SECURITY INCIDENT RESPONSE PLAN 2. IMPLEMEN-TATION AND TESTING OF CYBER SECURITY INCIDENT RESPONSE PLANS 3. CYBER SECURITY INCIDENT RESPONSE PLAN REVIEW	1. RECOVERY PLANS 2. RECOVERY PLAN IMPLEMEN-TATION AND TESTING 3. RECOVERY PLAN REVIEW, UPDATE, AND COMMUNI-CATION	1. CONFIGUR-ATION CHANGE MANAGE-MENT PROCESS 2. CONFIGUR-ATION MONITOR-ING 3. VULNER-ABILITY ASSESS-MENTS	1. INFORMATION PROTECTION PROCESS 2. BES CYBER ASSET REUSE AND DISPOSAL

CIP = Critical Infrastructure Protection.
NERC = North American Electric Reliability Corporation.
BES = Bulk Electric System

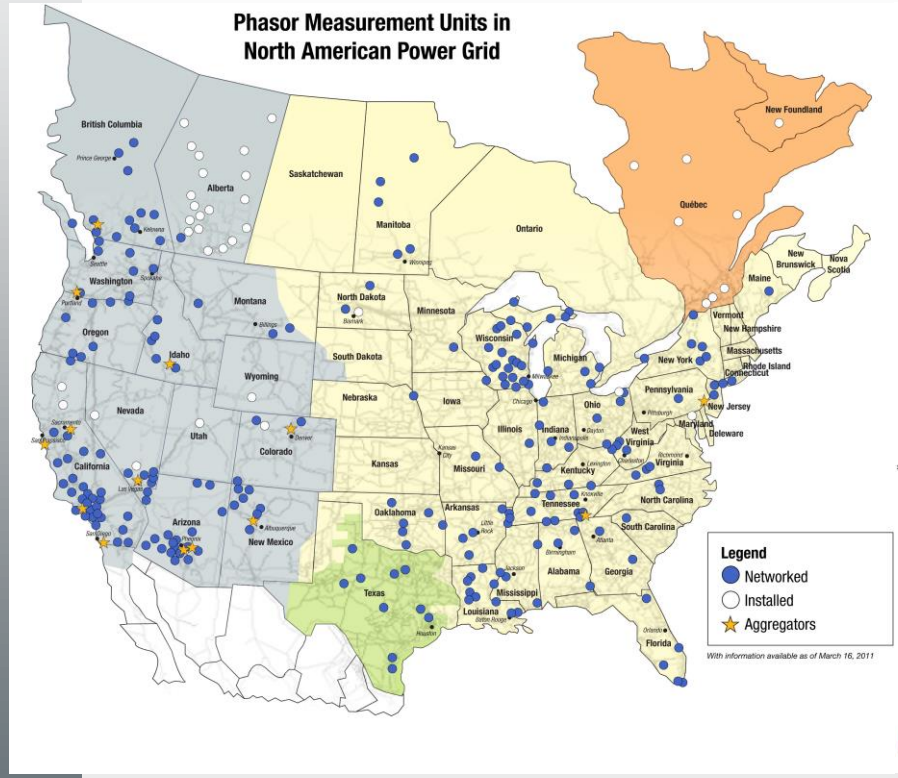
Source: NERC (www.nerc.com)

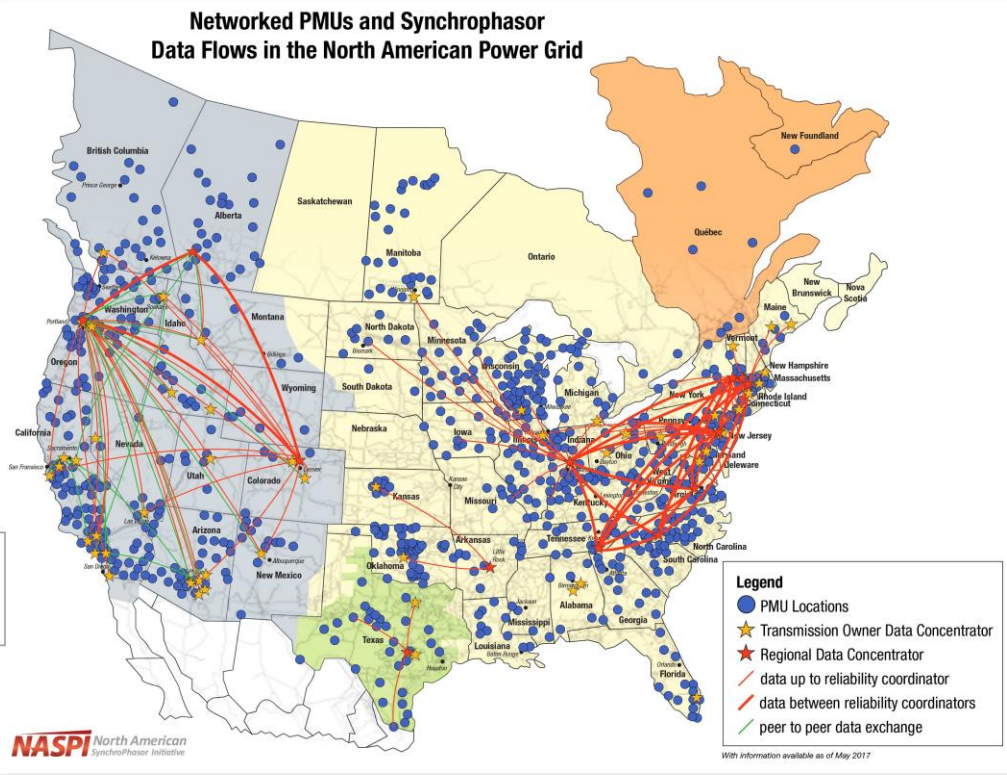
PAS

NovaTech

http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.

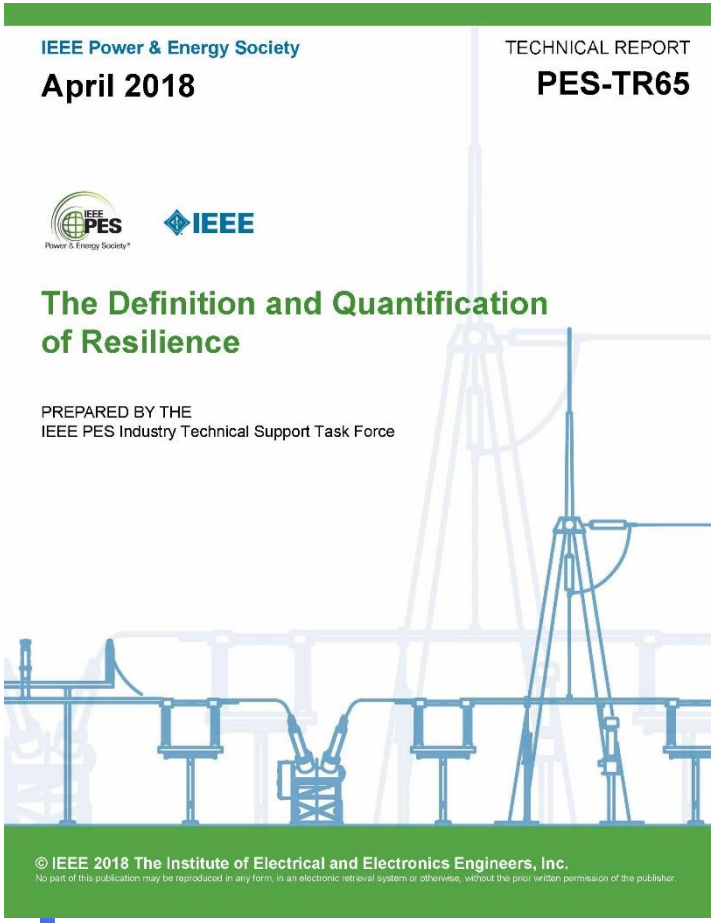




2011

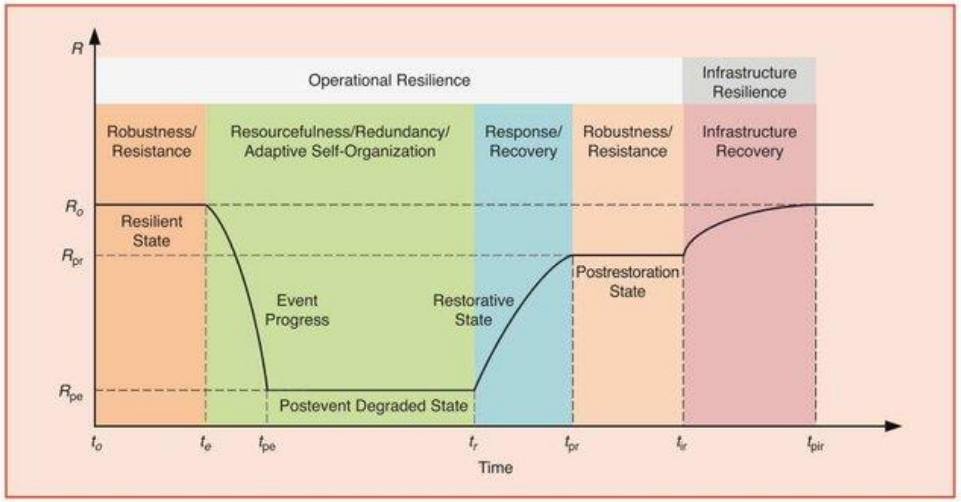
2017

What is Resilience Related to Power Grid?



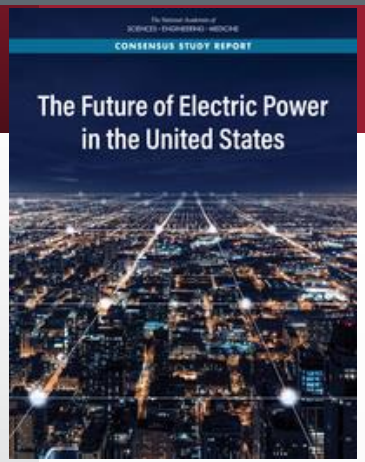
Resilience Definition

The definition presented to the TF:
"The ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event."



M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems", IEEE Transactions on Power Systems, vol. 32, no. 6, November 2017

Intersection of Power System and Cybersecurity
-
Recent Thoughts



The Future of Electric Power in the US | National Academies

6

Creating a More Secure and Resilient Power System

EVOLUTION OF THE GRID AND CYBERSECURITY THREATS AND CHALLENGES

Grid Control Systems

To improve efficiency and reliability, the electric grid has incorporated automated industrial control systems (ICS). The often unique and proprietary protocols, networks, and specialized devices used in an ICS environment are collectively referred to as operational technology (OT) and may include legacy and modern components. OT systems differ in important ways from conventional information technology (IT) systems. While IT systems focus on storage, management and movement of digital data, OT systems monitor and control physical processes using a tight coupling of digital communications and physical components to generate a physical action. Unlike most IT systems and some other cyber-physical systems, grid OT systems are typically 24/7 operational systems and significant negative consequences may result if they are unavailable for even short periods of time.

The first generation of wide-area ICS, supervisory control and data acquisition (SCADA) systems, was based on centralized mainframe computing technology in the mid-20th century. At that time, cyber threats were not a major concern. The OT communications networking protocols and processes were vendor-specific and custom-designed to meet the unique requirements of their function on the grid. The information communicated from sensors was openly passed to controllers, and actuators would respond to any properly formatted command. Typically, these OT devices were isolated from the IT and corporate environment. Confidentiality was not a concern, integrity was managed by message authentication protocols to protect primarily against noisy data transmission environments not malicious intent, and reliability and availability were ensured through redundancy. The ICT architecture for control systems was designed and deployed in an environment that assumed trustworthy behavior from all who interacted with it, and the protocols and processes emphasized deterministic, low-latency operations, not security.

As cybersecurity became a concern, initial OT security strategies emphasized prevention tactics and perimeter defenses. Because ICS were originally designed to operate in an environment of assumed trust, the security architecture focused on creating an electronic security perimeter that would ensure a trusted space within which the OT and control systems could function isolated from the threats. Security relied on protection defenses such as firewalls, "demilitarized zones," and "air gaps" to prevent attackers seeking to compromise the availability, integrity, or confidentiality of critical systems from gaining access to the OTnetworks, systems and assets inside the perimeter.

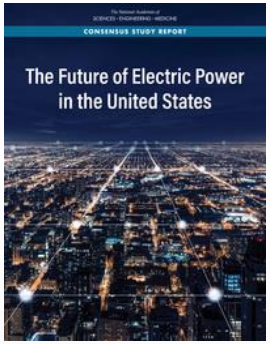
By the early 21st century, automation of grid ICS using ICT increased dramatically by exploiting low-cost Internet-based ICT. One notable example is automated metering—for example, advanced metering infrastructure (AMI) that enables two-way digital communication between the meter and the utility. The deployment of more sophisticated ICS has resulted in reliability and efficiency gains. However, as control systems and networks became more complicated, the underpinning ICT supporting those systems increased in complexity and in cybersecurity risks. Cybersecurity practices have changed over this time to address these new risks, but additional changes will be needed to keep up with future challenges.

Cybersecurity Challenges Presented by the Evolving Grid

TABLE 6.2 Traditional Approaches to Grid Cybersecurity and the Cybersecurity Vulnerabilities Associated with Individual Approaches Resulting from Recent and Future Changes to the Grid

Traditional Approach to Grid Cybersecurity	Cybersecurity Vulnerabilities Resulting from Recent and Potential Future Changes
Emphasis on perimeter security	Significant reduction in the degree of isolation of the industrial control system (ICS) from the outside world. Perimeter security is no longer an effective sole defense.
Operational technology (OT) in an environment of implicit trust surrounded by a heavily defended perimeter	More emphasis will be placed on segmentation or micro-segmentation of internal environments and implementation of machine learning/artificial intelligence algorithms to monitor performance.
Self-contained OT systems with no connection to external or corporate systems	More requirements for external connections, including control systems that require real-time contact with external parties, market-forced transitions to cloud-based systems, inter-utility connections to renewable energy sources, vendor requirements for remote access to update assets, etc.
OT-pure systems	Increased integration of information technology (IT) and information and communications technologies (ICT) driven by technologies and trends discussed in Chapter 5 increases the attack surface and exposure of OT systems to vulnerabilities new to those systems, such as vulnerabilities in the underlying operating systems of Microsoft or Linux.
Energy generation, transmission, and distribution primarily owned and operated by utilities	Increased participation by a highly diverse population of stakeholders with unclear roles and responsibilities for cybersecurity.
Centralized control of energy transactions	Decentralized distributed control will require additional and novel cybersecurity paradigms. For example, centralized control emphasizing a locked-down perimeter defense cannot work with a distributed control system that includes prosumers and microgrids.
Prevention of reliability impacts on the bulk power system owing to cybersecurity incidents primarily under utility control	Increasing interdependencies on other critical infrastructures, alternative energy sources such as renewables, and stakeholders that have few or no equivalent reliability or resilience requirements or expectations will significantly increase risks to utility operations and reliability.
Privately and publicly owned communications used and controlled by utilities	Increased use of commercially owned communications systems by new technologies and associated stakeholders that connect to the grid with unclear and undefined roles and responsibilities for cybersecurity of those communication systems.
OT and ICT on-premises	Increased use of cloud services by vendors for some utility functions is shifting the market and limiting availability of on-premises solutions and options that enable more utility control over cybersecurity practices.
Domestic supply chain as the primary source of physical and cyber assets used in the grid	Increasing reliance on international supply chains creating cybersecurity concerns about risks such as malicious implanted hardware, software, and/or firmware elements.
Innovation driven domestically resulting in domestic product development and domestic vendor standards	Increased internationally driven innovation changing the focus of product and services development and associated vendor standards, etc., resulting in potential mismatches between domestic utility requirements for cybersecurity products and internationally driven standards and product development.
Reliance on Indicators of Compromise to detect threats	Looking for indictors of things that are known to be bad will continue to be important but will not be sufficient. More of the advanced threats can only be detected by analyzing patterns of multiple events and finding evidence of behaviors indicative of a stress or attack.
Adversaries using malware as a primary tactic	Increasing use of native functionality of an ICS to implement attack goals rather than malware (also known as "living off the land").
Cryptography as a cybersecurity tool	Is one tool as part of an overall solution, and will likely be ineffective in its current form if quantum computing advances significantly.
Reliance on passwords for authentication	Increasing use of biometric-based (i.e., "something you are") and ownership-based (i.e., "something you have") for authentication.
Emphasis on prevention of incidents	To detect more sophisticated adversaries, more focus will be needed: to advance utility capabilities for detection and root cause analysis, which can drive resilience and response actions; and, to develop stronger capabilities for containment, remediation and recovery.

MAJOR NEEDS FOR THE FUTURE U.S. ELECTRIC POWER SYSTEM



- **Need #1: Improve our understanding of how the electric power system is evolving.** The U.S. electric system is undergoing rapid changes due to new technologies, efforts to decarbonize, and new patterns of electricity consumption. The nation needs to invest in research to support these changes, including analytical tools to understand how the grid of the future will behave and how operators and policy makers can ensure its continued reliability and resilience.

- **Need #2: Ensure that electricity service remains clean and sustainable, and reliable and resilient.** In the coming decades, reducing carbon emissions and other environmental impacts of electricity generation will remain a major challenge. It will also be important to increase the resilience of the grid to natural disasters and targeted attacks. Meeting these challenges will require continued investment in critical power system elements such as long-distance transmission, reliability requirements for the natural-gas delivery system, and improved cybersecurity capabilities and information-sharing.

- **Need #3: Improve understanding of how people use electricity and sustain the "social compact" to keep electricity affordable and equitable in the face of profound technological challenges**. Changes in the grid reveal opportunities for new services and configurations of electric resources, but these changes can also have large impacts on customers and low-income communities. It is crucial to develop our understanding of how people use electricity and devise regulatory responses to evolve and strengthen social compacts to deliver electricity fairly and affordably.

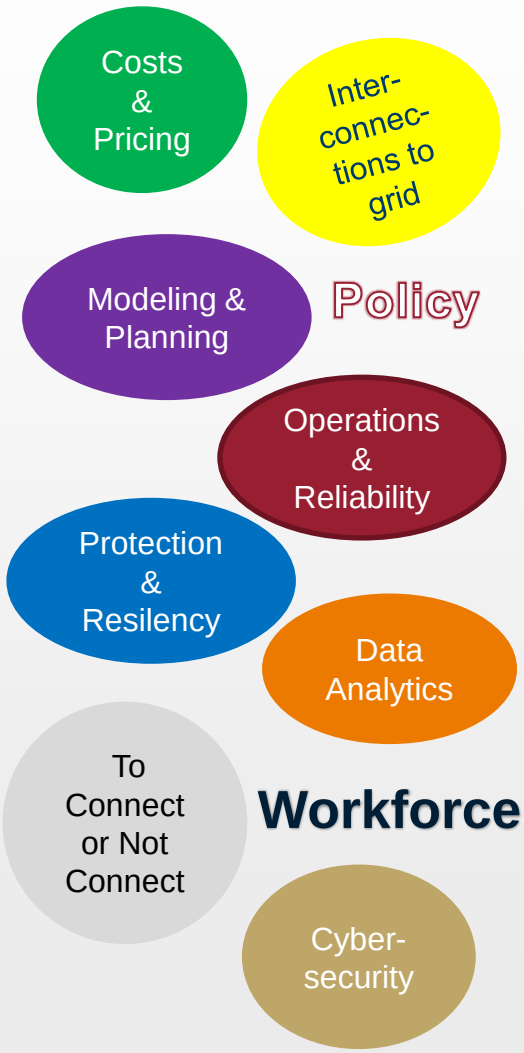
- **Need #4: Facilitate innovations in technology, policy, and business models relevant to the power system.** Understanding how electricity consumers behave, how devices and energy services can be aggregated for supply, and how such trends affect system loads is emerging as one of most profound technological challenges and opportunities facing the future of the grid. Increasing numbers of distributed devices also motivate the need for advanced situational awareness and control at the grid edge. Technology, policy, and business models must be flexible enough to coordinate and respond to changing conditions for large-scale and local-level electricity services.

- **Need #5: Accelerate innovations in technology in the face of shifting global supply chains and the influx of disruptive technologies.** Many power system technologies were first developed in the U.S., but supply chains for most critical components have now moved overseas. Massive new private and public investments are needed for cutting-edge technologies on which the future grid will depend. In this, the U.S. must balance competing goals to capitalize on global innovation while ensuring U.S. control and access to critical grid technologies.

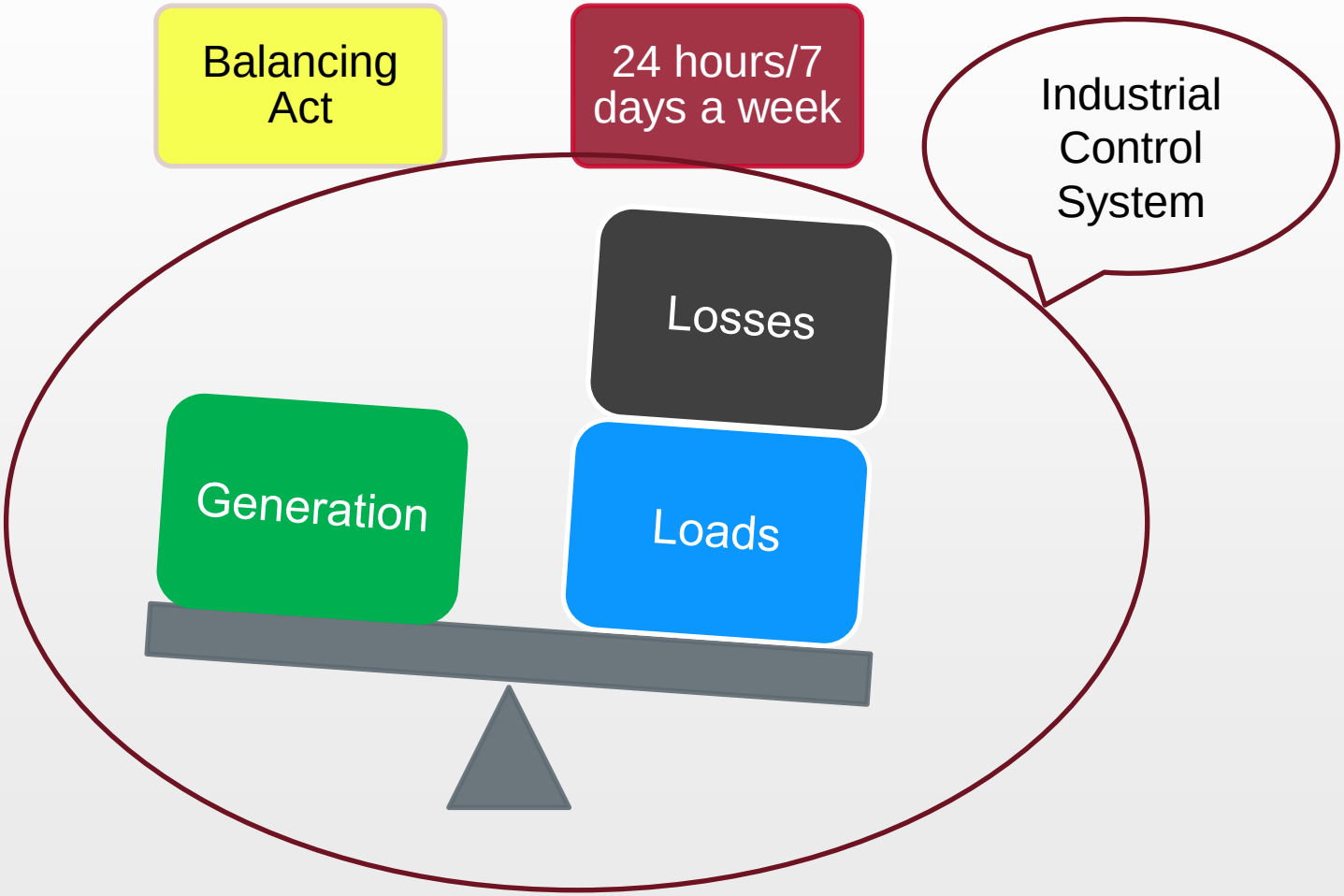
SMART Distribution Systems

Next Generation Distribution Systems

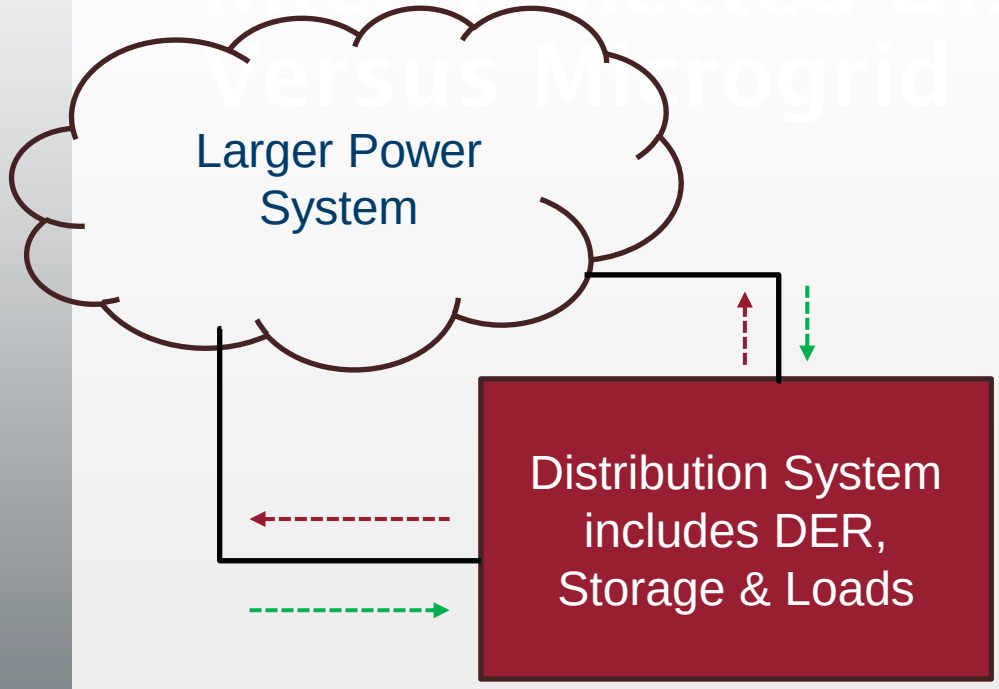
Traditional Distribution Systems	Next Generation Distribution Systems
Centralized G-T-D power system where power source elsewhere	Distributed Energy Sources (Solar, Wind, Other)
One-direction flow, minimal local control	Power Electronic Devices, Storage and Electric Vehicles
Information at substation and a few other spots	Advanced Metering, Monitoring and Control
Always connected to transmission system	Interconnected versus Microgrids

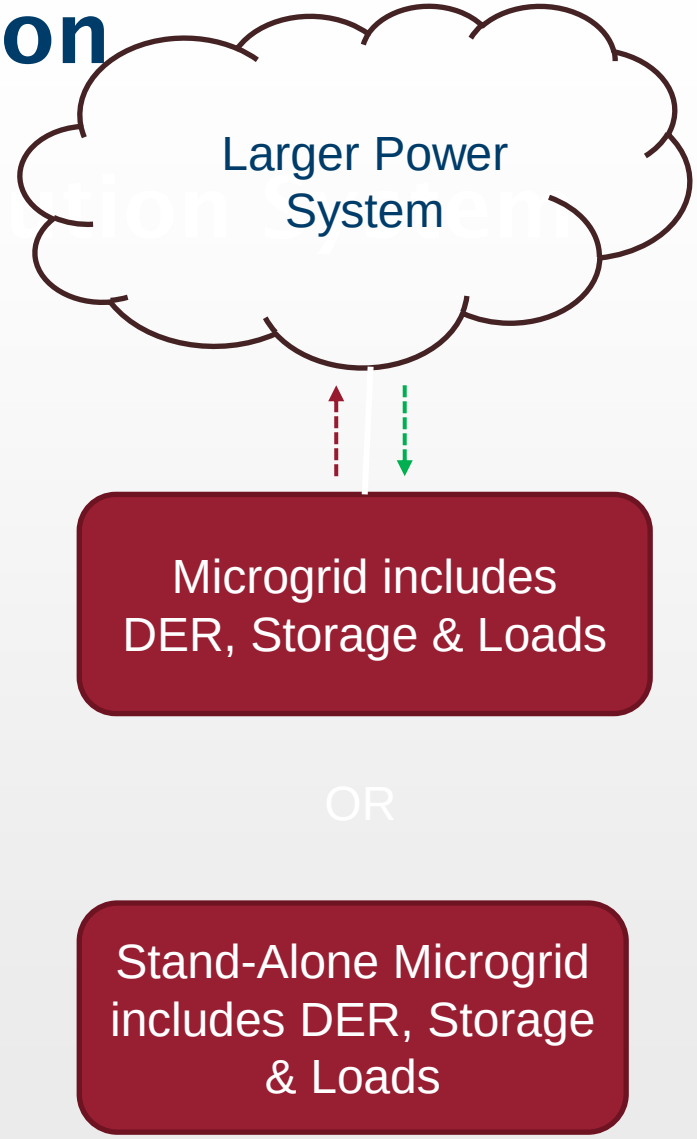


Operating a Power System



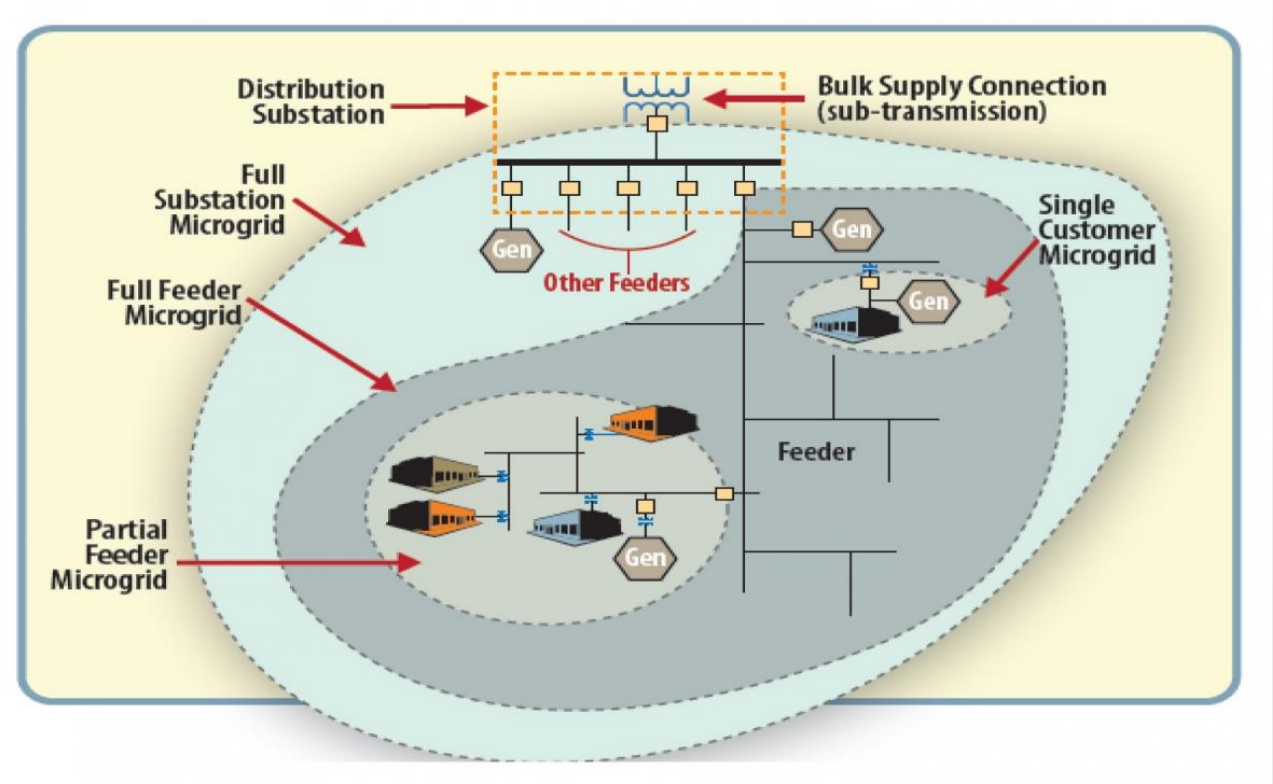
Interconnected Distribution System Versus Microgrid





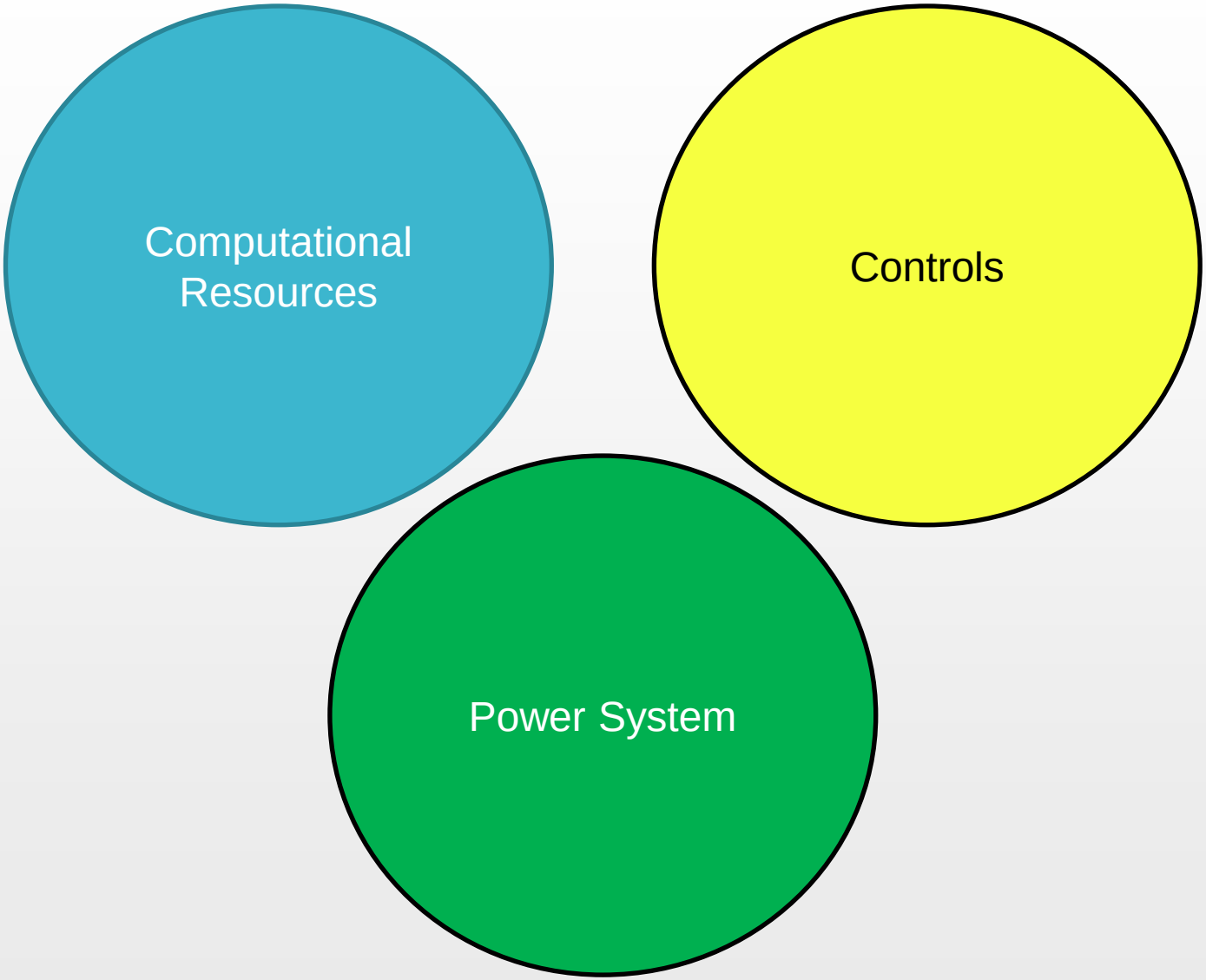
Microgrids

A group of interconnected loads and distributed energy resources with clearly defined electrical boundaries that act as a single controllable entity with respect to the grid.

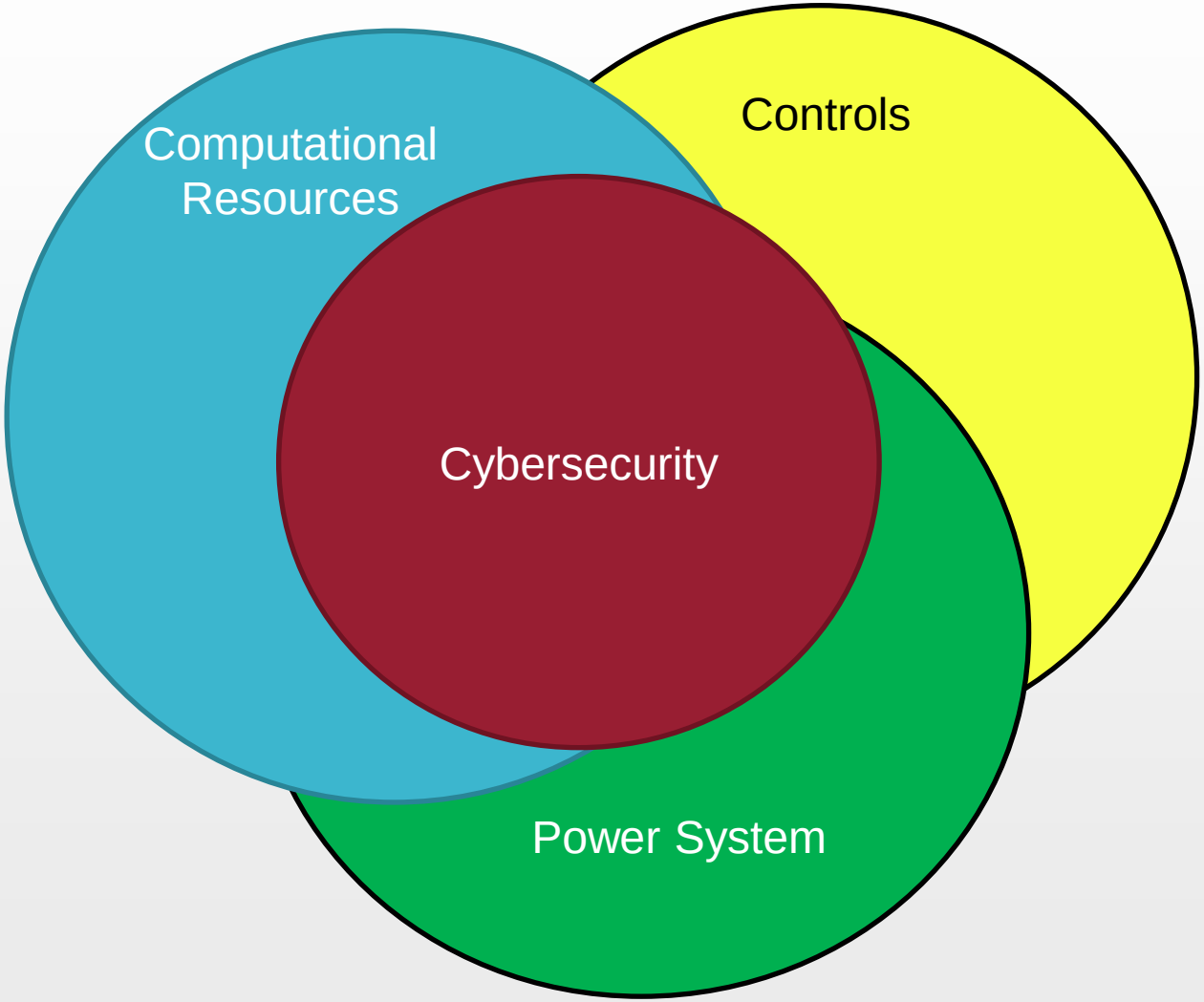


https://energy.gov/oe/services/technology-development/smart-grid/role-microgrids-helping-advance-nation-s-energy-system

Evolution of Power Grid Infrastructure – Past



Evolution of Power Grid Infrastructure – Today



Industrial Control System and Cybersecurity

Data
Analytics

Utilities

New
Sensors

Independent
Power
Producers

Aggregators

Prosumers

Questions?

Next Up – Tim Schulz, Scythe

https://www.linkedin.com/in/tim-schulz/

https://www.scythe.io/

Cybersecurity Applications for Industrial Control Environments