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

CySER Summer 2024 Workshop
May 21, 2024

Dr. Noel N. Schulz
Bob Ferguson Endowed Professor
Inaugural Director, Institute for Northwest Energy Futures (INEF)
Chief Scientist, PNNL (As Joint Appointment)
Washington State University WSU Tri-Cities
Noel.Schulz@wsu.edu
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 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, control and operation
- Outage and Storm Management including smart metering and resilience efforts
- Rural electrification and Microgrids
- Shipboard Power Systems
New Resources for WSU Tri-Cities and WSU System

**WA Governor and Legislature Funded Support**

- INEF Headquartered on WSU Tri-Cities campus
- $7.72M per biennium ($3.86M/year) recurring funds
- Purchasing Existing Building (Recycled Building 😊)
- Additional Positions
  - Administrative support – Director, Three Part-time positions (Assistant Directors & WSU Energy Office)
  - Six new staff positions
  - Seven new faculty positions (4 WSU Tri-Cities and Three WSU Pullman)
- Measuring the environmental impact of products, materials and processes
- Examining the economic feasibility and risks of processes and products with techno-economic analysis.
- Using energy data analytics to predict energy demand, improve distribution and understand customer consumption patterns.
- Assessing the social impacts of action/inaction to help facilitate sustainable and socially equitable results.
- Critical earth minerals
- Nuclear energy
- Power electronics faculty

[https://tricities.wsu.edu/inef/](https://tricities.wsu.edu/inef/)
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
- Power Grid Security
- Microgrids
- 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

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
- Blackout of 2003

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.
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
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

CIP-010  CIP-011
CONFIG. CHANGE & VULN. ASSESS.  INFORMATION PROTECTION

1. CYBER SECURITY POLICY FOR HIGH MEDIUM LEADERSHIP DOCUMENT DELEGATES
2. CYBER SECURITY POLICY FOR LOW MEDIUM PERIMETER PERSONNEL RISK ASSESSMENT ACCESS ACCESS REVOCATION PROGRAM
3. AWARENESS TRAINING PERSONNEL ACCESS MANAGEMENT
4. PLAN 2. SECURITY INCIDENT RESPONSE PLAN
5. ELECTRONIC SECURITY PERIMETER VENDOR EXTENDED MAJOR SYSTEMS INCIDENT RESPONSE PLAN
6. REMOTE ACCESS MANAGEMENT INSTALLATION MAJOR SYSTEMS INCIDENT RESPONSE PLAN
7. MAINTENANCE AND TESTING IMPLEMENTATION MAJOR SYSTEMS INCIDENT RESPONSE PLAN
8. SECURITY EVENT MONITORING TESTING MAJOR SYSTEMS INCIDENT RESPONSE PLAN
9. SYSTEMS ACCESS CONTROLS MAJOR SYSTEMS INCIDENT RESPONSE PLAN REVIEW
10. PORTS AND SERVICES IMPLEMENTATION AND TESTING MAJOR SYSTEMS INCIDENT RESPONSE PLAN REVIEW
11. SECURITY PATCH MANAGEMENT IMPLEMENTATION MAJOR SYSTEMS INCIDENT RESPONSE PLAN REVIEW
12. MAJOR SYSTEMS INCIDENT RESPONSE PLAN REVIEW

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

Source: NERC (www.nerc.com)

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.
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.”

Intersection of Power System and Cybersecurity - Recent Thoughts
### 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 other 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 have significant negative consequences if they are not available 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 functions on the grid. The information communicated from sensors was only passable to controllers, and actuators would respond to any properly formatted command. Typically, these OT devices were isolated from the IT and corporate environment. Centrality 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 ICI 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 framework 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 OT/networks, systems and assets inside the perimeter.

By the early 21st century, automation of grid ICS using ICI increased dramatically by exploiting low-cost Internet-based ICT. One notable example is automation 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 efficiency and reliability gains. However, as control systems and networks become more complicated, the underlying ICT supporting these 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.

<table>
<thead>
<tr>
<th>Traditional Approach to Grid Cybersecurity</th>
<th>Cybersecurity Vulnerabilities Resulting from Recent and Potential Future Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emphasis on perimeter security</td>
<td>Significant reduction in the degree of isolation of the industrial control system (ICS) from the outside world. Perimeter security is no longer as effective a defense.</td>
</tr>
<tr>
<td>Operational technology (OT) in an environment of implicit trust exposed to a heavily attacked perimeter</td>
<td>More emphasis will be placed on segmentation or micro-segmentation of internal environments and implementation of machine learning/artificial intelligence algorithms to monitor performance.</td>
</tr>
<tr>
<td>Self-contained OT systems with no connection to external or corporate systems</td>
<td>More requirements for external connections, including control systems that require real-time control with external parts, multi-tiered transitions to cloud-based systems, integrity connections to renewable energy sources, vendor requirements for remote access to update assets, etc.</td>
</tr>
<tr>
<td>Off-grid systems</td>
<td>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.</td>
</tr>
<tr>
<td>Energy generation, transmission, and distribution primarily owned and operated by utilities</td>
<td>Increased participation by a highly diverse population of stakeholders with unclear roles and responsibilities for cybersecurity.</td>
</tr>
<tr>
<td>Centralized control of energy transactions</td>
<td>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 processors and microprocessors.</td>
</tr>
<tr>
<td>Prevention of reliability impacts on the bulk power system owing to cybersecurity incidents primarily under utility control</td>
<td>Increasing interdependencies on other critical infrastructures, alternative energy sources such as renewables, and stakeholders that have few if any equivalent reliability or resilience requirements or expectations will significantly increase the risks to utility operations and reliability.</td>
</tr>
<tr>
<td>Privately and publicly owned communications used and controlled by utilities</td>
<td>Increased use of commercial-owned communications systems by new technologies and associated stakeholders that connect to the grid with nuclear and undefined roles and responsibilities for cybersecurity of those communication systems.</td>
</tr>
<tr>
<td>OT and ICI on premises</td>
<td>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.</td>
</tr>
<tr>
<td>Domestic supply chain as the primary source of physical and cyber assets used in the grid Innovation driven domestically resulting in domestic product development and domestic vendor standards</td>
<td>Increasing reliance on international supply chains creating cybersecurity concerns about risks with a maliciously implanted hardware, software, and firmware elements.</td>
</tr>
<tr>
<td>Reliance on indicators of compromise to detect threats</td>
<td>Increased internationally driven innovation changing the focus of product and services development and associated vendor standards, enabling in potential vulnerabilities between domestic utility requirements for cybersecurity products and internationally driven standards and product development.</td>
</tr>
<tr>
<td>Adversaries using malware as a primary tactic</td>
<td>Increasing reliance on international supply chains creating cybersecurity concerns about risks with a maliciously implanted hardware, software, and firmware elements.</td>
</tr>
<tr>
<td>Cryptography as a cybersecurity tool</td>
<td>Increasing use of biometric-based (i.e., “something you are”) and ownership-based (i.e., “something you have”) for authentication.</td>
</tr>
<tr>
<td>Reliance on passwords for authentication</td>
<td>To detect more sophisticated adversaries, more focus will be needed to advance utility capabilities for detection and threat cause analysis, which can deter resilience and response actions, and to develop stronger capabilities for containment, remediation, and recovery.</td>
</tr>
</tbody>
</table>

**Cybersecurity Challenges Presented by the Evolving Grid**
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

- Centralized G-T-D power system where power source elsewhere
- One-direction flow, minimal local control
- Information at substation and a few other spots
- Always connected to transmission system

Next Generation Distribution Systems

- Distributed Energy Sources (Solar, Wind, Other)
- Power Electronic Devices, Storage and Electric Vehicles
- Advanced Metering, Monitoring and Control
- Interconnected versus Microgrids

Costs & Pricing
Interconnections to grid
Modeling & Planning
Operations & Reliability
Protection & Resiliency
Data Analytics
Policy
To Connect or Not Connect
Cyber-security
Workforce

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

To Connect or Not Connect
Costs & Pricing
Interconnections to grid
Modeling & Planning
Operations & Reliability
Protection & Resiliency
Data Analytics
Policy
Cyber-security
Workforce
Operating a Power System

- Balancing Act
- 24 hours/7 days a week

Industrial Control System

- Generation
- Loads
- Losses
Interconnected Distribution System Versus Microgrid

Interconnected Distribution System includes DER, Storage & Loads

Larger Power System

Distribution System includes DER, Storage & Loads

Larger Power System

Microgrid includes DER, Storage & Loads

OR

Stand-Alone Microgrid includes DER, Storage & Loads
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.

Evolution of Power Grid Infrastructure – Past
Evolution of Power Grid Infrastructure – Today

- Controls
- Computational Resources
- Cybersecurity
- Power System
- AI
Industrial Control System and Cybersecurity

Data Analytics

Utilities

New Sensors

Independent Power Producers

Aggregators

Prosumers

New Sensors

Independent Power Producers

Aggregators

Prosumers
Questions?

Dr. Noel N. Schulz
Noel.Schulz@wsu.edu

Next Up – Tim Schulz, Verizon
https://www.linkedin.com/in/tim-schulz/
AI, Cybersecurity and You