Cybersecurity for DER Systems

Dr. Chris Farnell
NCREPT Managing Director

Dr. H. Alan Mantooth
Distinguished Professor of Electrical Engineering

University of Arkansas

February 15, 2021

Presentation Outline

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Presentation Outline

- **NCREPT Facility Overview**
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

NCREPT's Mission & Focus

Background:

NCREPT was formed in 2005 as a result of the 2003 Northeast Blackout and began investigating advanced power electronic solutions for the grid and transportation applications.

Research Focus:

Design and test advanced, solid-state solutions applicable to:

- **Grid Reliability**
- **Power Interface Applications**
- **Transportation**
- **Energy Exploration**
- **Cybersecurity**

Associated Centers

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)

https://seedscenter.uark.edu/

GRid-connected Advanced Power Electronics Systems (GRAPES)

http://grapes.uark.edu/

Power Optimization of Electro-Thermal Systems (POETS)

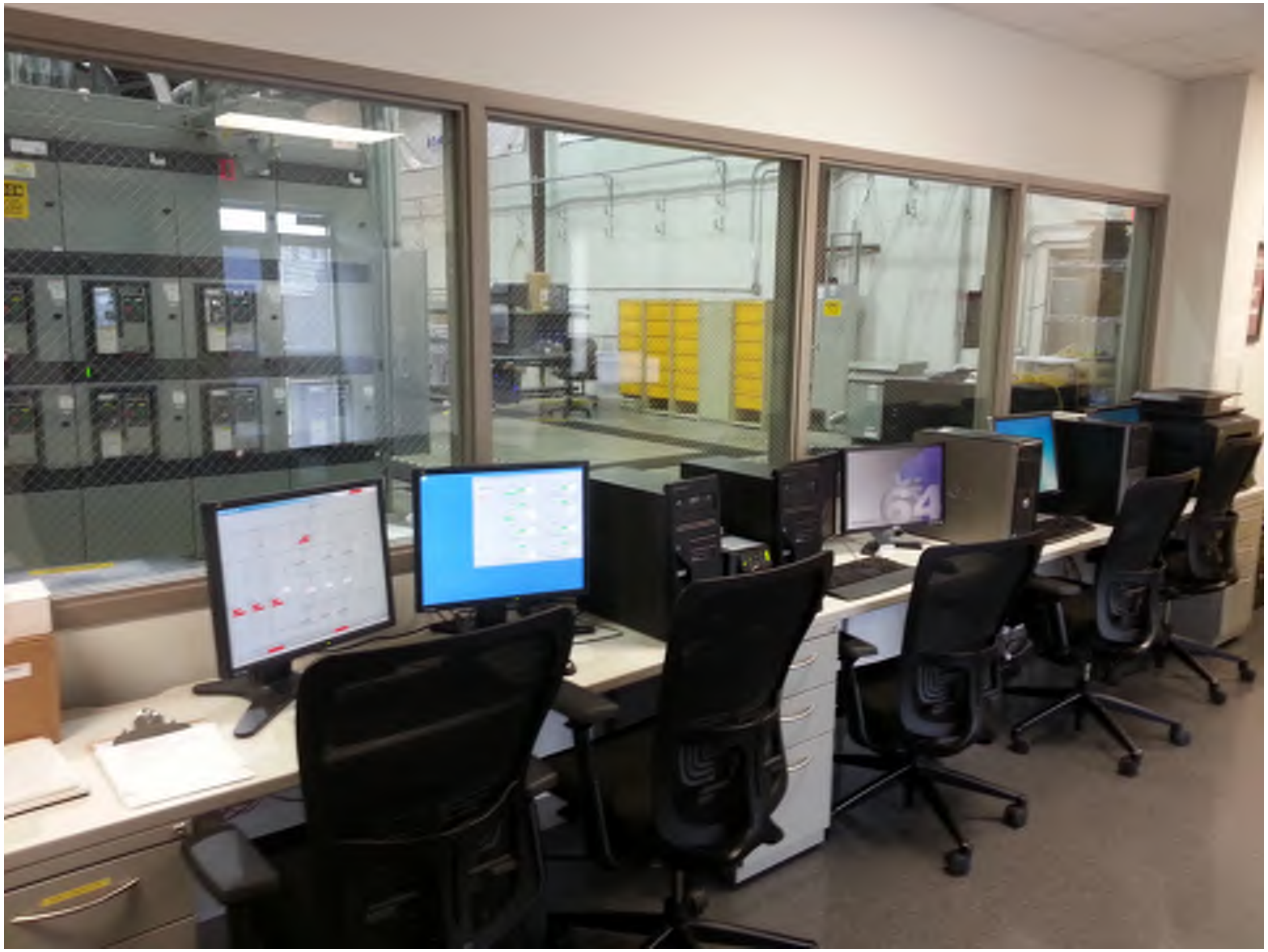
https://poets-erc.org/

NCREPT Facility

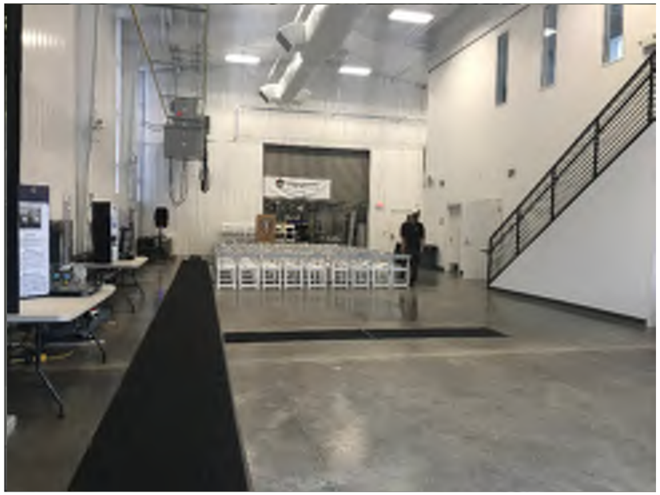
- **12,000 square foot building**
- **Cost-effective facility for businesses, national labs, and universities**
- **IEEE 1547 and UL 1741 testing**

Parameter	Rating
Power	up to 6 MVA (3 x 2 MVA Circuits)
Medium Voltage (ac)	13.8 kV or 4.16 kV (line-line) Variable from 0 V to 15.18 kV
Low Voltages (ac)	480 V (line-line), Variable from 0 V to 528 V
Frequency	40 Hz to 70 Hz Values outside this range (up to 400 Hz or down to 20 Hz) are possible, but require de-rating
Currents (ac)	300 A at 13.8 kV 1,000 A at 4.16 kV 2,500 A at 480 V
Loads	Active loads fully programmable; Test energy is recirculated 700 kW Resistive Load Bank Various Passive Components Available
Active Cooling	120 ton Chiller (420 kW Heat Rejection)
DC	2.25 MW (1500 Vdc / 1500 A) [Testing In Progress] 750 kW (660 Vdc / 1.1 kA)
Dynamometer	100 kW with Overload Capability 6,600 rpm @ 220 Nm

NCREPT Control Room

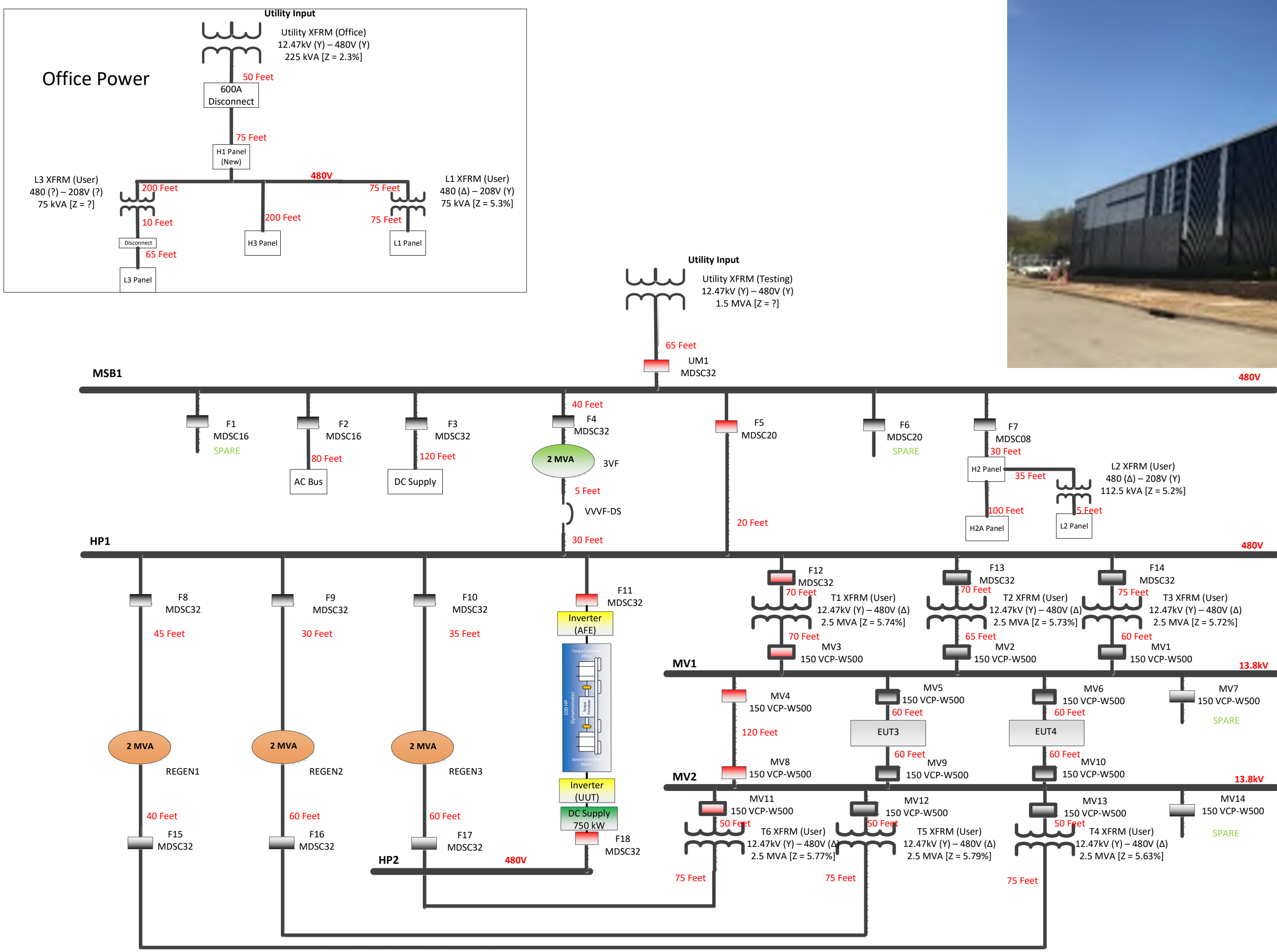


NCREPT Bay Area



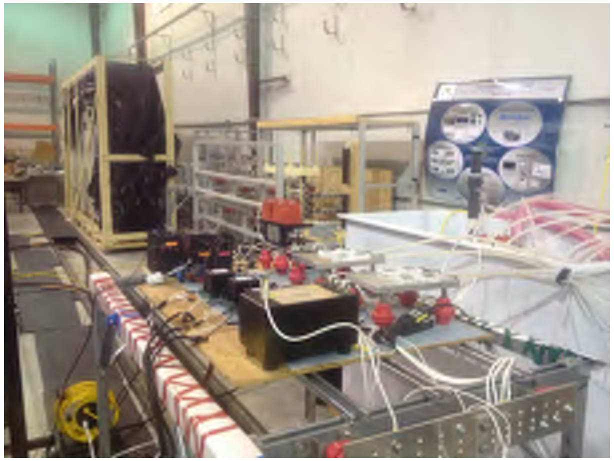
NCREPT One-line Configuration

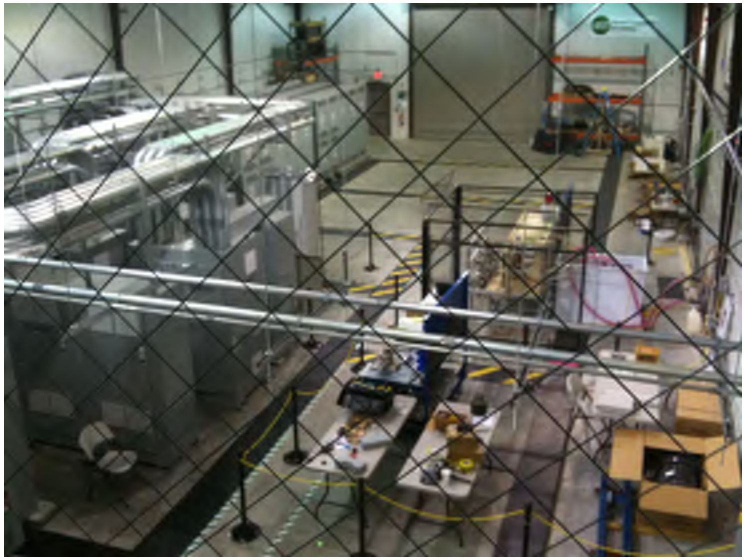
Cybersecurity for Energy Delivery Systems



Carnegie Mellon University Electrical & Computer Engineering
UA Little Rock
University of Arkansas
Electric Cooperatives of Arkansas — Your Local Energy Partners
Lehigh University
MIT
FIU Florida International University

Examples of Previous Power Testing





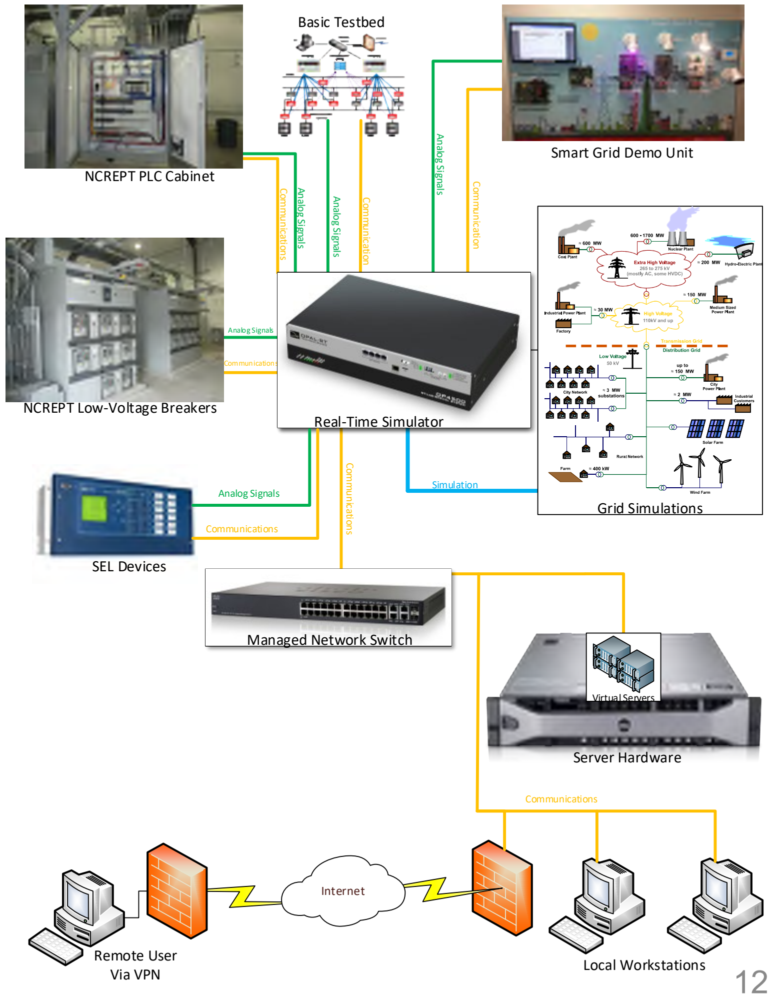
Presentation Outline

- NCREPT Facility Overview
- **Cyber Testbed**
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Cyber Testbed: Overview and Purpose

Cybersecurity for Energy Delivery Systems

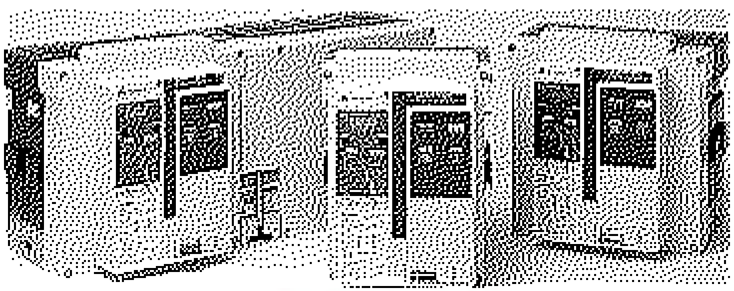
- Allows for Alpha testing in a realistic environment
- Simulated and real-world power flows
- Intra and Inter substation topologies emulated
- Utilize industry standard communication protocols
  - ✓ IEC 61850
  - ✓ DNP3
  - ✓ OPC UA
  - ✓ Modbus TCP
  - ✓ RS-232
- Utilize industry standard hardware devices
  - ✓ Real-Time Automation Controllers
  - ✓ Protection Relays
  - ✓ PLCs
  - ✓ Security Gateways
  - ✓ Various Network Devices

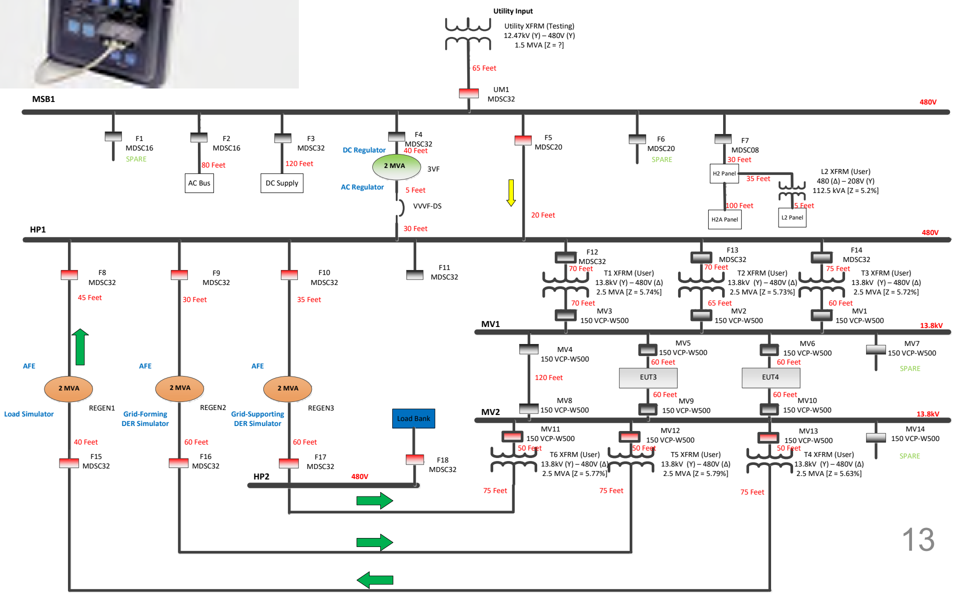


Testbed Assets: Hardware Systems

Cybersecurity for Energy Delivery Systems

- **480 V LV 3-Phase Breakers [PRs]**
  - **INCOM**
  - **Modbus TCP (PXG900)**
- **13.8 kV MV 3-Phase Breakers [PRs]**
  - **INCOM**
  - **Modbus TCP (PXG900)**
- **Grid Simulator (750 kVA)**
  - **Modbus RTU**
- **Regenerative Load Banks (3 x 2 MVA)**
  - **Modbus RTU**
- **PLC Cabinet and SCADA Control**
  - **Modbus TCP**
  - **OPC UA**





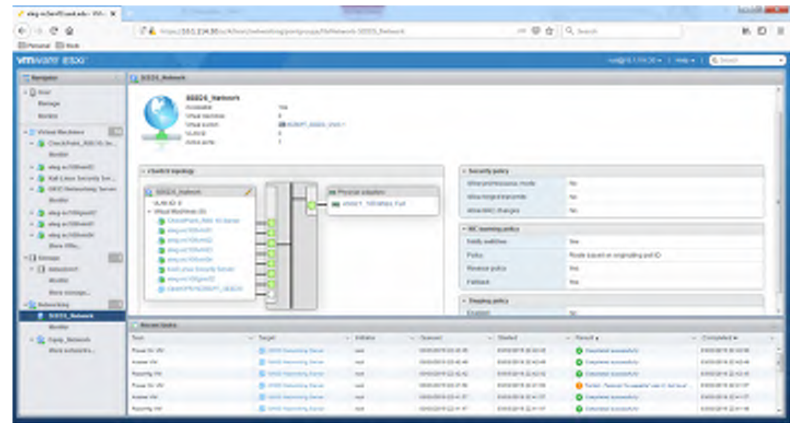
Carnegie Mellon University Electrical & Computer Engineering | UA LITTLE ROCK | UNIVERSITY OF ARKANSAS | Electric Cooperatives of Arkansas | LEHIGH UNIVERSITY | MIT | FIU FLORIDA INTERNATIONAL UNIVERSITY

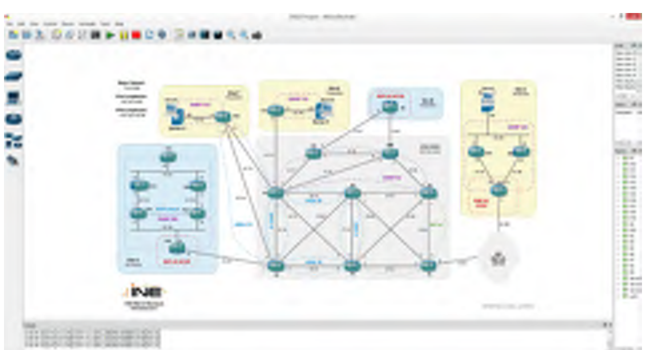
Testbed Assets: Software Systems

SEEDS

Cybersecurity for Energy Delivery Systems

- **VMWare ESXI Hypervisor**
  - CheckPoint Security Management Server
  - Kali Linux Pen-Testing Server
  - GNS3 Network Simulator
  - Virtual Routers and Switches
- **Simulation Resources**
  - Matlab
  - ETAP
  - OpenDSS
- **Remote Access**
  - Linux and Windows Workstations
  - OpenVPN Servers



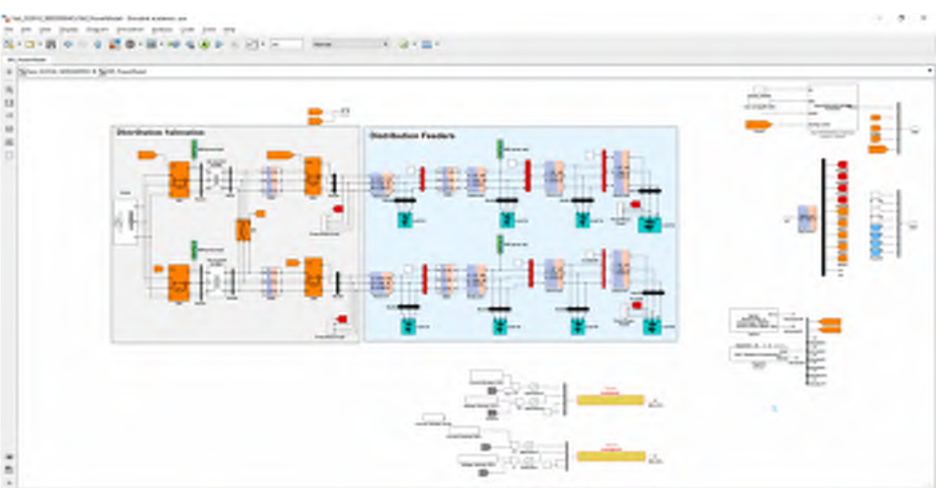


Testbed Assets: Cross-Domain Systems

Cybersecurity for Energy Delivery Systems

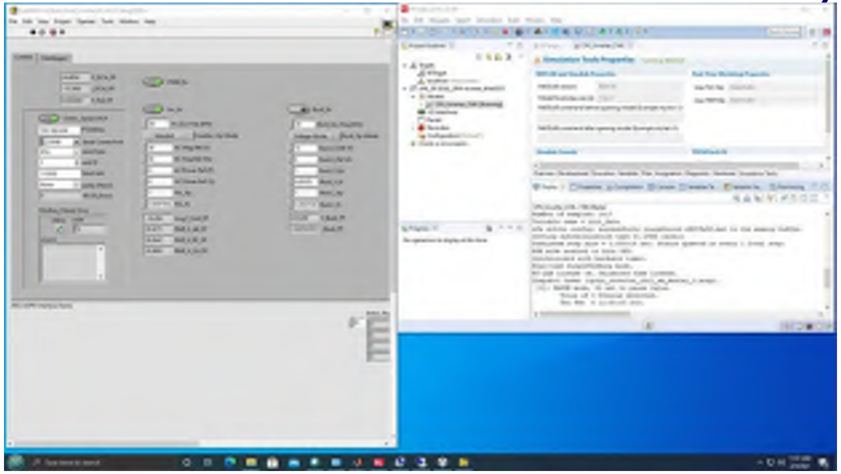
Available HIL/cHIL Systems at NCREPT

- **Typhoon HIL**
  - **6-Series**
- **OPAL-RT**
  - **OP5030 and OP4520**
- **dSPACE**
  - **MicroLabBox**

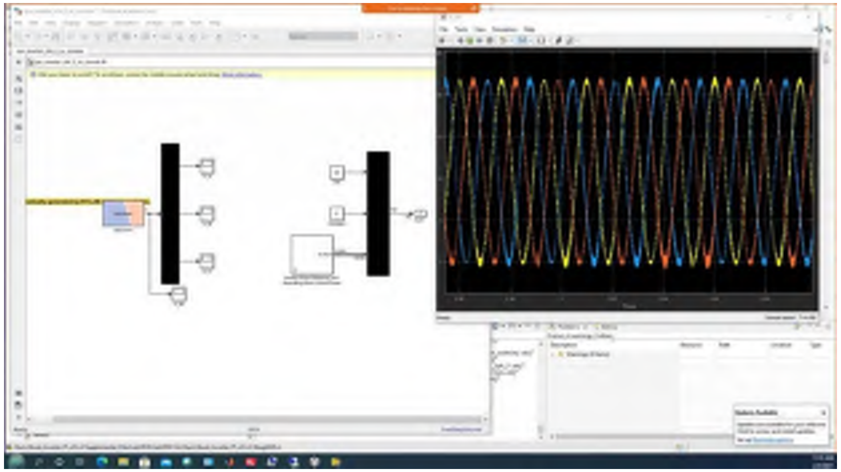


Carnegie Mellon University Electrical & Computer Engineering | UA Little Rock | University of Arkansas | Electric Cooperatives of Arkansas | Lehigh University | MIT | FIU Florida International University

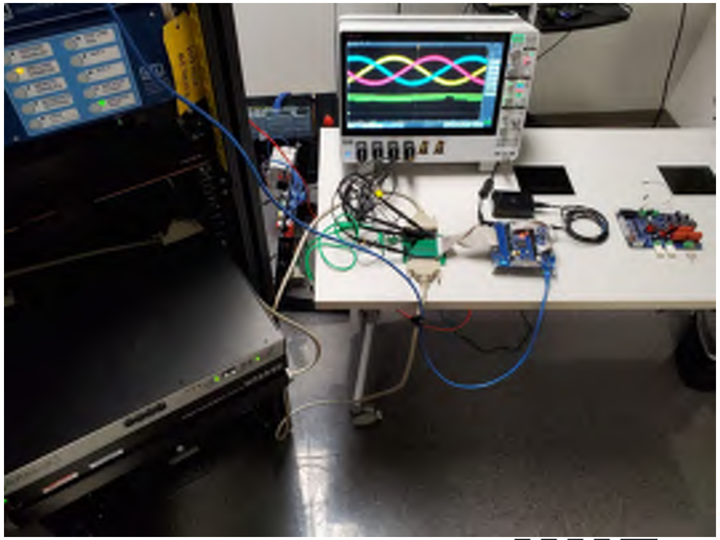
Testing Example: cHIL of 3-Phase Inverter



LabVIEW/Modbus Control Interface



OPAL-RT IDE and Real-Time Simulation Display

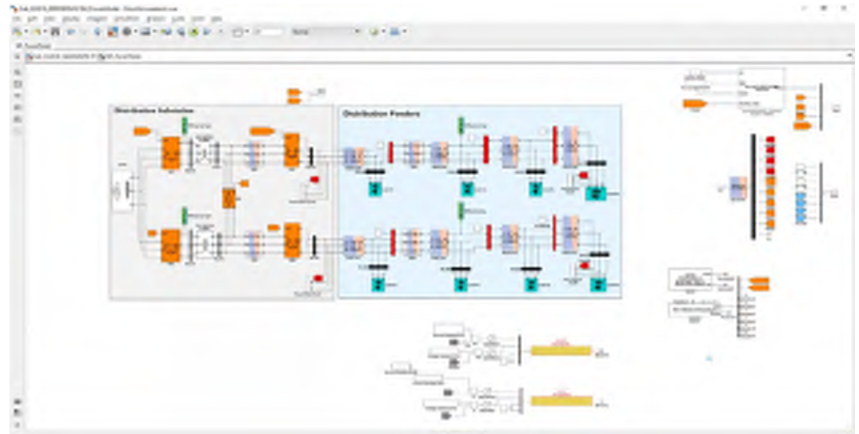


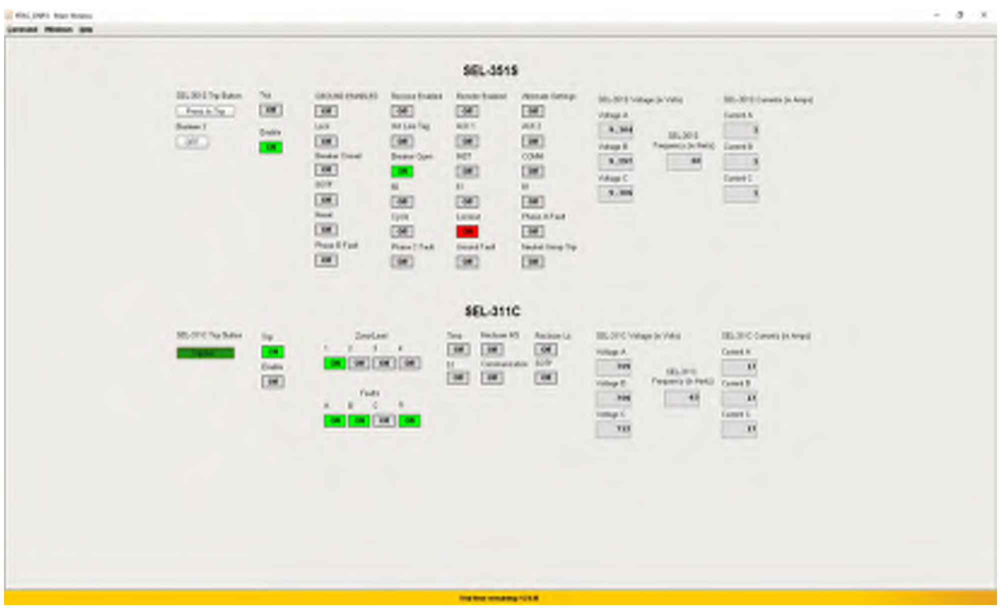
Testbed Assets: Cross-Domain Systems

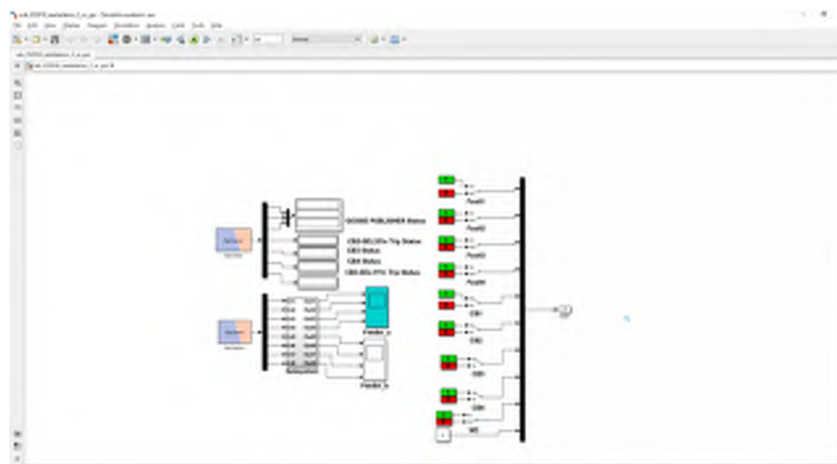
Cybersecurity for Energy Delivery Systems

HIL Discussion / Benefits

- Enables Multi-Feeder Simulation in Real-Time
- Analog/Digital I/O of Voltages/Currents
- PTs/CTs of Protection Relays bypassed
- IEC 61850 and DNP3 Communications
- PR Feedback into Simulation
- Shows Greater Grid Impact (PNNL Demo)







Carnegie Mellon University Electrical & Computer Engineering
UA Little Rock
University of Arkansas
Electric Cooperatives of Arkansas Your Local Energy Partners
Lehigh University
MIT
FIU Florida International University

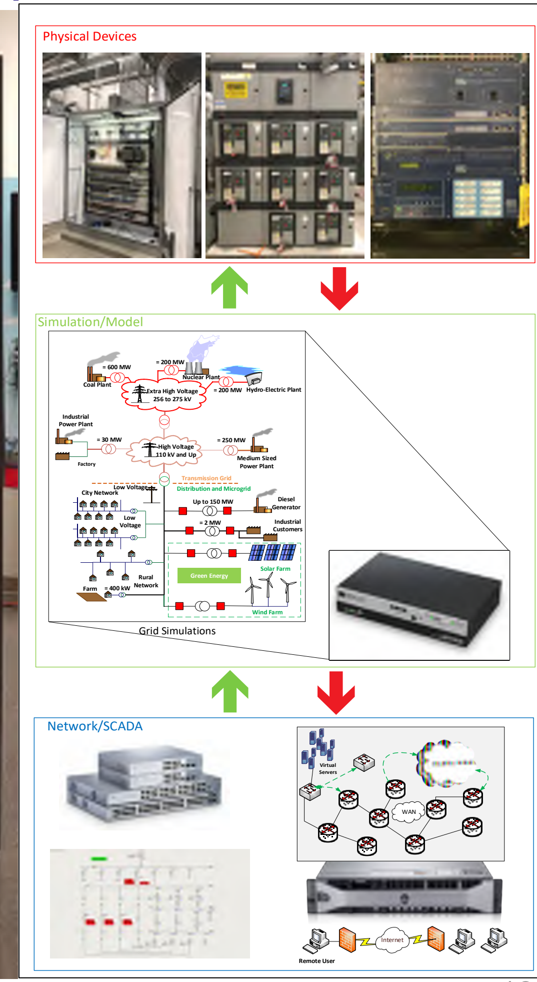
SEEDS

Integration: Cyber-Physical Approach

Cybersecurity for Energy Delivery Systems

Cyber-Physical Testing Approach

- **Real Power Flows**
  - Grid Simulator
  - Regenerative Loads
  - Resistive Loads
  - Integrated Metering
- **Emulated Networks**
  - Inter and Intra Substation Comms
  - Virtual Hypervisor Networking
  - GNS3 Network Simulations
- **Real-Time Simulations**
  - Initiate large-scale Fault Scenarios
  - Emulate Fault currents Safely
  - Virtual Devices

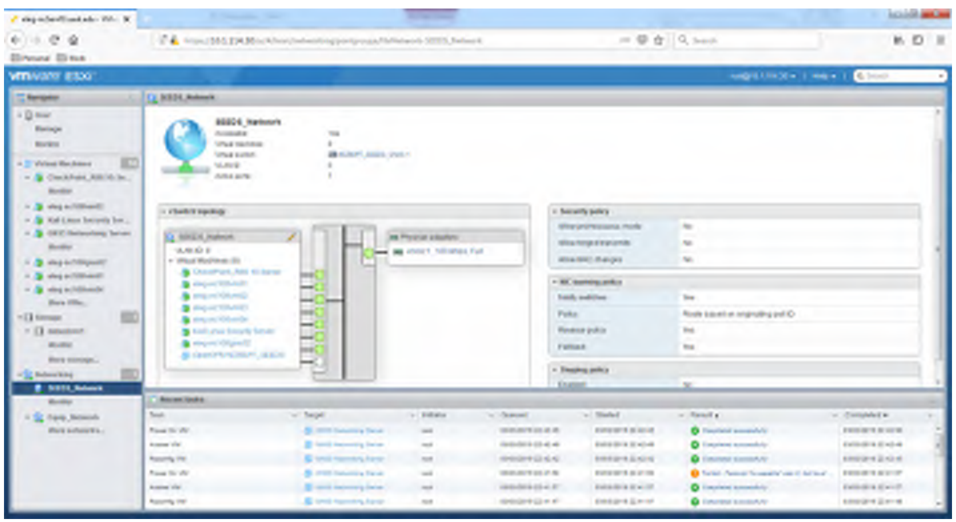


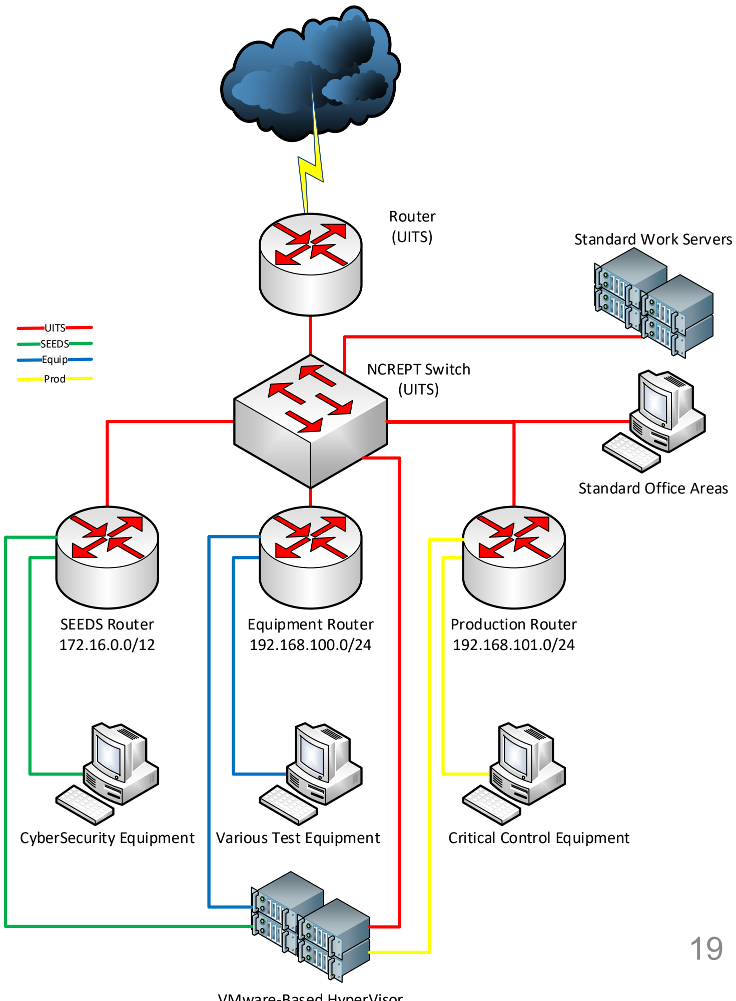
Networking: Network Segmentation

Cybersecurity for Energy Delivery Systems

Available Networking Resources at NCREPT

- **Networks**
  - Four Physical Network Segments
  - Virtually Infinite Simulated Networks
- **VMWare ESXI Hypervisor**
  - GNS3 Network Simulator
  - Virtual Routers and Switches
- **Remote Access**
  - Linux and Windows Workstations
  - OpenVPN Servers

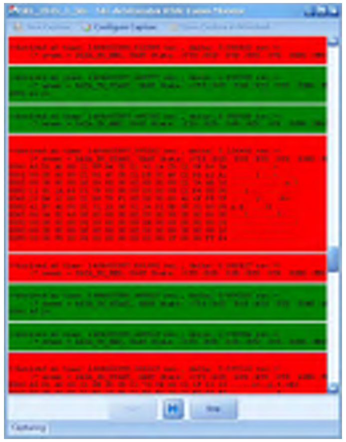


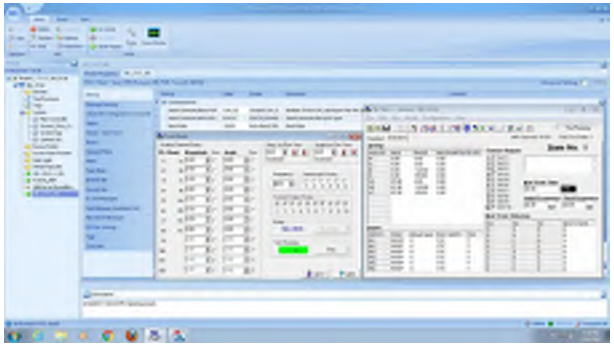


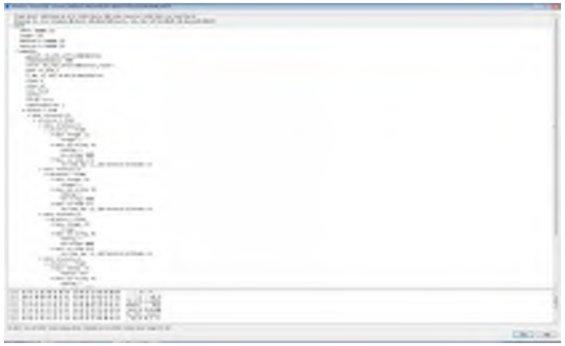
SEEDS

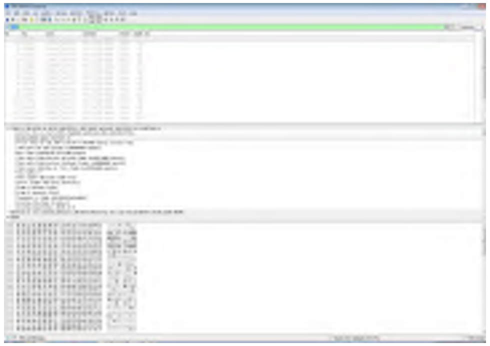
Protection Relays: SEL Resources

Cybersecurity for Energy Delivery Systems



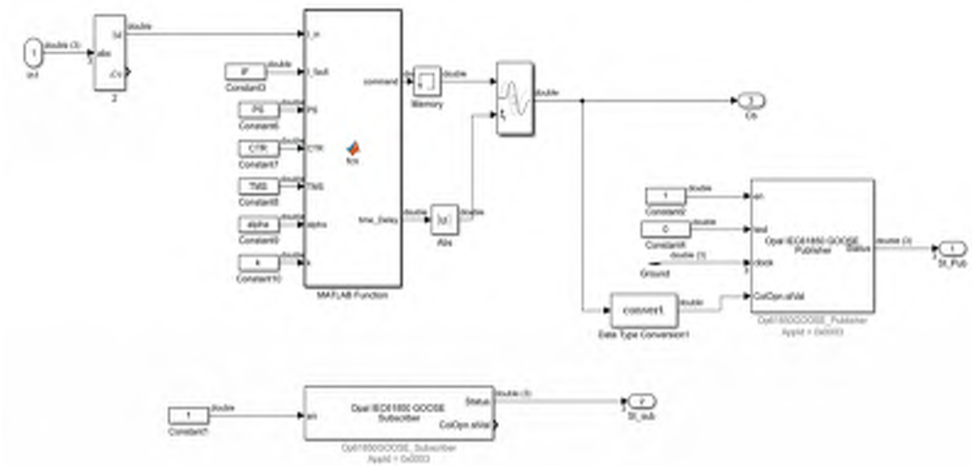


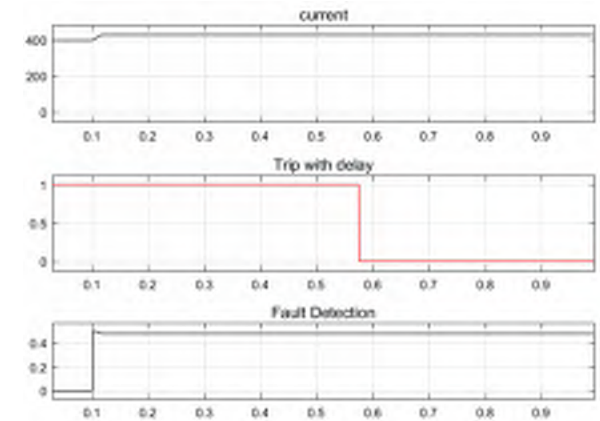


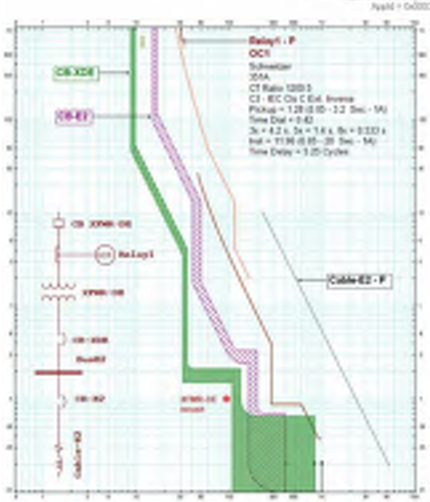


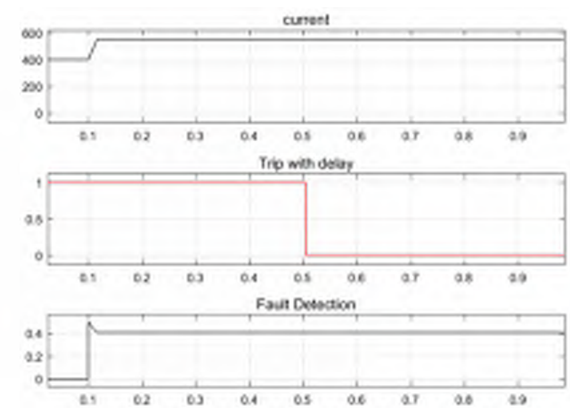
Real-Time Simulator: Protection Relay Design

Cybersecurity for Energy Delivery Systems









Future Work: Integration

Cybersecurity for Energy Delivery Systems

- **Super Lab and DETER Lab Integration**
- **Investigate integration and collaboration**
- **Multi-Site and International Effort**
- **Unique Challenges for Resource Sharing**

Source: https://ieeexplore.ieee.org/document/8458285

FIG 5 The Global RT Superlab participants and their interconnections. (Map courtesy of RWTH Aachen University.)

Table 1. The simulation models making up the Global RT Superlab.

Site	Grid	# Busses	Peers	HIL	Simulator
INL, Idaho Falls	Western Systems Coordinating Council	Nine	RWTH, WSU, USC, SNL, NREL, CSU	—	RTDS, Typhoon HIL, OPAL-RT
RWTH Aachen University, Germany	International Council on Large Electric Systems–High Voltage	12	INL, POLITO	—	RTDS
POLITO, Italy	International Council on Large Electric Systems–Medium Voltage	14	RWTH	—	OPAL-RT
Sandia National Laboratories, New Mexico	Distribution grid	Seven	INL	PHIL for PV inverters	OPAL-RT
NREL, Golden, Colorado	Distribution grid	Three	INL	PHIL for wind turbines	RTDS
University of South Carolina, Columbia	IEEE distribution test system	123	INL	CHIL, network emulation	OPAL-RT
Colorado State University, Fort Collins	IEEE distribution test feeder	13	INL	—	OPAL-RT
Washington State University, Pullman	Simplified Consortium for Electric Reliability Technology Solutions microgrid	Nine	INL	—	RTDS

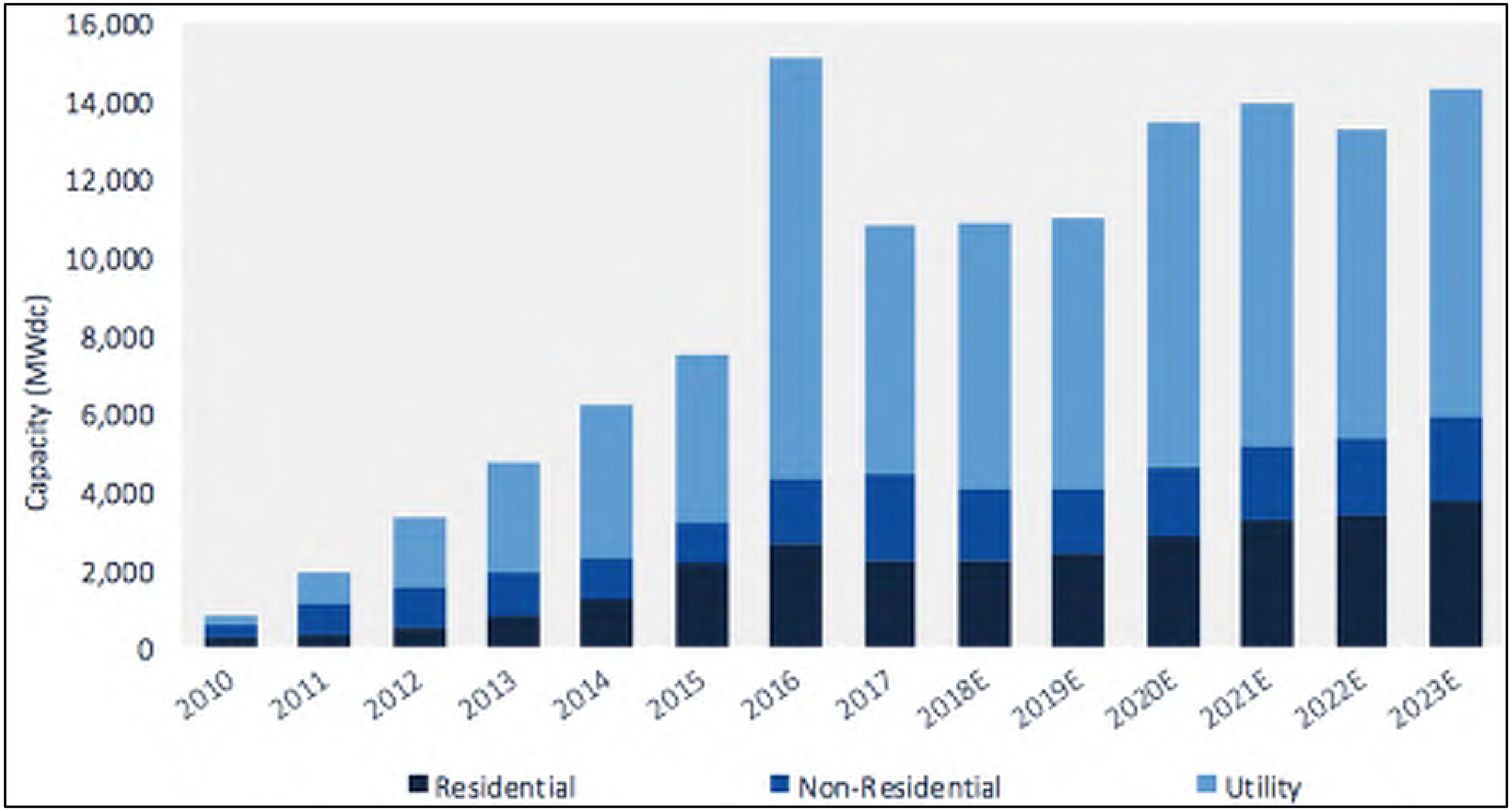
Carnegie Mellon University Electrical & Computer Engineering · UA Little Rock · University of Arkansas · Electric Cooperatives of Arkansas · Lehigh University · MIT · FIU Florida International University

Presentation Outline

- NCREPT Facility Overview
- Cyber Testbed
- **Distributed Energy Resources**
  - **History and Projections**
  - **Example Installations**
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

History and Projections: Solar Energy

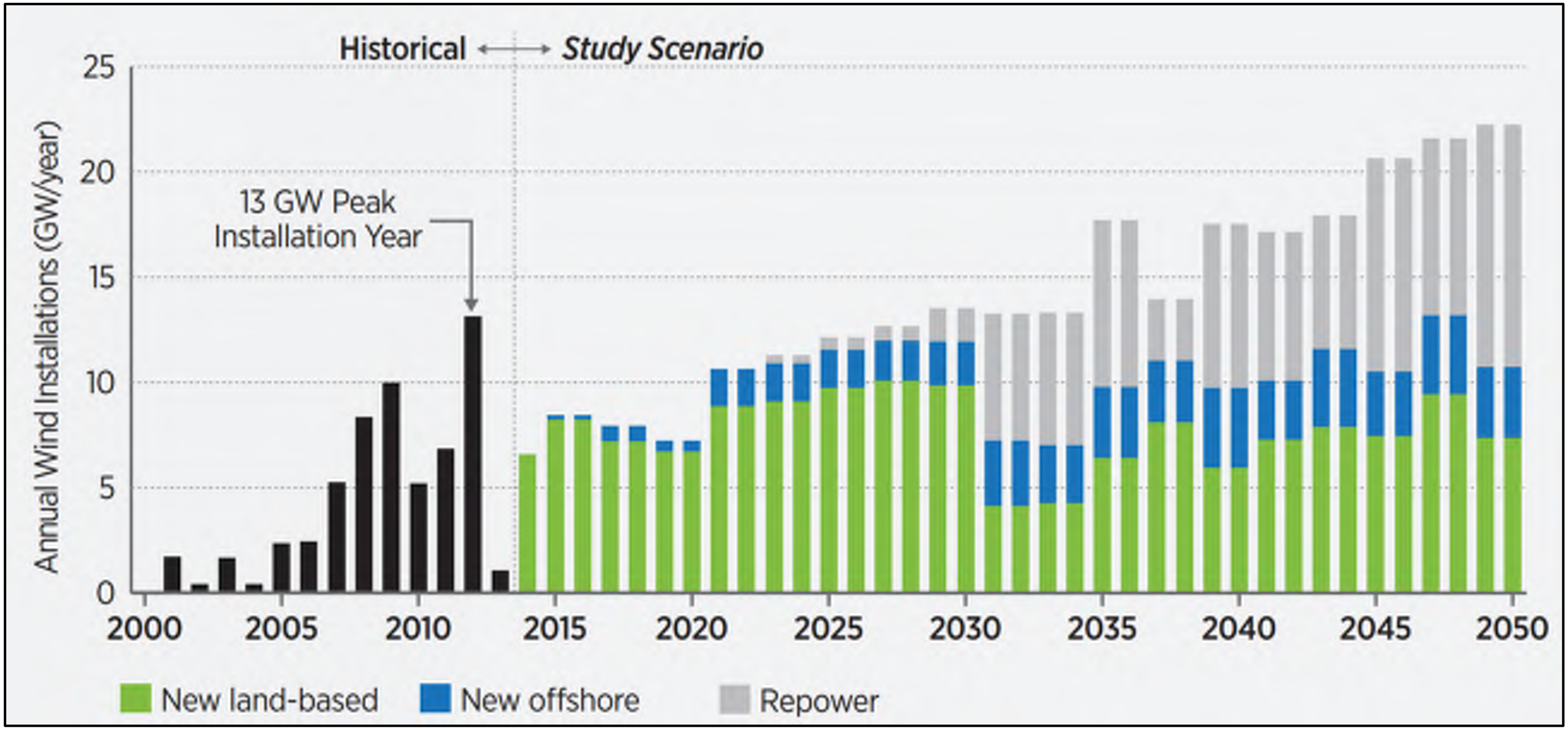
Cybersecurity for Energy Delivery Systems



Central and distributed solar energy generation [1]

History and Projections: Wind Energy

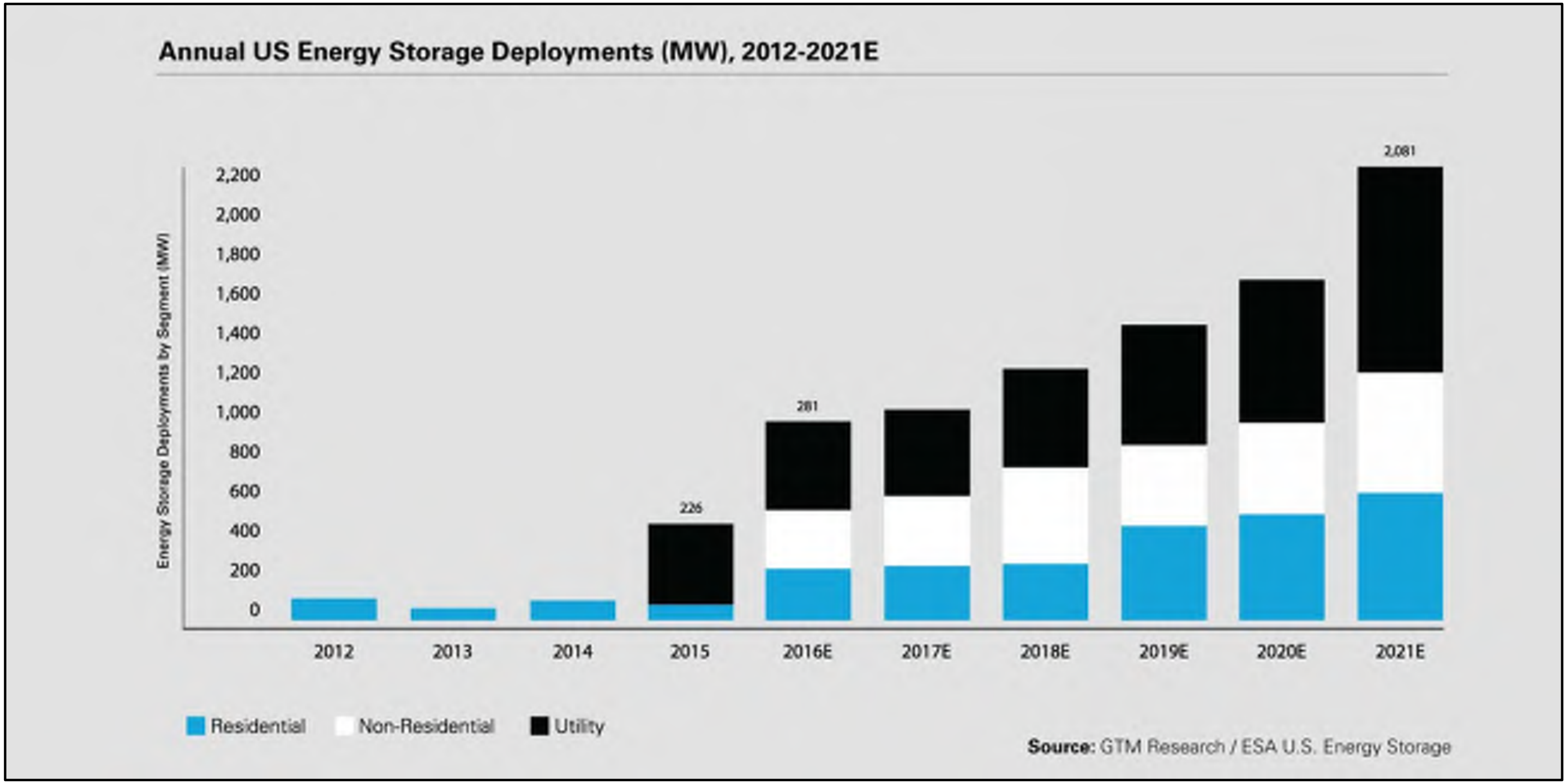
Cybersecurity for Energy Delivery Systems



Trends in wind energy generation [2]

History and Projections: Energy Storage

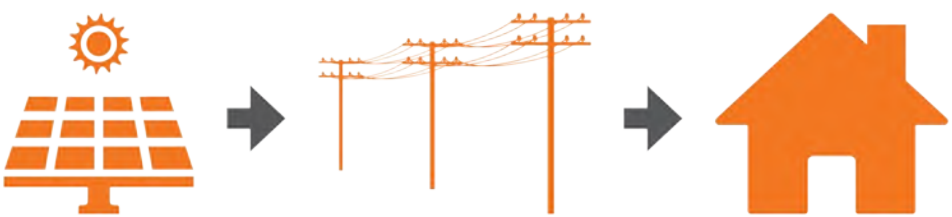
Cybersecurity for Energy Delivery Systems



Central and distributed energy storage [3]

Example: Solar Installation

- Solar Power is increasing in popularity with home owners and businesses.
  - According to a recent article solar utilization has doubled since last year in Arkansas
  - It has increased more than 40x since 2007
- Local utilities are also installing solar arrays such as the “Ozark One” project.
  - Residents may participate in this communal solar installation via purchasing shares.
- Communications between inverters and the utility are critical for optimal operations and accurate billing.



Community Solar Installation
Credit: ozarksecc.com/one

Example: BESS Installation

- With the increasing penetration of renewable energy, intermittent availability is a growing issue
- More efficient use of generation resources, such as peak shaving techniques, also contributes to sustainability
- Battery Energy Storage Systems (BESS) provide solutions to both of these issues
- Advanced Controls, Communication, and Coordination are needed for these systems to operate properly

Tesla PV Installation
Credit: Tesla

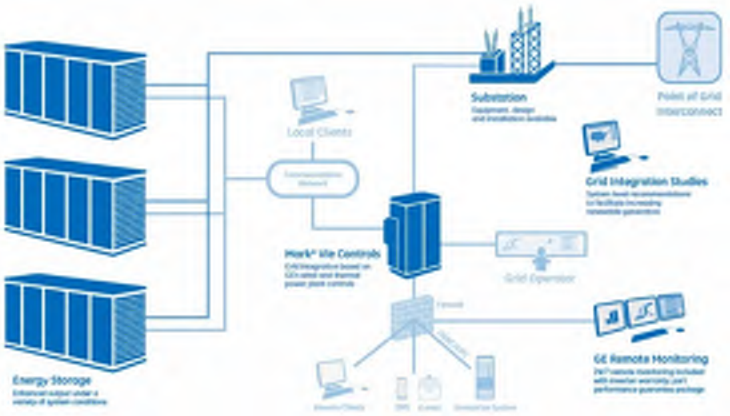


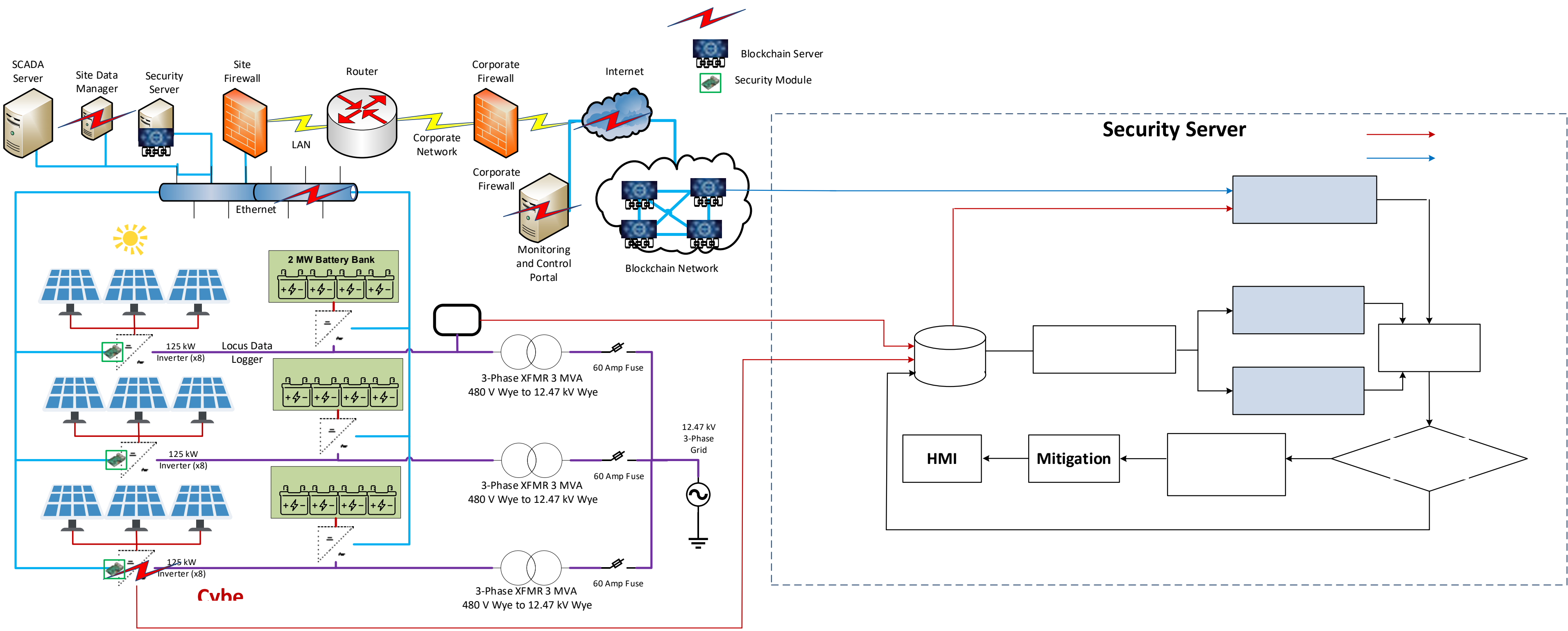
Diagram of Energy Generation and Storage
Credit: GE

Presentation Outline

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- **Example DER Cybersecurity Problem**
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Example DER Cybersecurity Problem

Cybersecurity for Energy Delivery Systems



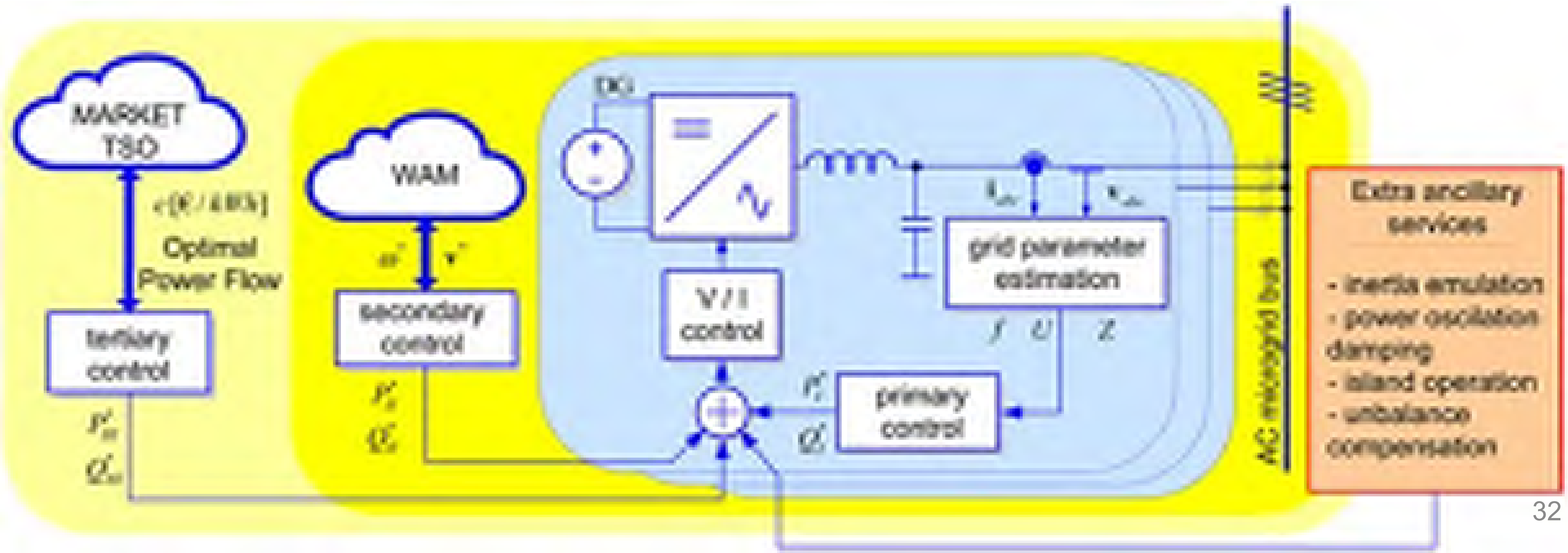
Presentation Outline

Advanced Controls

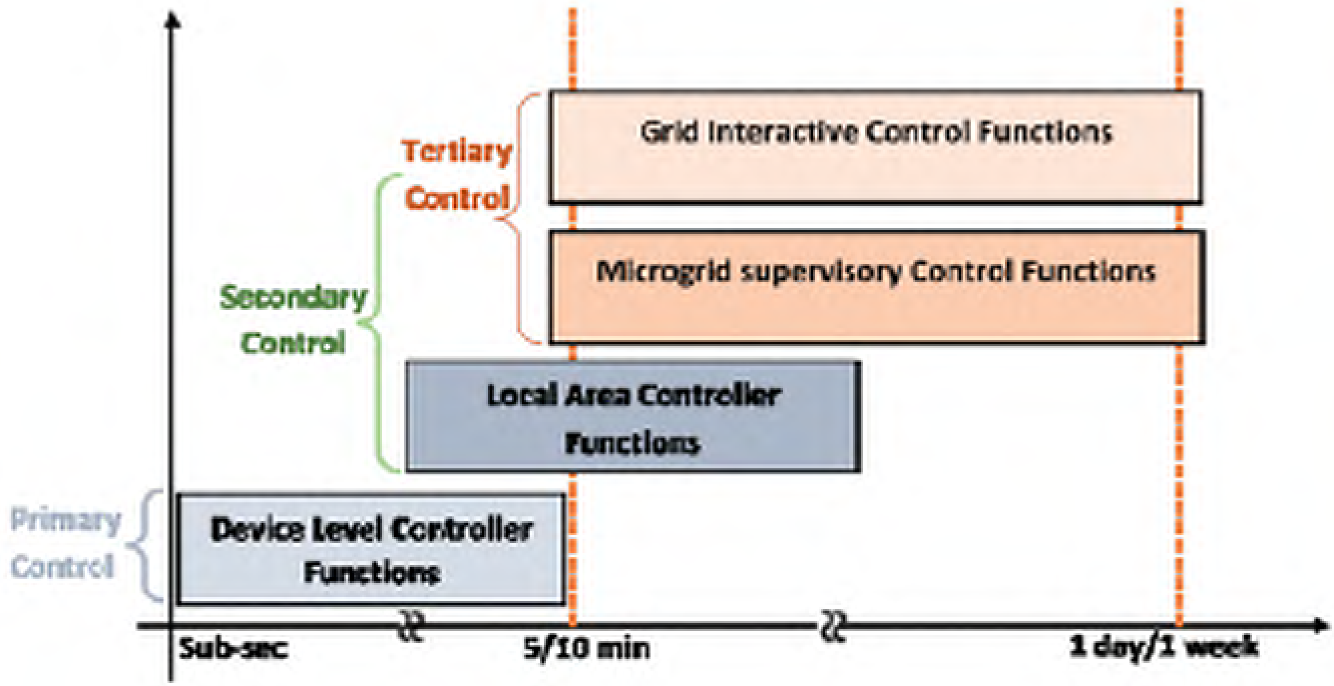
❖ Need for Secondary and Tertiary Control

- ➢ Coordination of Resources for Optimal Power Flow
- ➢ Maximize Generation while maintaining Power Quality

❖ Increased Attack Surfaces



Advanced Controls



Control Level Time-Scales. Credit: IEEE Std 2030.7-2017

Presentation Outline

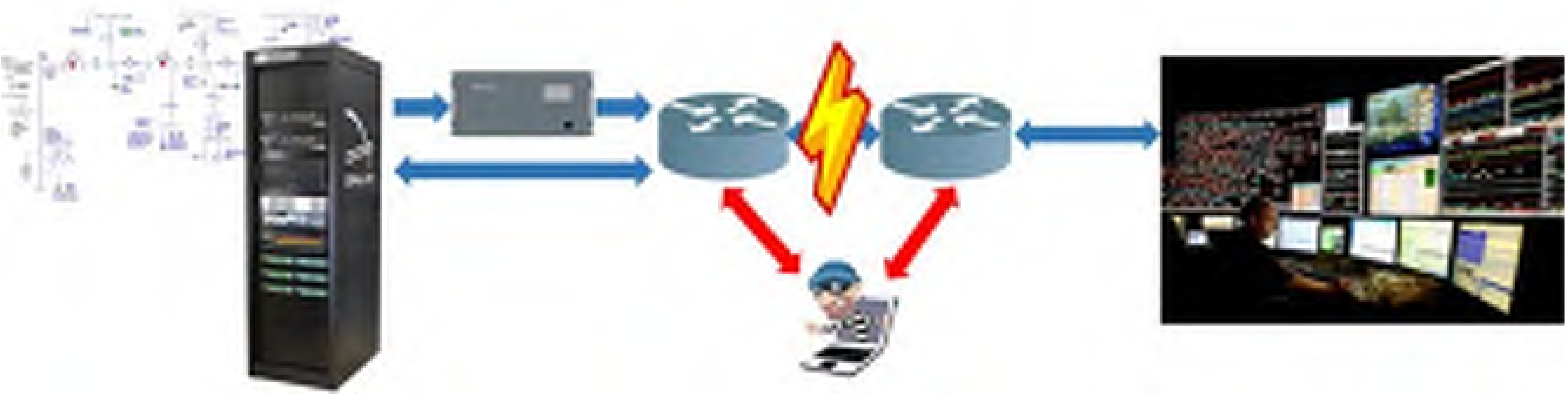
- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- **Attack Scenarios**
- Best Practices
- Research Trends
- Summary
- Further Reading & References

SCADA Definition

- What is SCADA?
  - Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS), Distributed Control System (DCS), etc. generally refer to the systems which control, monitor, and manage the nation's critical infrastructures such as electric power generators, subway systems, dams, telecommunication systems, natural gas pipelines, and many others. Simply stated, a control system gathers information and then performs a function based on established parameters and/or information it received.

*Source: https://us-cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

Attack Scenario I


Man-in-the-Middle attack diagram. Credit: OPAL-RT

Man-in-the-Middle (MitM)
A MitM situation occurs when an external attacker is capable of intercepting, modifying, suppressing or replaying network packets undetected by tricking two communication nodes to believe they are still communicating normally.

Attack Scenario II

Denial-of-Service attack diagram. Credit: OPAL-RT

Denial-of-Service (DoS)
DoS can render a service unavailable either through a direct or indirect attack. It also refers to physical attacks on communication infrastructure, such as the cutting of wires or wireless jamming.

Attack Scenario III

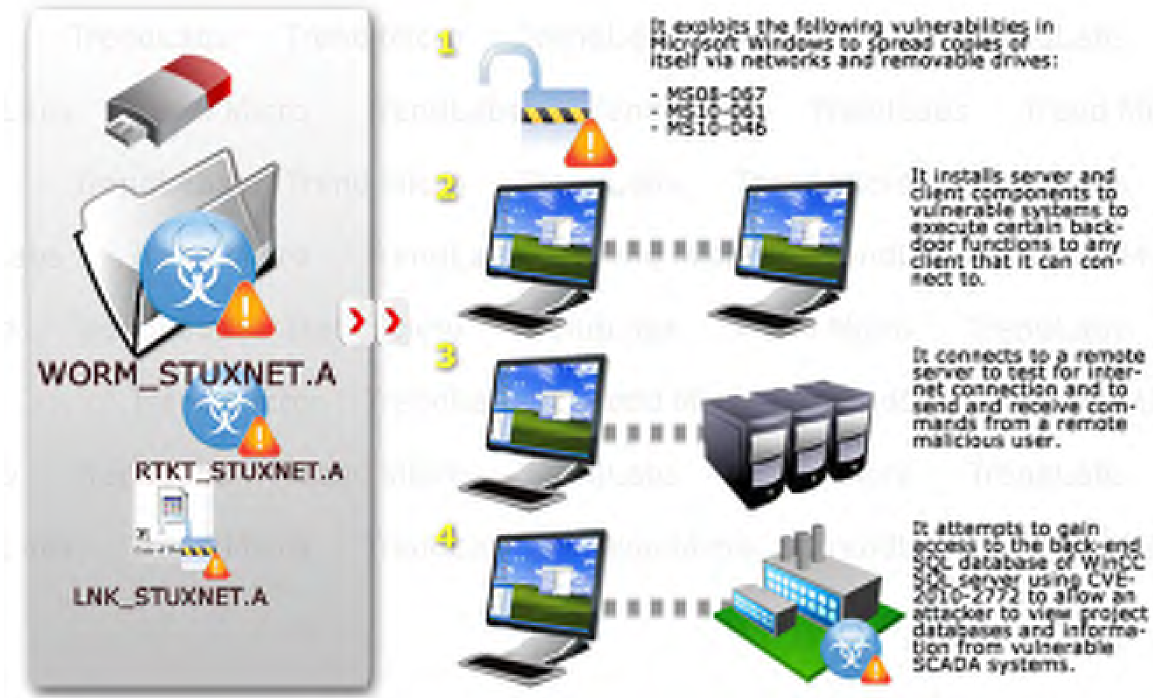
GPS Spoofing attack diagram. Credit: OPAL-RT

GNSS Spoofing/Meaconing

The act of causing Global Navigation Satellite System (GNSS) receivers to lock onto simulated or replayed satellite signals instead of real ones, effectively causing the receiver to locate itself at the wrong position and/or time. This class of attack is a major threat to PMU and synchrophasor systems, which are heavily reliant on time synchronization.

Stuxnet Attack

Cybersecurity for Energy Delivery Systems



Stuxnet diagram.
Credit: Trendmicro [7]

- **Advanced Malware Targeting Industrial Systems [4]**
- **Allowed Access to Discover Facility Architecture**
- **Specific System Function Calls Sent to Field Devices [5]**
- **Destroyed an Estimated 984 Nuclear Centrifuges [6]**

SEEDS

2015/2016 Ukraine Attack

Cybersecurity for Energy Delivery Systems

- **Utilized "Black Energy 3" Malware**
- **Gained Access to Industrial Control Systems (ICSs)**
- **Target Field Devices Using Custom Malicious Firmware**
- **225,000 Customers Without Power (1-6 hours)**
- **30 Substations Disabled**

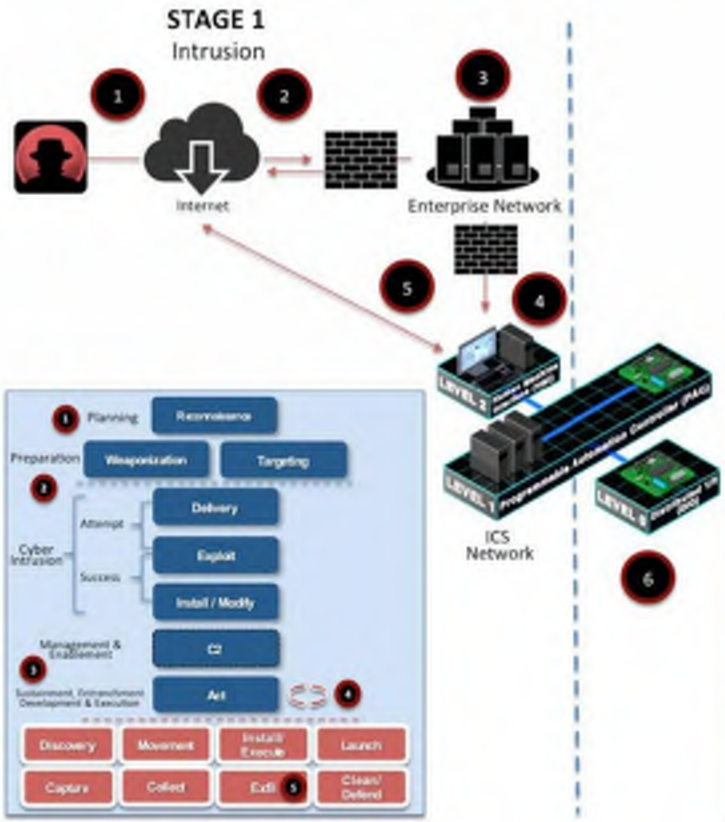
Overlapping vulnerabilities and attacks related to Ukraine Event. Source: E-ISAC-TLP Report [8]

- **DoS Attack** Utilized bots to "flood" Call/Service centers
- **Malicious Firmware** Disabled and/or destroyed devices
- **Spearfishing** Resulted in employees providing credentials
- **Malware** Implemented DDoS and Trojan Botnet "Black Energy"

Carnegie Mellon University Electrical & Computer Engineering · UA Little Rock · University of Arkansas · Electric Cooperatives of Arkansas · Lehigh University · MIT · FIU Florida International University

Cyber Kill Chain

Cybersecurity for Energy Delivery Systems



STAGE 2
Attack

Stage 1: Planning, Preparation, Cyber Intrusion, Management and Enablement (Explore/Exploit), Deployment and Entrenchment (Execute Malware)

Stage 2: Attack Development, Validation, ICS Attack

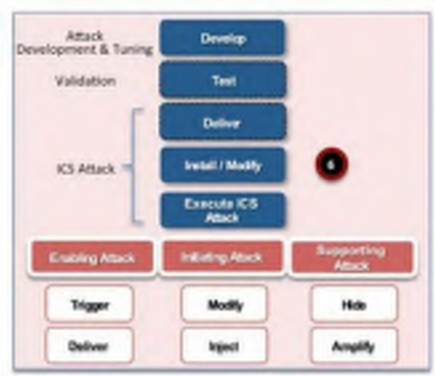


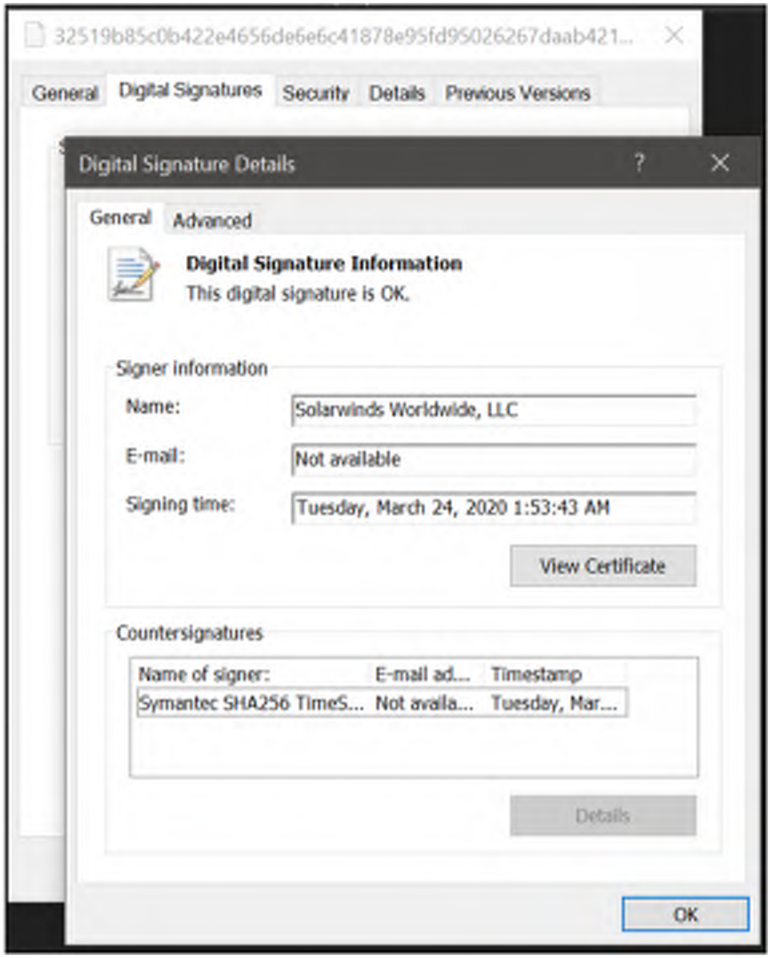
Diagram of stages of ICS Cyber Kill Chain. Source: Idaho National Labs Aug 2016 "INL/EXT-16-40692" [9]

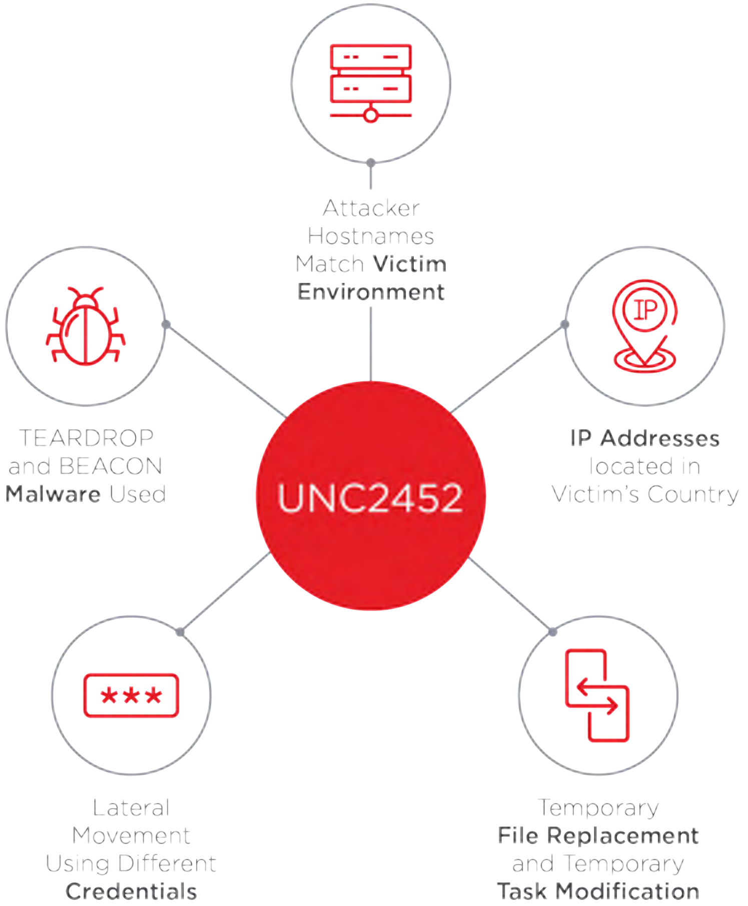
- **Common Attack Scenario against Utilities**
- **Incorporates Phishing, Waterhole, Malware, and MiTM Attacks**

Attacks/Notes

- Florida's Oldsmar Water Treatment System
  - Sodium hydroxide, or lye, to more than 100 times normal
  - TeamViewer, Potential of shared passwords for remote access
- Aurora Generator Test
  - 27-Ton Generator vs less than 30 lines of code
  - Kinetic Attacks
- Bingham County Ransomware
  - Brute-Force Attack on Open Port
  - Paid Ransom to restore two servers
- Coffee Machine Ransomware
  - Unencrypted WiFi
  - No code signing for firmware updates
- SolarWinds
  - Software Supply Chain and Firmware Attacks
  - Compromised update to SolarWinds' Orion software
  - Currently believed March 2020 Campaign Start Date
  - Backdoor access to allow credential harvesting and pivoting

Solarwinds Orion





*Source: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- **Best Practices**
- Research Trends
- Summary
- Further Reading & References

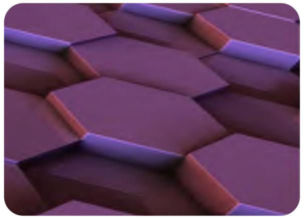
Approaches to Cybersecurity

Cybersecurity for Energy Delivery Systems

Eliminate the Bad Guys

Protect the Perimeter

Reduce Vulnerabilities



Segment the Architecture

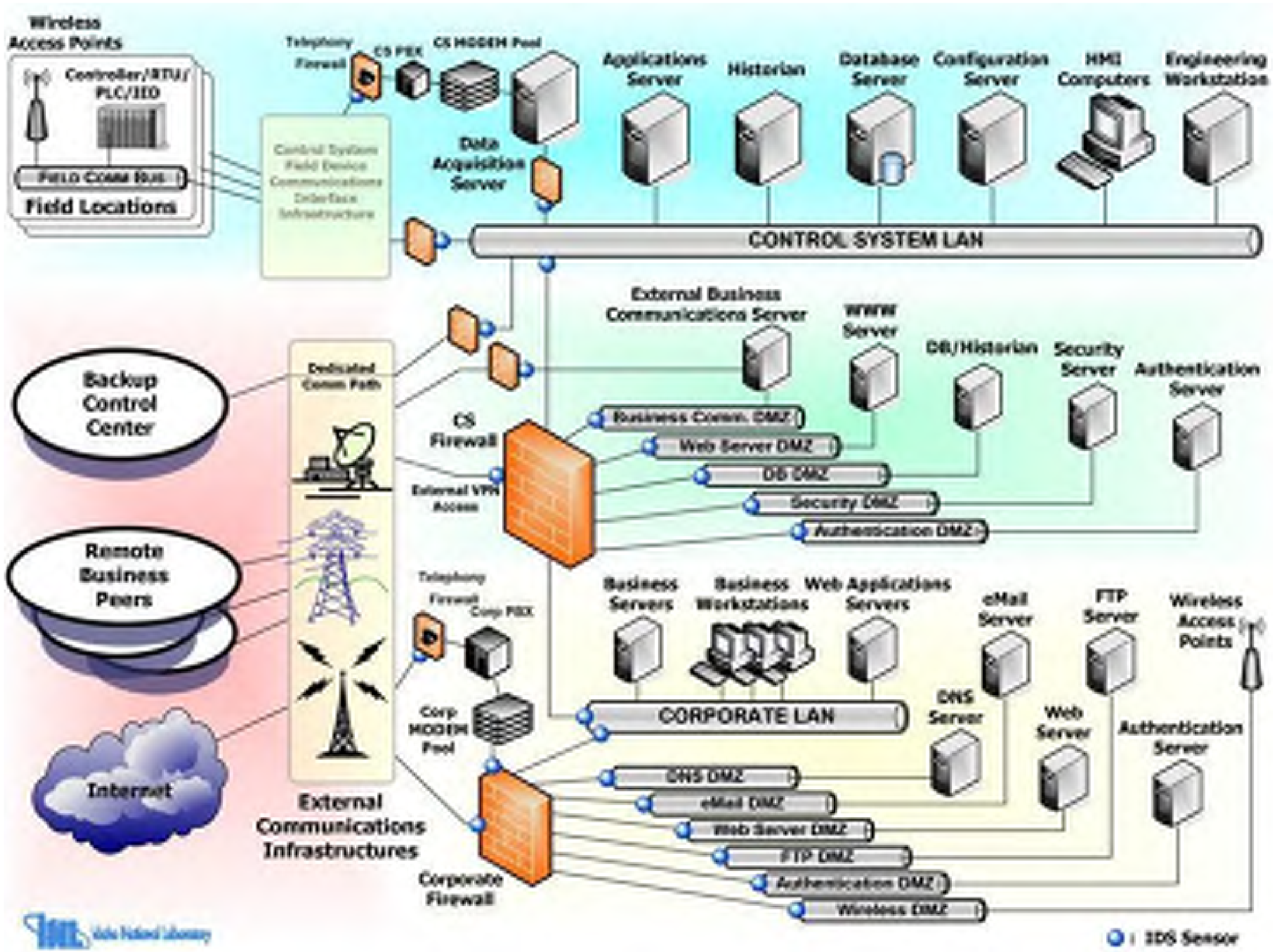
React to Breach

**Source: Craig Miller - NRECA*

SEEDS

Secure Architecture Design

Cybersecurity for Energy Delivery Systems



CISA Best Practices

- CISA Recommended Practices
  - Keep Antivirus Software/Definitions Up-to-date
  - Implement ICS Defense-in-Depth Strategies
  - Create Cyber Forensics Plans for Control Systems
  - Develop ICS Cybersecurity Incident Response Plan
  - OT/IT Collaborations for Proper Firewall Deployment
  - Patch Management
  - Secure ICS Modems\Access
  - Cross-Site Scripting Mitigation
  - Managing Remote Access to ICS

*Source: https://us-cert.cisa.gov/ics/Recommended-Practices

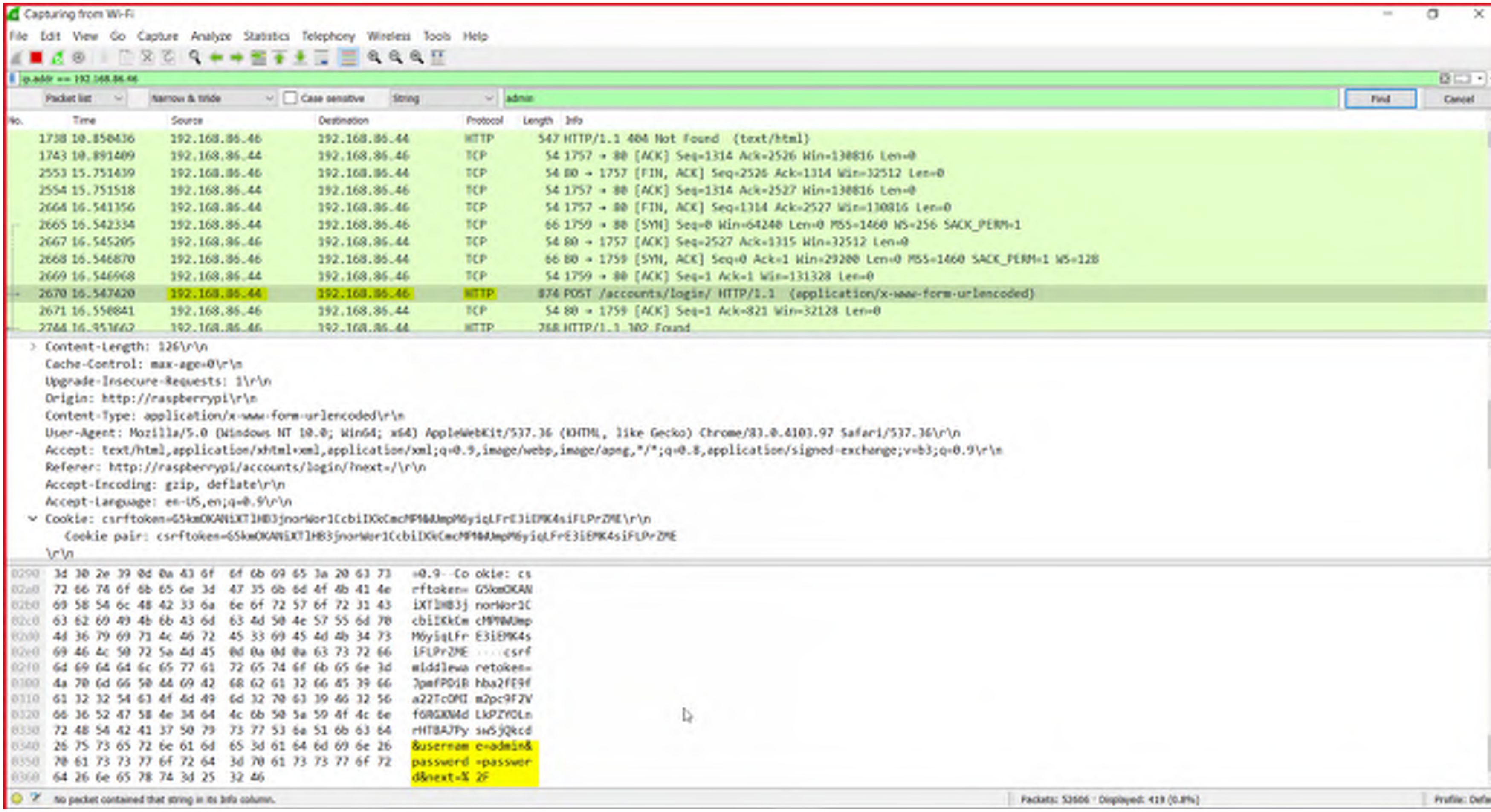
NERC CIP Standards

- NERC Current CIP Standards
  - NERC CIP-002-5.1a (BES Cyber System Categorization)
  - NERC CIP-003-8 (Security Management Controls)
  - NERC CIP-004-6 (Personnel & Training)
  - NERC CIP-005-6 (Electronic Security Perimeter(s))
  - NERC CIP-006-6 (Physical Security of BES Cyber Systems)
  - NERC CIP-007-6 (System Security Management)
  - NERC CIP-008-6 (Incident Reporting and Response Planning)
  - NERC CIP-009-6 (Recovery Plans for BES Cyber Systems)
  - NERC CIP-010-2 (Configuration Change and Vulnerability Assessments)
  - NERC CIP-011-2 (Information Protection)
  - NERC CIP-013-1 (Supply Chain Risk Management)
  - NERC CIP-014-2 (Physical Security)

*Source: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

TPM Benefits: Encryption

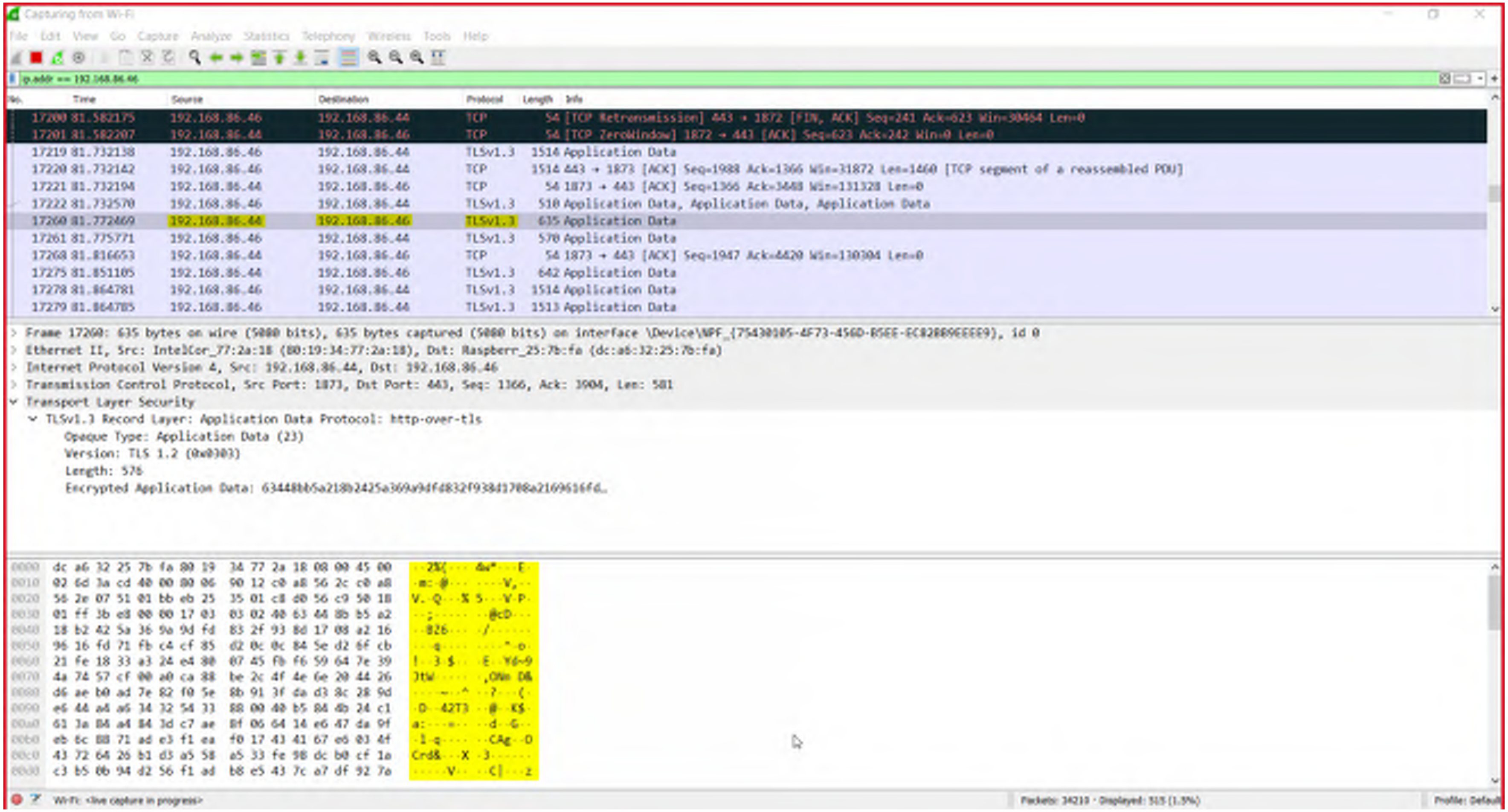
Cybersecurity for Energy Delivery Systems



WireShark Capture of Unencrypted User Credentials (HTTP)

TPM Benefits: Encryption

Cybersecurity for Energy Delivery Systems

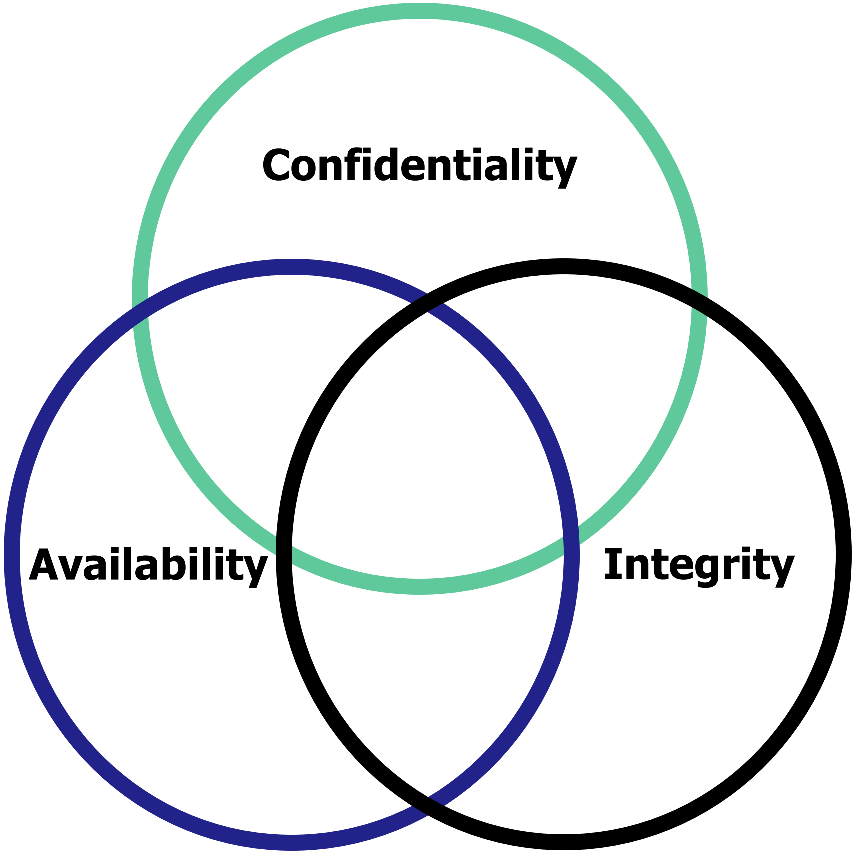


WireShark Capture of Encrypted User Credentials (HTTPS)

Presentation Outline

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- **Research Trends**
- Summary
- Further Reading & References

CIA Triad Overview

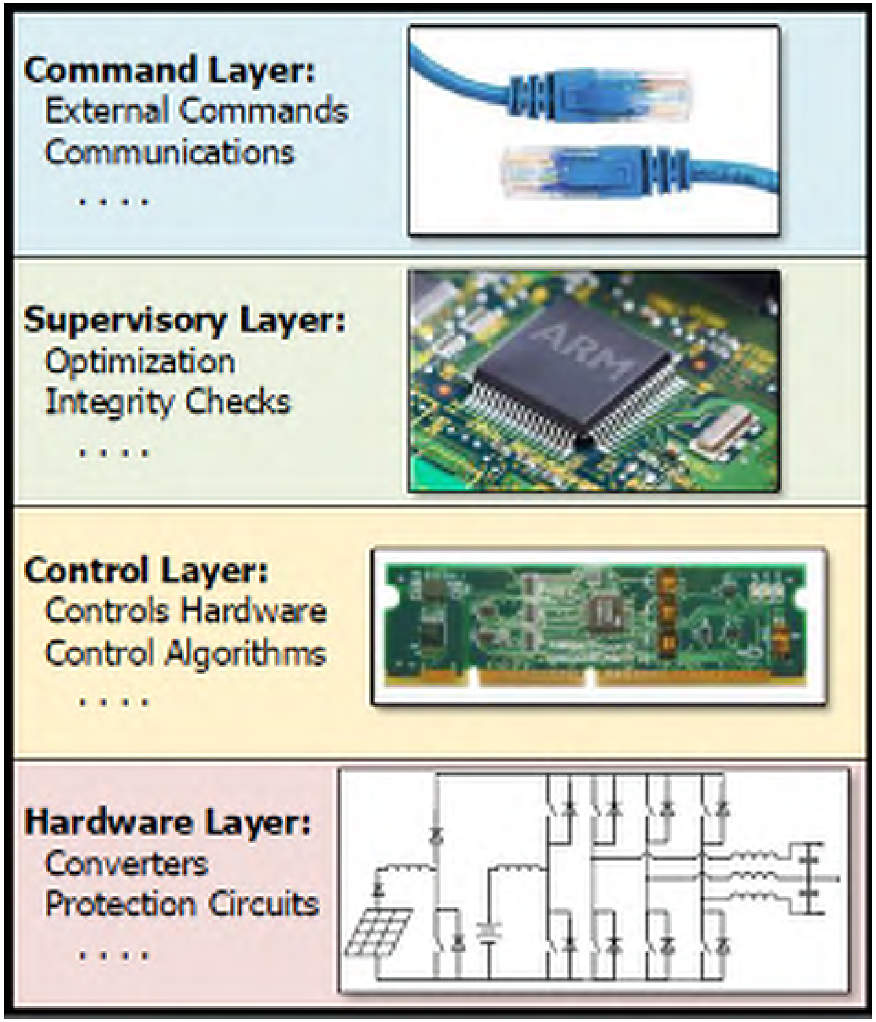


Information security CIA Triad

- Confidentiality of Data
  - Authorized Use and View
  - Privacy
- Availability of Data
  - Access
  - Control
- Integrity of Data
  - Validity
  - Consistency
  - Predictability
- Energy Systems
  - Availability of Power
  - Integrity of Power

Layered Approach

- ❑ **Command Layer**
  - Command Validation
  - Communication Encryption
- ❑ **Supervisory Layer**
  - Watchdog Timers
  - Algorithmic State Machines
- ❑ **Control Layer**
  - Reference Limits
  - State Awareness
  - Dead Time Enforcement



Cyber-Secure by Design Layered Approach

Carnegie Mellon University Electrical & Computer Engineering · UA Little Rock · University of Arkansas · Electric Cooperatives of Arkansas · Lehigh University · MIT · FIU Florida International University

Cyber-Hard by Design

- Robust Protection Requires Multiple Layers
- Hardware-Level sub-Module Authentication
  - Custom Keys Installed on sub-Modules for Identification
  - Encrypted Communication Between sub-Modules
- External Authentication
  - Certificate Keys Managed by Trusted Certificate Authority
  - Custom Hardware Key Required for Firmware Update
  - Encrypted Communications for Local/Remote SCADA
- Software and Hardware Intrusion Detection
- New Encryption Techniques for Higher Performance
- Control systems (e.g., state machines) must address all possible states
- Non-sensical/destructive acts must be disallowed by design

Cost of Security

- Processing overhead of encryption
  - Benchmark performances
  - Interrupt Service Routine/Polling/Co-Processor
- Impact on system operation
  - Cost/Benefit analysis of securities
  - Time delay of communication
  - Control algorithm stability with added security
  - Additional resources required, increasing cost or lowering performance
- Additional development time of grid-connected power electronics
  - Possible time savings by reuse of standard and secure techniques
  - Reduced downtime by using robust designs and software
  - Flexible controls to allow upgrades and reduce replacement of hardware

Presentation Outline

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- **Summary**
- Further Reading & References

Summary

- Penetration of Distributed Energy Resources is Increasing
- Higher-Level Coordination is Required
  - Increased Power Quality
  - Optimized Power Flow
- Coordination Requires Communication
  - Peer-to-Peer
  - TOU Pricing
  - Protection Relays
  - Dispatch and Load Predictions
- Increased Communications mean Increased Attack Surfaces
- Implement Best Practices to Mitigate Risks
- Additional Research Required
  - Coordinate Resources
  - Optimize Power Flow
  - Mitigate Current and Future Risk

Presentation Outline

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
  - History and Projections
  - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- **Further Reading & References**

Further Reading

- https://us-cert.cisa.gov/ics/Recommended-Practices
- https://us-cert.cisa.gov/ics/Secure-Architecture-Design
- https://blog.rsisecurity.com/what-are-the-10-fundamentals-of-nerc-cip-compliance/
- https://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf
- https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- https://us-cert.cisa.gov/ncas/alerts/aa21-042a
- https://us-cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf
- https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/

References

[1] https://www.greentechmedia.com/research/subscription/u-s-solar-market-insight#gs.wpfDw8k
[2] "Wind Vision," Energy.gov. [Online]. Available: https://www.energy.gov/eere/wind/maps/wind-vision. [Accessed: 25-Sep-2018].
[3] "Electric energy storage: preparing for the revolution | White & Case LLP International Law Firm, Global Law Practice." [Online]. Available: //www.whitecase.com/publications/insight/electric-energy-storage-preparing-revolution. [Accessed: 25-Sep-2018].
[4] "Stuxnet worm brings cyber warfare out of virtual world." [Online]. Available: https://phys.org/news/2010-10-stuxnet-worm-cyber-warfare-virtual.html. [Accessed: 25-Sep-2018].
[5] R. Langner, Cracking Stuxnet, a 21st-century cyber weapon. Available: https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon/transcript. [Accessed: 25-Sep-2018].
[6] "Stuxnet Worm Attack on Iranian Nuclear Facilities." [Online]. Available: http://large.stanford.edu/courses/2015/ph241/holloway1/. [Accessed: 25-Sep-2018].
[7] "STUXNET Malware Targets SCADA Systems - Threat Encyclopedia - Trend Micro USA." [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems. [Accessed: 25-Sep-2018].
[8] R. M. Lee, M. J. Assante, T. Conway, Analysis of the Cyber Attack on the Ukrainin Power grid, 2016, [online] Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[9] Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. (2016). [ebook] Mission Support Center, Idaho National Laboratory. Available at: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf [Accessed 25 Sep. 2018].