Industrial Control System (ICS) – Communications, Sensors & Cybersecurity 101

Emma Stewart (LLNL)

Integrated Distribution System Planning Training
for Midwest/MISO Region
October 13-15, 2020

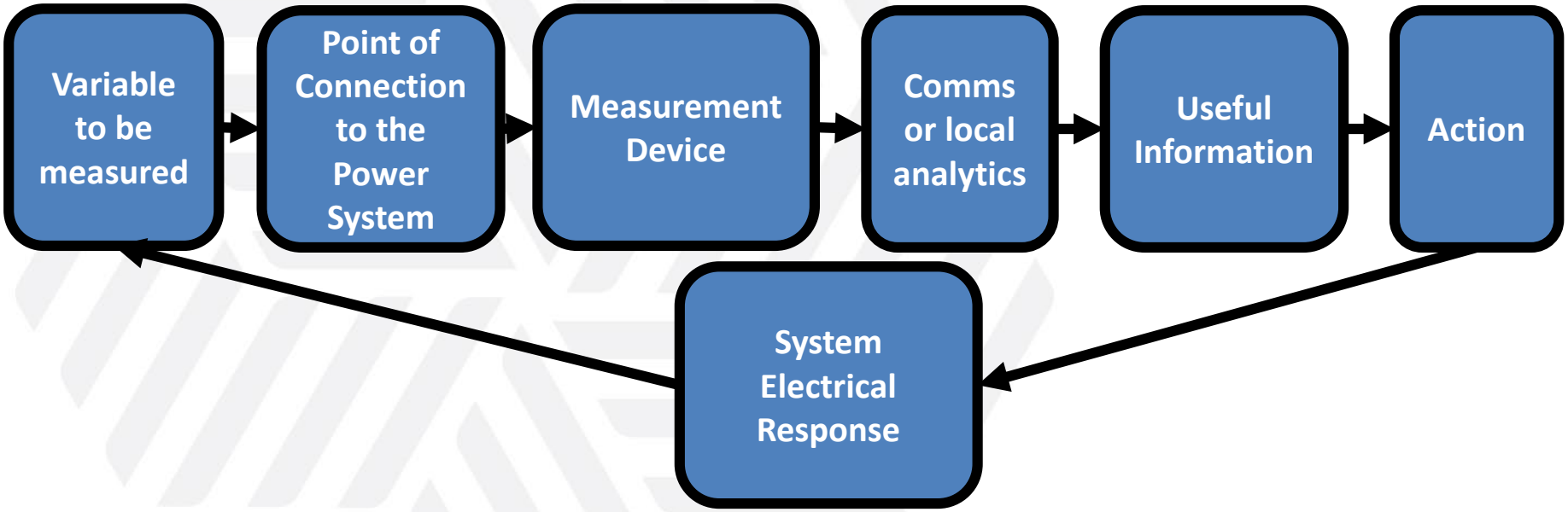
LLNL-PRES-753282

Goals of this session

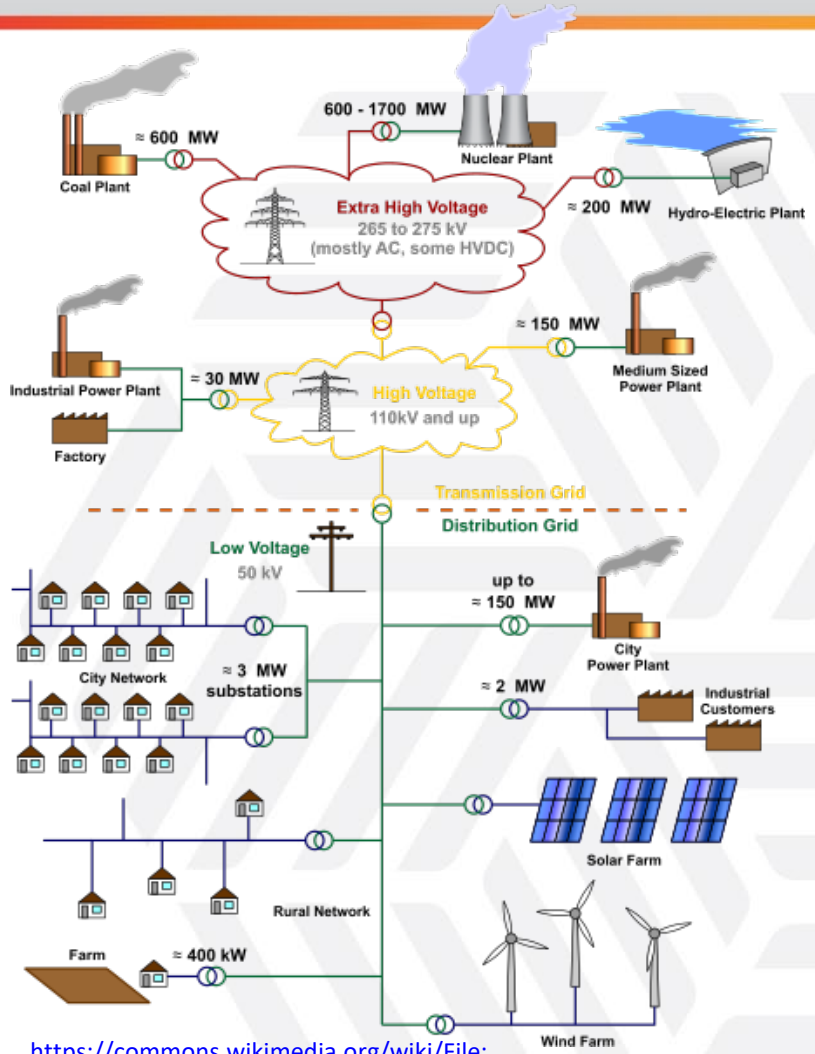
- Understand the communications system in the distribution grid and its function – fundamentals of the system, measurement & communications as it relates to the cyber physical system
- Intro to “what is cyber”
- Discuss OT/IT and the difference in management of those – and the concerned systems
- Introduction to NIST and the cyber security framework, threat tiers and protections
- Goals: understanding of the words and background

Communications and Sensors

What is Sensing and Measurement?



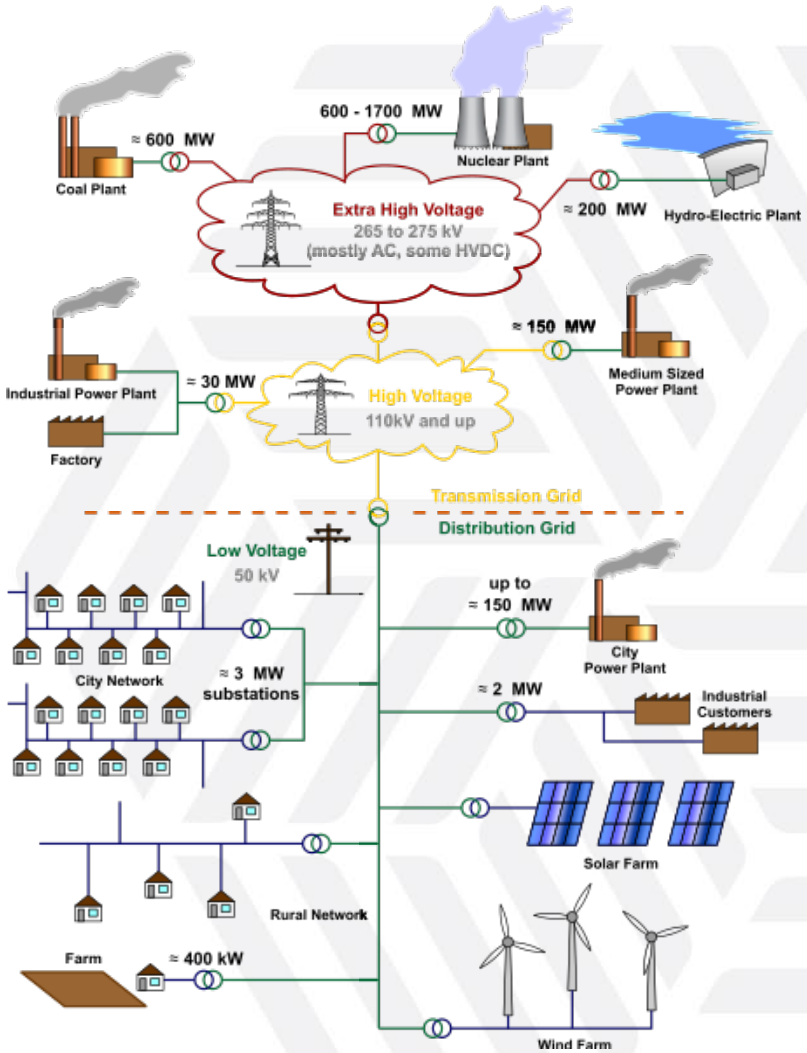
Communications are critical to many functions of the grid



https://commons.wikimedia.org/wiki/File:Electricity_Grid_Schematic_English.svg

- Telecom networks support:
  - Real-time monitoring and control
  - Protective relays
  - Energy management
  - Outage management
  - Smart meter communications
  - Substation automation
- Utilities rely on both public and private communications networks
  - Telco fiber lines could be dedicated to utilities
  - Utilities also can purchase private communications networks

Different communications media are used throughout the grid



Generation

- Wireless and radio networks are used to transmit control and monitoring messages within plants
- Cell, POTS (plain old telephone service), and fiber are used to transmit messages between plants

Transmission

- Power lines can be used to transmit information – power line carrier
- Substations use radio and wireless within substations and microwave between substations
- Land mobile radios and satellite phones are used during restoration and repair

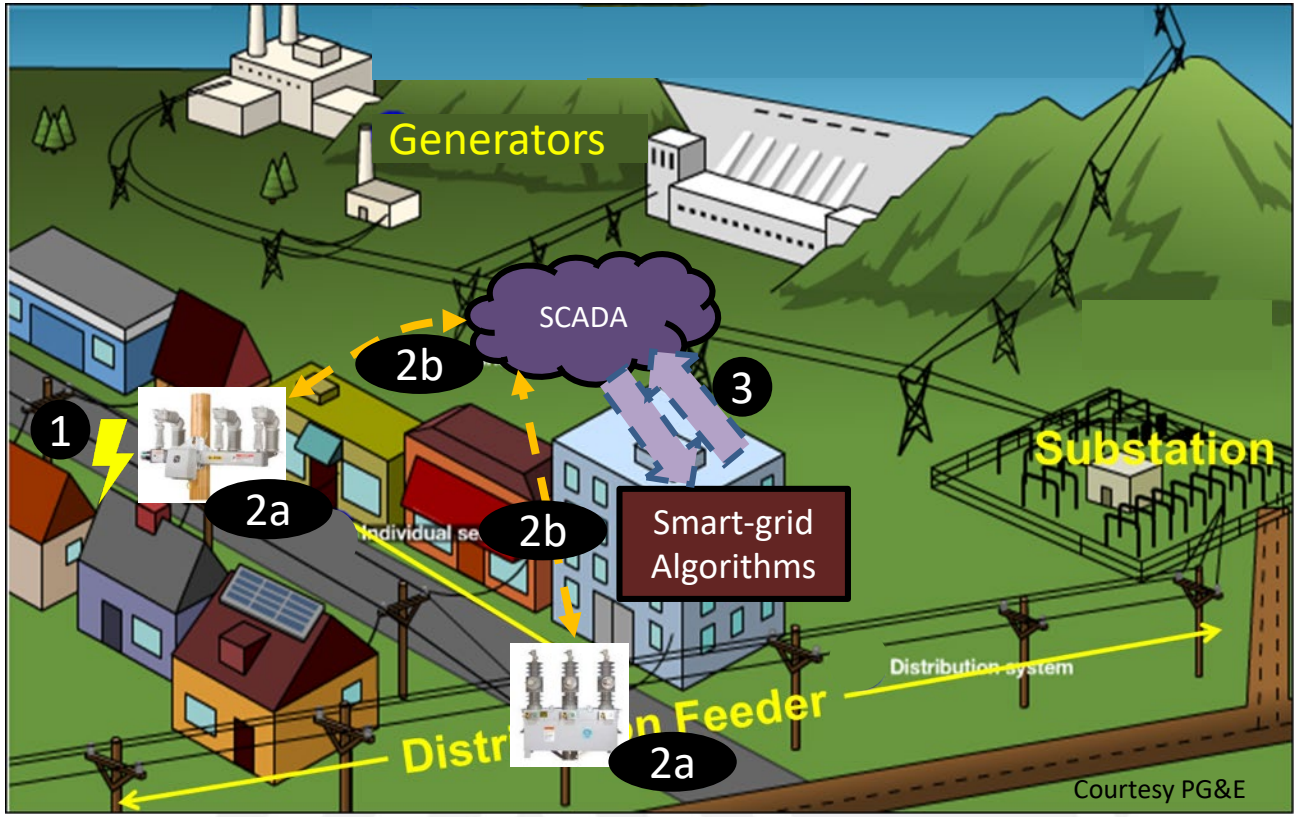
Distribution

- Some fiber used for controlling loads, but is generally expensive to run
- Microwave links, land mobile radio, and satellite phones are used

Smart Grid Communications

- For smart meter networks and control of distributed generation, wireless mesh networks can be formed

Interdependencies in smart grid communications



- Mitigating potential DA device failures caused by communications network issues
- Utility primarily relies on DA devices to detect/isolate faults
  - Local operation
  - Remote operation
- If we have communications issues, we can't send operational commands to devices

1 Fault occurs

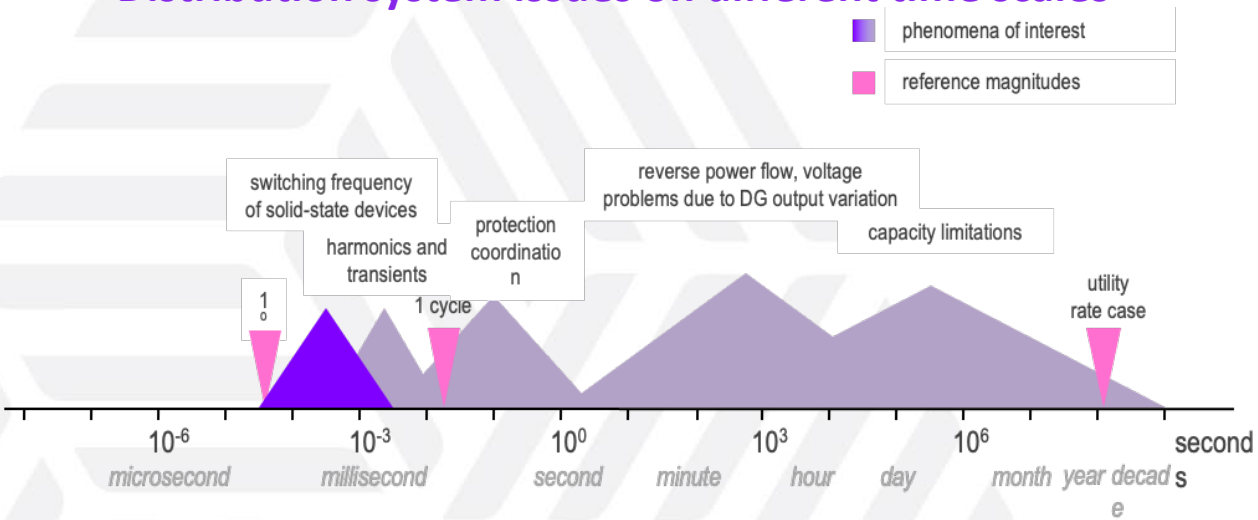
2a Lack of power inhibits DA devices operation, or

2b Communication networks fail

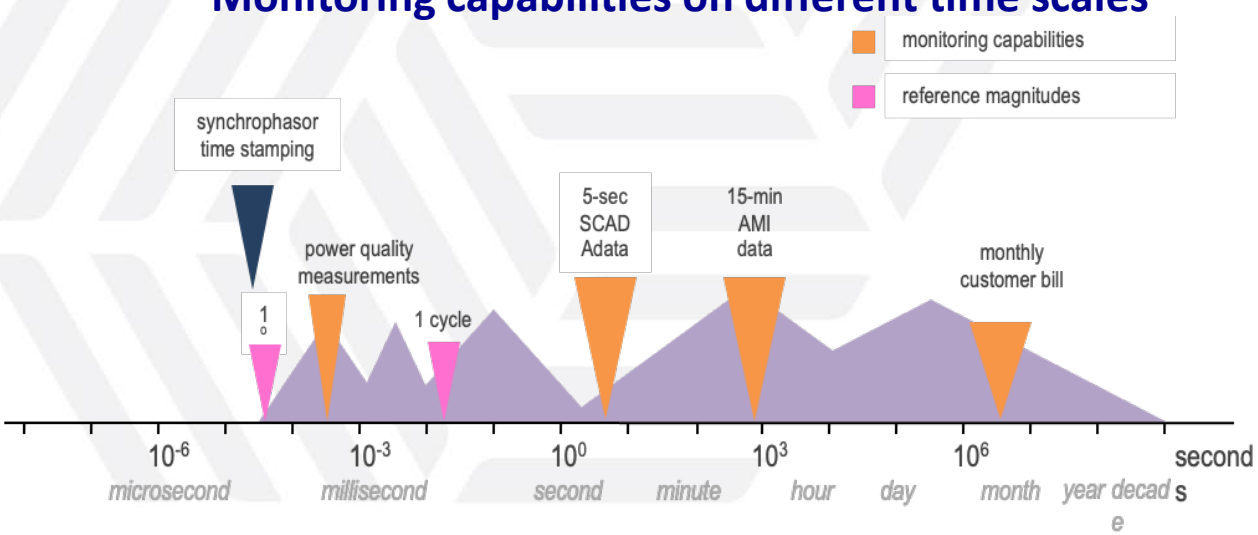
3 Remote switch operations prevented

Events versus Measurement

Distribution system issues on different time scales

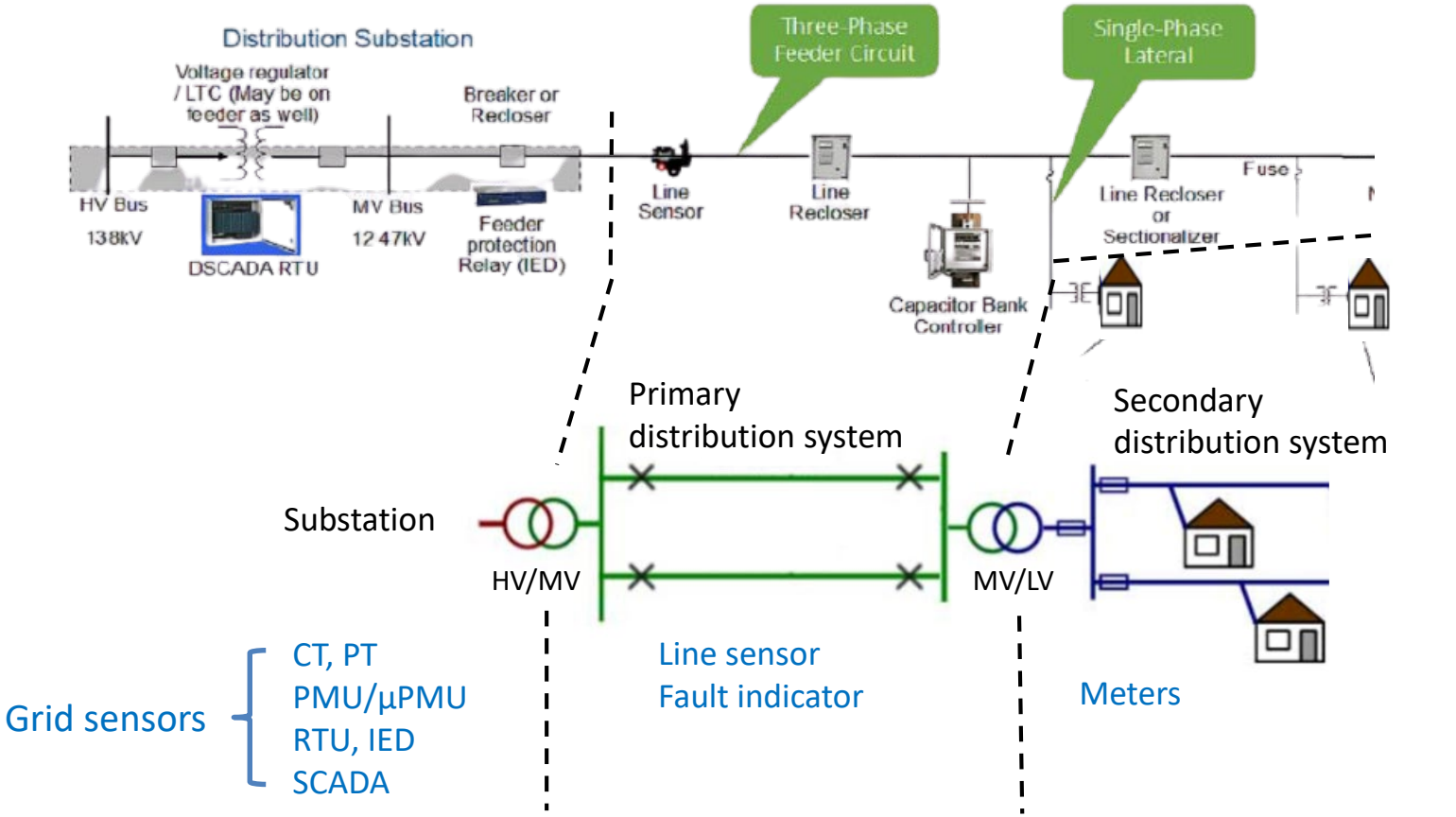


Monitoring capabilities on different time scales



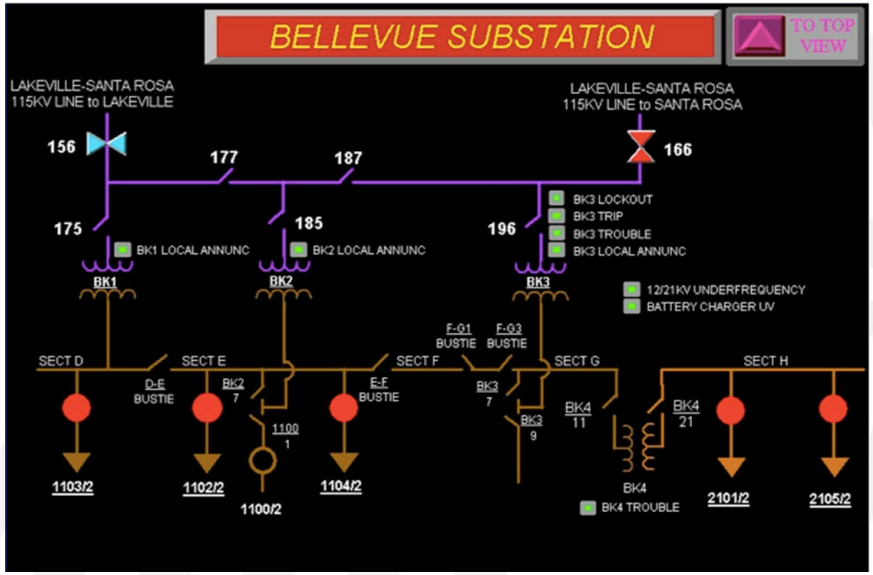
Distribution System Sensing and Measurement

- **Overview**

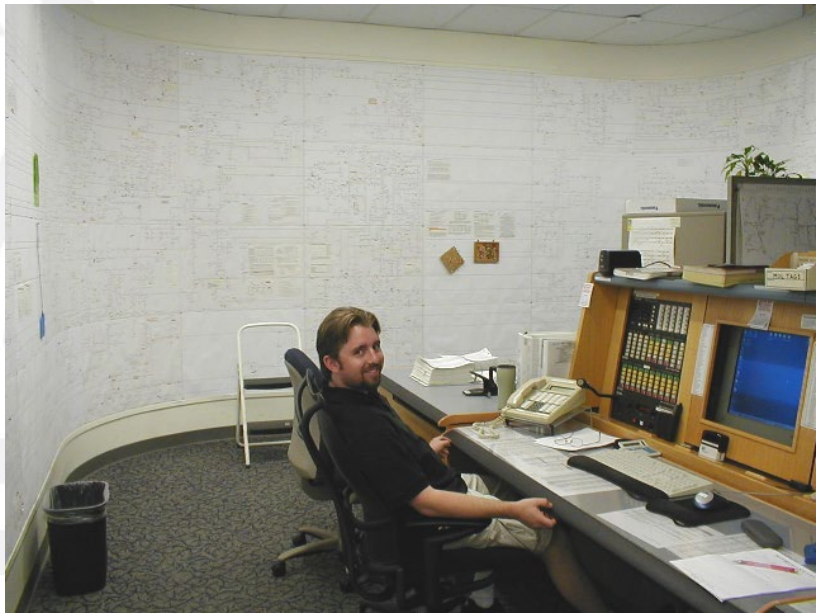


Communication and automation devices with sensing capacities Environmental sensors

Distribution System Monitoring and Control



Visibility



Present State: Distribution Operator's control room, 2003

Visualization and analytics integration at the utility: Large Plant historical information database

Discussion: Transmission vs. Distribution Sensing

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

How are distribution systems different than transmission systems?
1. Architecture 2. Diversity 3. Variation 4. Vulnerability 5. Opacity

- Monitoring and control technology has not historically been cost-effective to install, in many cases
- SCADA* typically available at substation level, but not on 100% of distribution circuits
- Many distribution circuits are without sensing beyond substation, grid operators usually can't see what's going on
- AMI and smart metering provide customer level visibility – but lacking info past this point to the connected larger system

** Supervisory Control and Data Acquisition*

Supervisory Control and Data Acquisition (SCADA)

SCADA Components:

Sensors: instruments measuring physical quantities (current, voltage)

Remote terminal units (**RTUs**): perform analog-to-digital "A to D" conversion of sensor signals; may include basic control capability

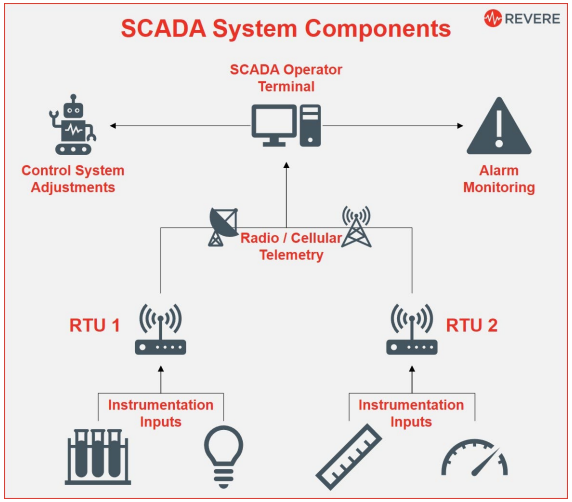
Programmable Logic Controllers (**PLCs**): similar to RTUs, more sophisticated controls

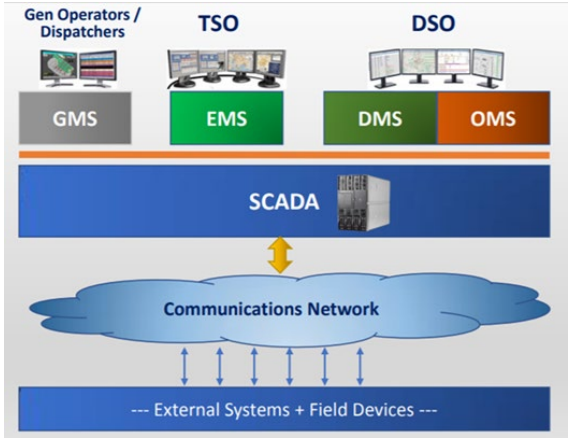
Telemetry: provides connection for signals between field devices and control center, using some **physical communication layers** (telephone wires, radio, satellite, microwave, 3G wireless)

Data Acquisition Server: manages data from field devices

Data Historian: stores data

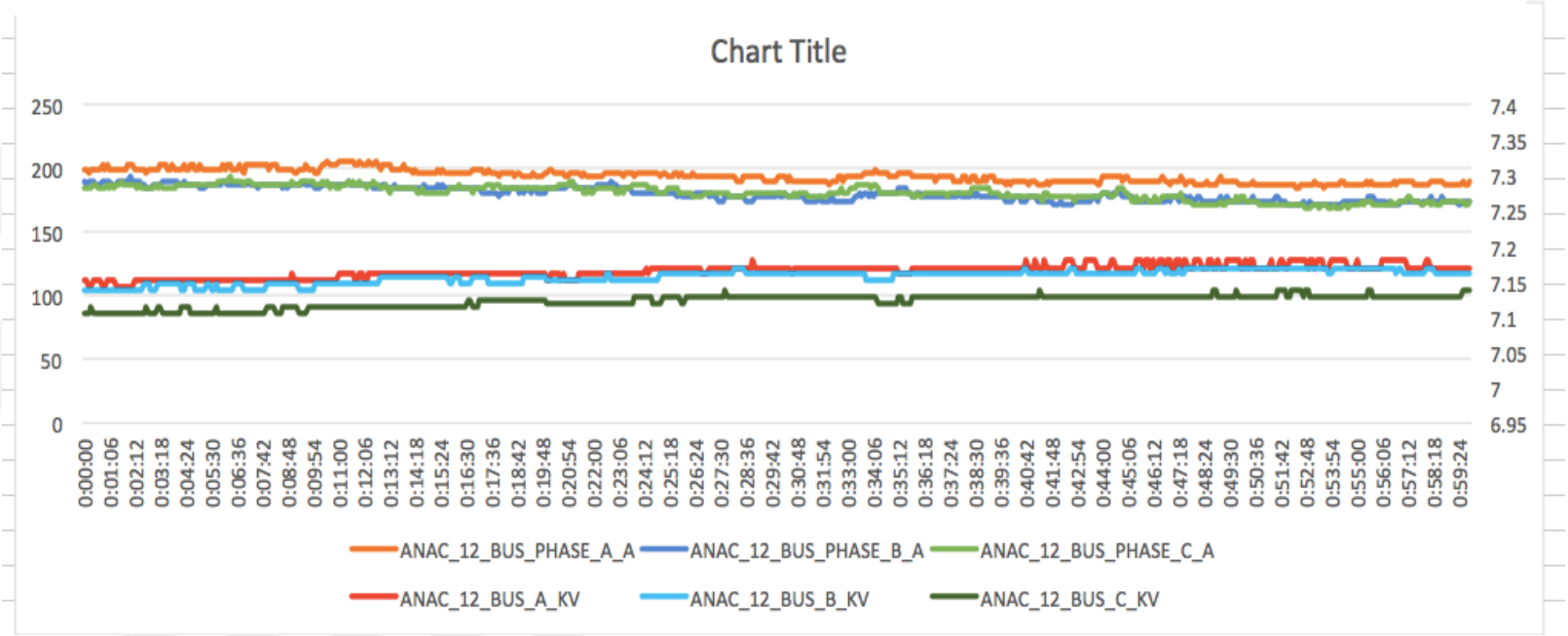
Human-machine interface (HMI): client for data from server; presents to operator; may receive control inputs from human operator





Supervisory Control and Data Acquisition (SCADA)

Typical time-series SCADA data from a distribution substation



One problem: time synchronization among locations!

Smart Meter and Advanced Metering Infrastructure (AMI)

- **Smart Meter**

Primary purpose: Settlement
(time-differentiated meter reading)

Secondary purpose:
identify outages
other operations support

Typical activity:

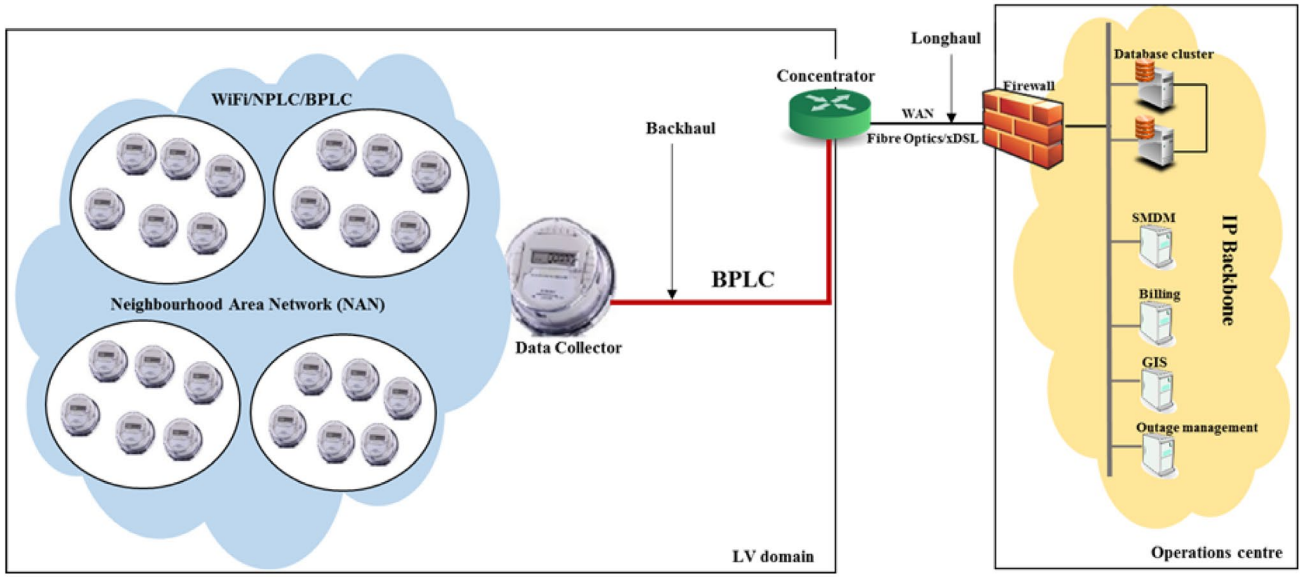
record kWh usage, voltage at 15-min intervals
report 8 hrs worth of 15-min kWh data to access point 3x per day
send "death chirp" in case of outage

Headroom on communications network allows querying subset of meters for some additional data, reported within minutes

Automated Meter Reading (AMR): one-way communication
Advanced Metering Infrastructure (AMI): two-way communication

Present State in Normal Deployment
- not enough resolution to observe short-term power variations
- typically do not report voltage (although it is sensed)
- data may not be provided in real-time
- data may be provided only to billing department, not operations
- most likely early operational application: fault location, isolation and service restoration (FLISR)

Smart Meter and Advanced Metering Infrastructure (AMI)

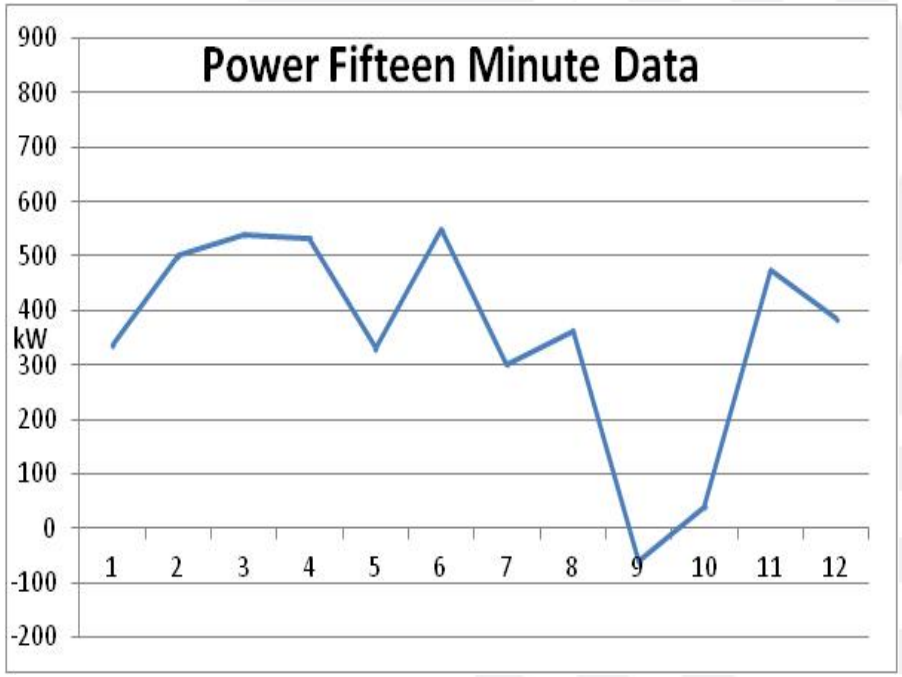


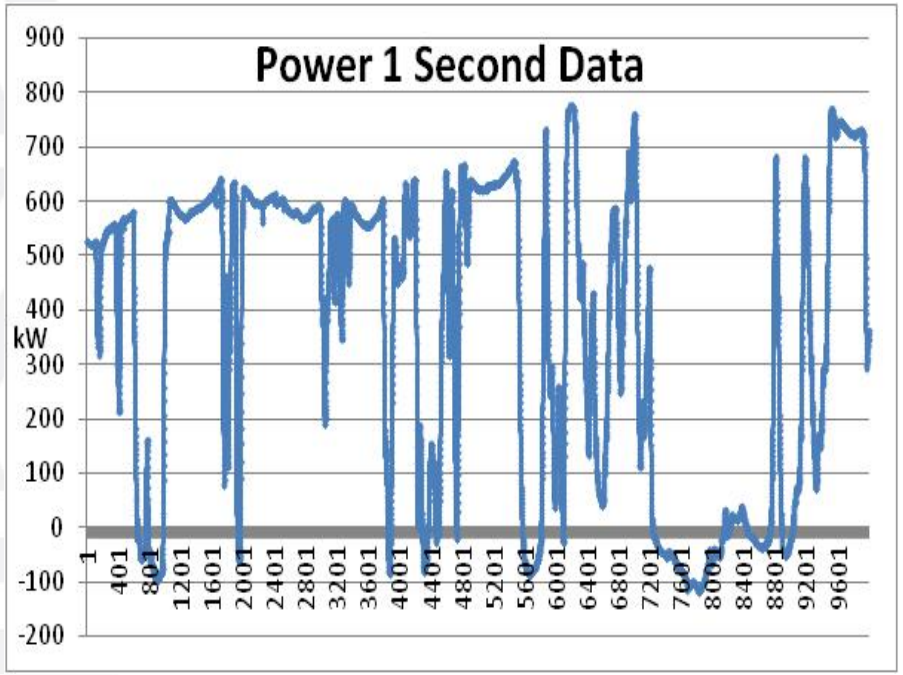
- AMI: Set of technology which encompasses smart meters, communication networks and information systems to inform the utility at a basic level on customer and network behavior as it pertains to billing and performance
- Smart Metering is a subset of technology within AMI
- Over 98M smart meters in the US today (*Smart Meters at a Glance*)
- Rate of adoption varies depending on state policies, regulatory incentives, and technology experience levels within the utilities.

Smart Meter and Advanced Metering Infrastructure (AMI)

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

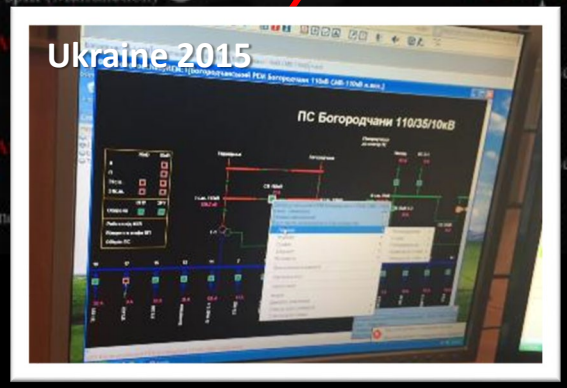
Resolution is important





Cybersecurity 101

The problem is harder when adversaries try to disrupt systems….



Explosion of Siberian natural gas pipeline (Targeted Attack)
Maroochy shire wastewater plant compromised (Targeted Attack)
Taum Sauk dam failure (Malfunction)
Aurora Generator Test (Research)
Worm cripples industrial plants (Collateral damage)
Texas power company hack (Targeted Attack)
Houston water distribution system hack (Targeted Attack)
SF Muni rail ransomware (Targeted Attack)
Unidentified water facility (Targeted Attack)
German steel mill (Targeted Attack)
Ransom attacks on hospitals (Targeted Attack)
Los Angeles traffic system attack (Targeted Attack)
Lodz, Poland tram hack (Targeted Attack)
Unidentified nuclear power plant (Targeted Attack)
Alpine ski resort ransomware (Targeted Attack)
Ukrainian power grid attacks (Targeted Attack)
Dallas emergency sirens hack (Targeted Attack)
Researchers remotely take control of cars (Malfunction)
"WannaCry" Ransomware Campaign (Targeted Attack)
Browns Ferry nuclear plant (Malfunction)
San Bernardino pipeline rupture (Malfunction)
Pacific Energy Resources hack (Targeted Attack)
Marshall, Michigan crude oil spill (Malfunction)
Worm cripples CSX transport system (Collateral damage)
82 97 99 00 03 05 06 07 08 09 10 11 13 14 15 16 17

Ivezic, Marin. **Cyber Kinetic Attacks**. *http://ivezic.com/cyber-kinetic-book/*

"Our adversaries and strategic competitors will increasingly use cyber capabilities to seek political, economic, and military advantage over the United States and its allies and partners."

*"**China has the ability** to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure in the United States."*

*"**Russia has the ability** to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure…. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."*

Daniel R. Coats, Director of National Intelligence
Testimony to Senate Select Committee on Intelligence, January 29th 2019

Taking a step back

- If we think about cyber… we need to think about communications system
- Large difference between intrusion into the ICS versus IT
- Consider malware and lock outs versus control disruption….

IT vs OT Networks

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Information Technology (IT) Networks

- Manage data
- Non real-time, high throughput needed, high delays tolerable
- Availability of the system not critical, rebooting ok
- Data confidentiality and integrity paramount
- Systems use common operating systems, updates and patching straightforward
- Lifetime on the order of 3-5 years
- Systems typically local and accessible

Operational Technology (OT) Networks

- Manage physical processes
- Real time, modest throughput ok, high delays prohibitive
- Availability of systems may be critical enough to require redundant system
- Human safety paramount, followed by undisrupted processes, fault tolerance essential
- Diverse and often proprietary operating systems, software updates typically must be done through the vendor
- Lifetime on the order of 10-15 years
- Systems can be isolated and remote

IT and OT networks differ significantly in terms of requirements, priorities and risks. As a result IT cybersecurity does not directly map into OT cybersecurity, and some practices that are essential in IT cybersecurity can disrupt the physical processes controlled by OT networks if they are not adapted to the requirements of the system.

NIST Cybersecurity Framework

Framework Function
Identify
Protect
Detect
Respond
Recover

Identify

- Know thyself…
- Have an accurate inventory of assets, data, people
- Understand how the network works and behaves
- Understand risks, identify vulnerabilities and potential impacts
- Understand criticality of assets to the mission

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management

Understanding your own system, how it works and what's on it is essential for cybersecurity – we can't defend what we don't know is there.

Protect

- Manage identities and control access
- Authenticate users, devices and other assets
- Network segregation and segmentation
- Use encryption to protect data when available
- Integration checks for verifying software, firmware and data
- Develop, maintain and test incident response and recovery plans
- Reduce the attack surface
- Patching, vulnerability scanning, properly configured firewalls

Function	Category
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology

There is no perfect security, but the objective is to make it increasingly hard for the adversary to gain access to the OT network.

Detect

- Establish baseline network and user behavior to enable anomaly detection
- Monitor for unusual activity both from devices and users
- Keep libraries of known malicious signatures and TTPs (Tactics, Techniques and Procedures) up-to-date
- Monitor for unauthorized connections and users
- Perform regular vulnerability scans
- Report and investigate incidents

Function	Category
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes

The adversaries will always find a way to get in, but timely detection can minimize the effectiveness of the attack and prevent it from spreading.

Respond

- Establish an incident response plan and execute it accordingly
- Share information among stakeholders and coordinate
- Investigate detection alerts and determine root cause
- Contain and mitigate discovered incidents and understand the impacts of the mitigations
- Perform forensic analysis to understand the scope of compromise
- Mitigate newly identified vulnerabilities

Function	Category
Protect	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements

Adequate response to an incident will ensure that its impacts are minimized, making it increasingly difficult for an adversary to achieve their objectives.

Recover

- Establish a recovery plan and execute it accordingly
- Update plans with lessons learned
- Ensure all systems are “clean” before bringing them online
- Perform activities in “identify” and “protect” steps to establish new baselines
- Recovery activities are coordinated and include internal and external stakeholders (vendors, customers, etc.)

Function	Category
Recover	Recovery Planning
	Improvements
	Communications

Recovery can be time consuming, but it’s essential in ensuring the adversary cannot re-use the same attack in the future.

Common Intrusion Paths

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

- Attacks directly from Internet to Internet connected ICS device
- Attacks initiated using remote access credentials stolen from authorized ICS organization users
- Attacks on external business web interface
  - Leverage exploits and vulnerabilities existing in web server applications
  - Pivot into the ICS historian that provides ICS data to the web server applications
- Attacks initiated by insertion of infected mobile media into a system component
  - Pivot deeper into the ICS network as attacker finds opportunities
- Attacks through phishing emails to establish presence on enterprise network
  - Pivot deeper into the ICS network as attacker finds opportunities

*From "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," US-CERT

Defense-in-depth

- Multi-layered approach designed to impede the progress of a cyber intruder while enabling the organization to respond with the goal of minimizing the impacts of the attack

*From "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," US-CERT

Layered defense strategy for the electric grid – mapping strategy to attack type

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

NIST	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify			
Protect			
Detect			
Respond	USE vulnerabilities	DISCOVER vulnerabilities	CREATE vulnerabilities
Recover			
Endure			

Lawrence Livermore National Laboratory

Layered defense strategy for the electric grid

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover	Pre-planning	OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, component diversification, decentralization		

Lawrence Livermore National Laboratory

Layered defense strategy for the electric grid

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Industry	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect		Data aggregation, threat detection	Cross-domain operational intelligence, novel data analytics for threat detection
Respond		Orchestration and remediation	Reinforcement learning for self-healing cyber systems
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, component diversification, decentralization		

Lawrence Livermore National Laboratory

Layered defense strategy for the electric grid

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Industry	Utility / Industry Partnerships	Firmware verification, Control verification
Detect			Cross-domain operational intelligence, novel data analytics for threat detection
Respond			Reinforcement learning for self-healing cyber systems
Recover			Optimized black start strategies leveraging DER
Endure	Microgrids, component diversification, decentralization		

Lawrence Livermore National Laboratory

DHS NCCIC Recommended Strategies

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

1. Application Whitelisting
2. Proper Configuration/Patch Management
   - Avoid watering hole attacks
   - Use DNS reputation system
   - Validate the authenticity of downloads
3. Reduce Attack Surface Area
   - Isolate ICS networks
   - Close unused ports and services
   - Identify all IT/OT connections and monitor them
4. Build a Defendable Environment
   - Segment network into local enclaves
   - Restrict host-to-host communication paths
5. Manage Authentication
   - Multifactor authentication
   - Enable only necessary privileges for each user
   - Lengthy passwords, change every 90 days
   - Separate credentials for business and ICS networks
5. Implement Secure Remote Access
   - Do not allow persistent vendor connections
   - Remote access should be operator controlled and time limited
   - Use 2-factor authentication
6. Monitor and Respond
   - Watch IP traffic on ICS boundaries for abnormal comms
   - Monitor IP traffic within control network
   - Use host based monitoring and detection
   - Use login analysis to detect stolen credentials or improper access
   - Watch user and administrator actions to detect access control manipulation

ICS Cybersecurity – Summary & Resources

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

- Numerous guidelines, best practices exist (DHS/ICS-CERT, NIST, SANS, NSA, DoD, DOE…)
- NIST Cybersecurity Framework provides comprehensive approach to cybersecurity for ICS
- Framework provides a set of cybersecurity activities, outcomes and informative references that are common across critical infrastructure sectors
- Meant for asset owners to use as part of their risk management process
- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Questions & Contact

Emma M Stewart
Associate Program Leader, Defense Infrastructure
Cyber and Infrastructure Resilience
Lawrence Livermore National Laboratory
Livermore, CA
Tel: 925-583-4159
Email: stewart78@llnl.gov

Extra Slides

Other Sensors and Measurement Devices

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Common Sensor Types

Sensor Type	Description
faulted circuit indicator	Provides a binary indication of the passage of a fault current (based on magnitude) past the sensing point.
line sensor	Typically sample voltage and/or current and provide various derived quantities, such as RMS volts and/or amps, real and reactive power, power factor, a small number of harmonics of voltage or current, and THD. Transducers may be electrical, magnetic, or optical.
PMU	Phasor measurement unit – provides voltage and current synchrophasors; may also provide line frequency and power flows.
partial discharge	Detects and counts arcing partial discharges in power transformers
cable tan delta	Measures phase shift on cable insulation
line temperature	Measures temperature distributions on power lines, typically done with fiber optics.
residential meter	In addition to usage (energy), may measure secondary voltage; may record data on voltage sags as measured on the secondary at the premise; a few also record real and reactive power and power quality measures such as voltage Total Harmonic Distortion (THD)
Commercial and Industrial (C&I) meter	In addition to usage (energy), measures secondary voltage and current, computes real and reactive power, THD and a variety of other configurable quantities; may capture power waveforms on a trigger basis for later retrieval
feeder meter	Provides meter quality measurement of feeder primary quantities, including voltage, current; real and reactive power

Courtesy of Jeff Taft - PNNL

Other Sensors and Measurement Devices

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Common Grid Devices with Sensing Capability

Device	Sensing capability
switch controller	Measure voltage, may record peak fault currents
capacitor controller	Measure voltage, may record peak fault currents, may compute real and reactive power
recloser controller	Measure voltage, may record peak fault currents
voltage regulator	Measures line voltage
substation IED's (microprocessor relays)	Can take transducer inputs for voltage and current directly; can compute many derived values, including real and reactive power, phasors, THD, power factor, etc; also act as a gateway for other kinds of measurements, such as oil temperature, partial discharge data, etc

Courtesy of Jeff Taft - PNNL

Other Sensors and Measurement Devices

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Relevant Building Sensors

Device	Sensing capability
Smart Metering	RMS voltage and current and power flow at whole building level
Solar	Irradiance and kWh generated
Thermal Comfort	Dry bulb air temperature
Occupancy	Measures presence and number of people based on IR or sound or both

Courtesy of Jeff Taft - PNNL