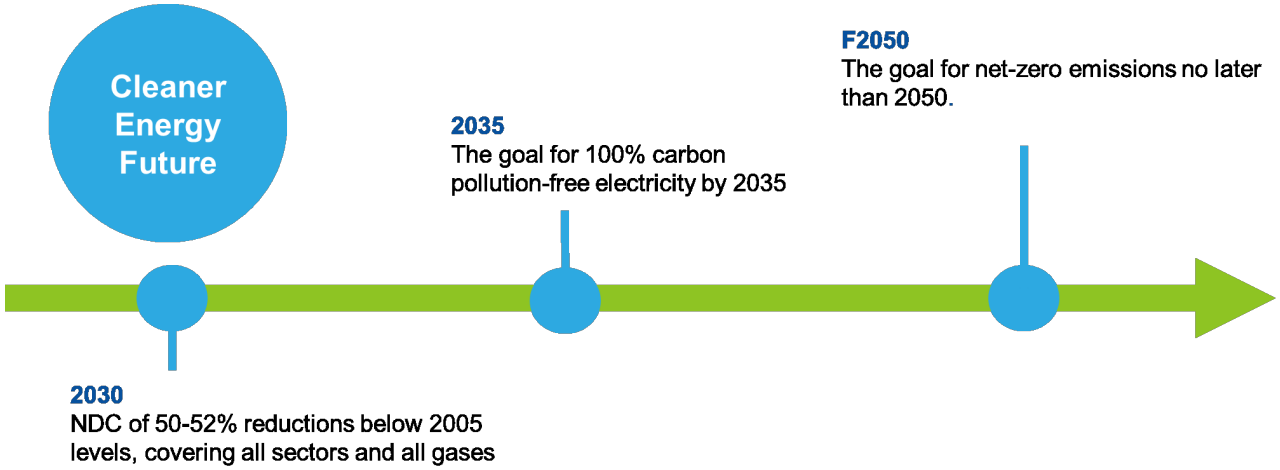
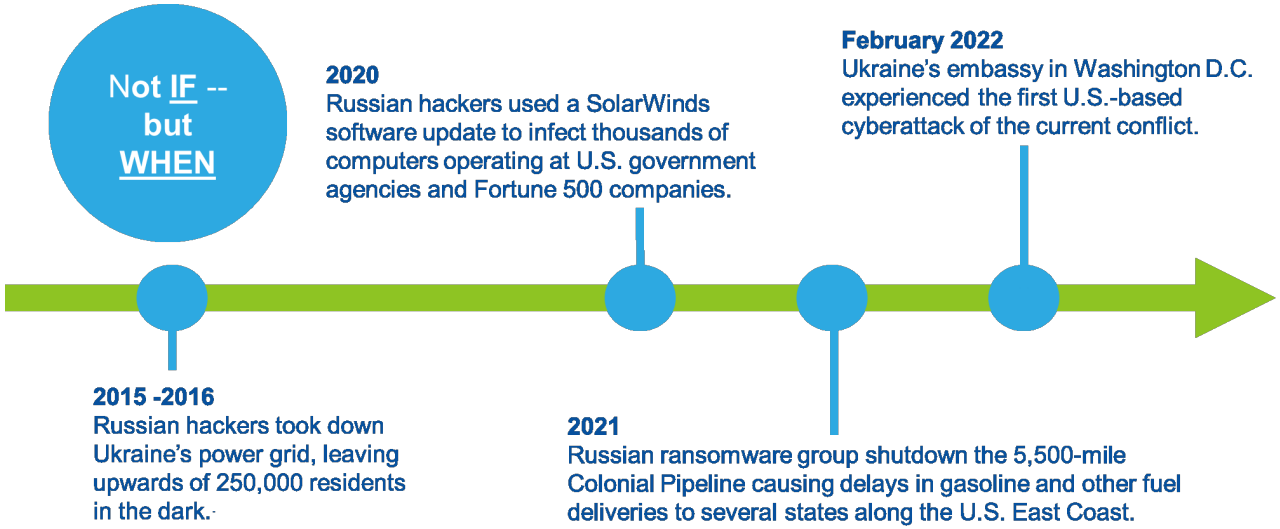
Securing Path to Net Zero: Enabling Concept to Scale Capabilities

Idaho National Laboratory

INL/MIS-23-73313

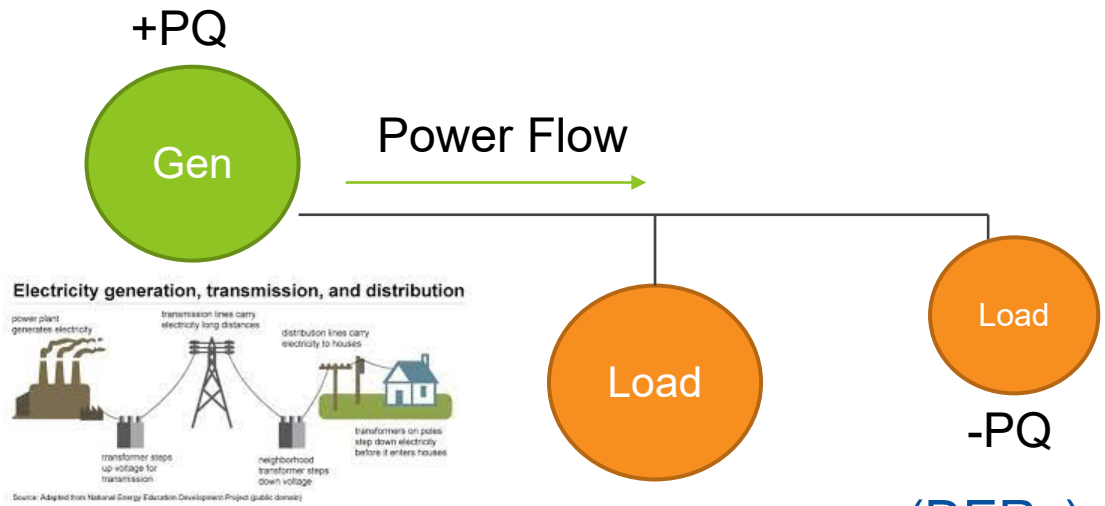
Why the focus on ‘Secure Renewables’ ?

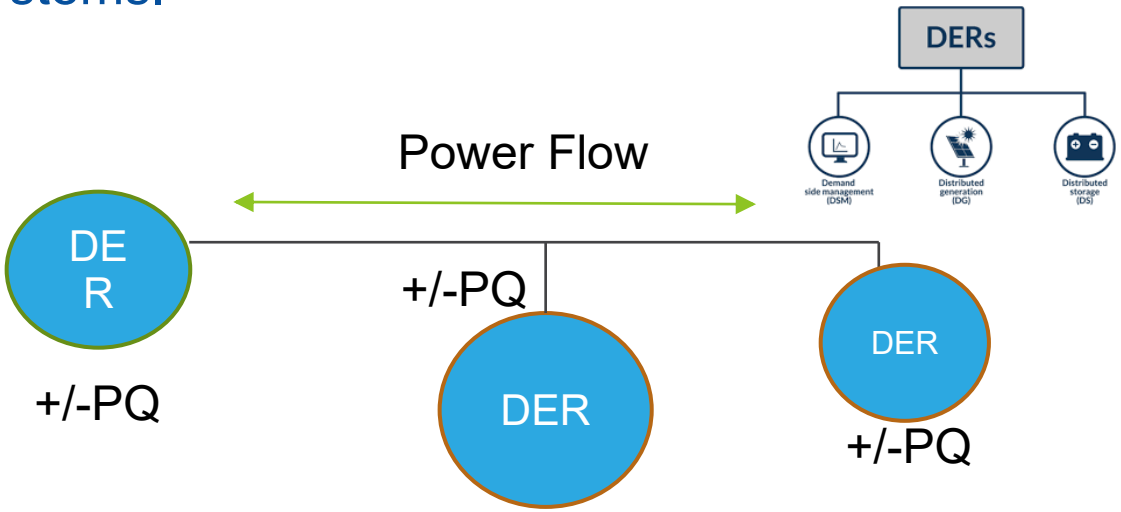




Background to the distributed energy resource (DER) concept

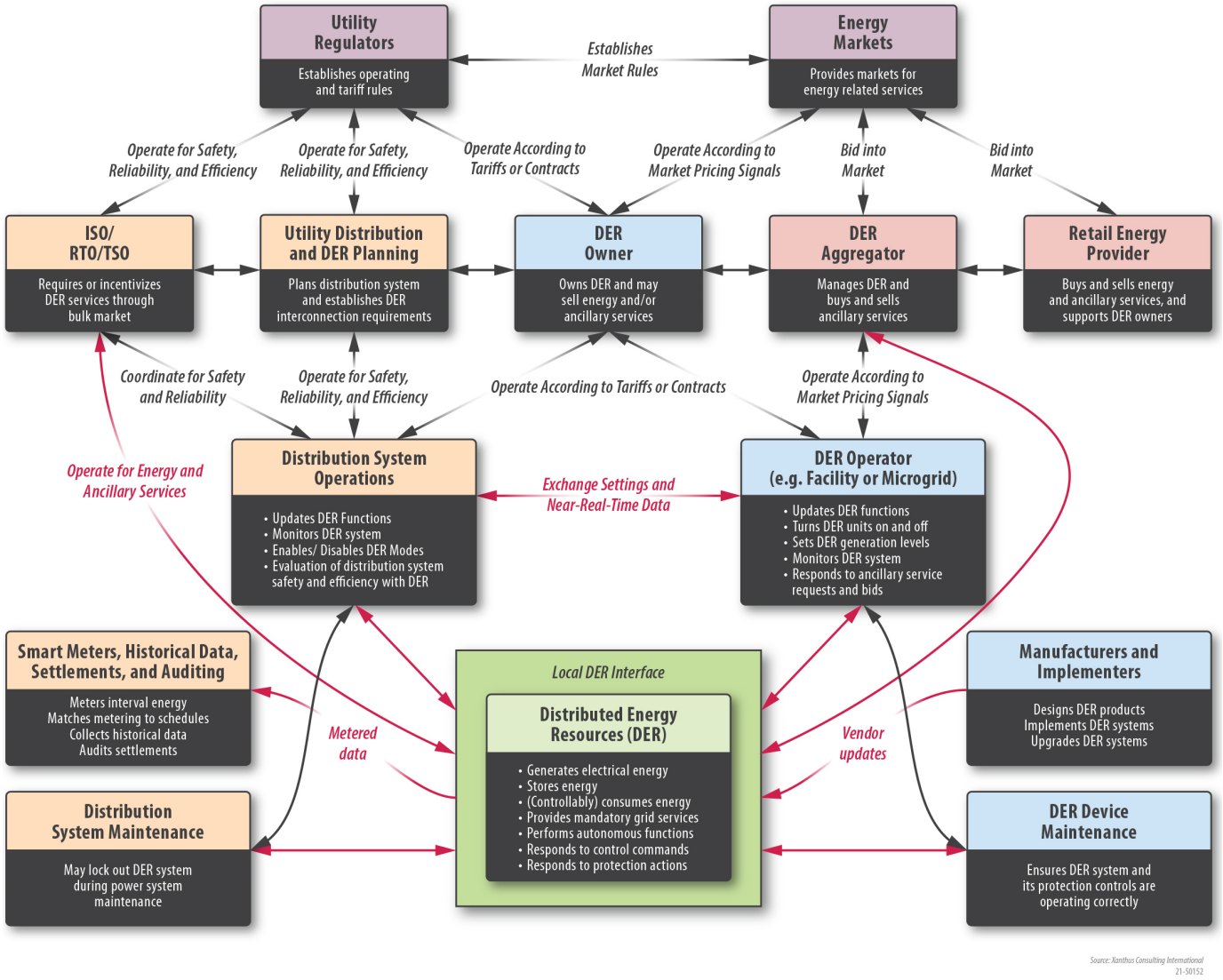
- Historically the utility was the owner and seller of electrical generation. The consumer (industrial, commercial, residential) purchased the electrical energy to service their electrical loads The utility built large scale electrical generation remotely for economies of scale and connected to loads via distribution systems.





- Distributed energy resources (DERs) a term that has evolved from the introduction of a smaller generation resources that have been integrated at different voltage and power levels to the larger grid ultimately not the traditional large scale remote generation. Frequently DER is used as a term to identify onsite or local generation, but also controllable loads.

DER Stakeholders

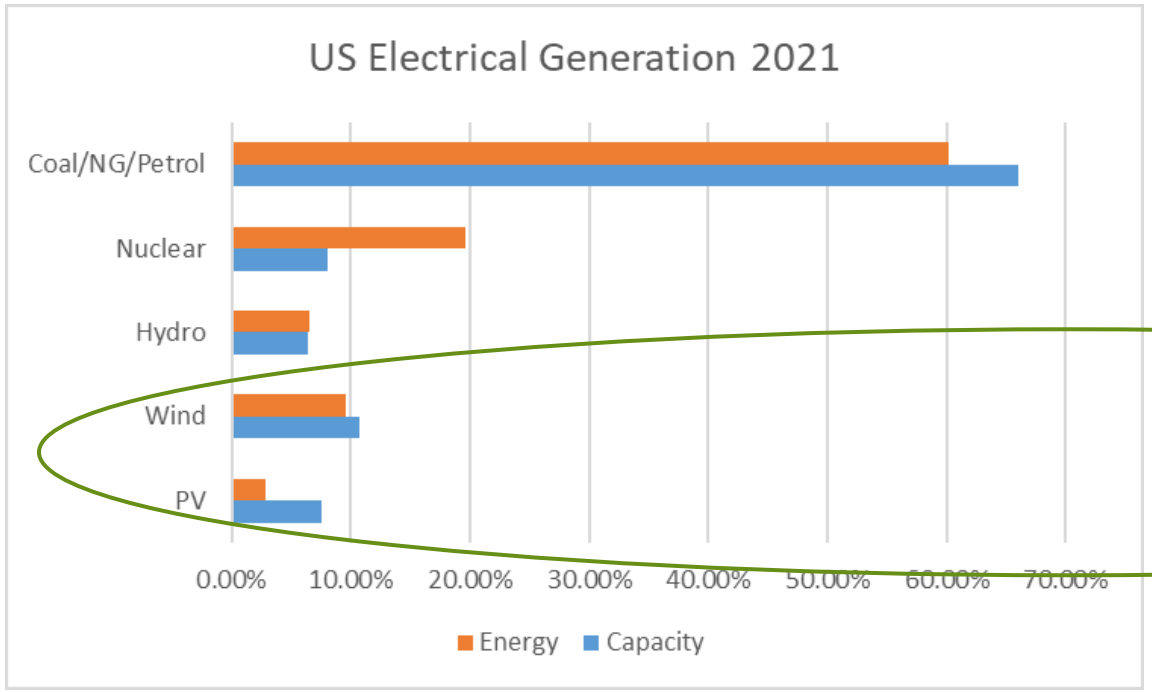


Market stakeholders
Utility stakeholders
Aggregator stakeholders
Facility stakeholders
DER systems

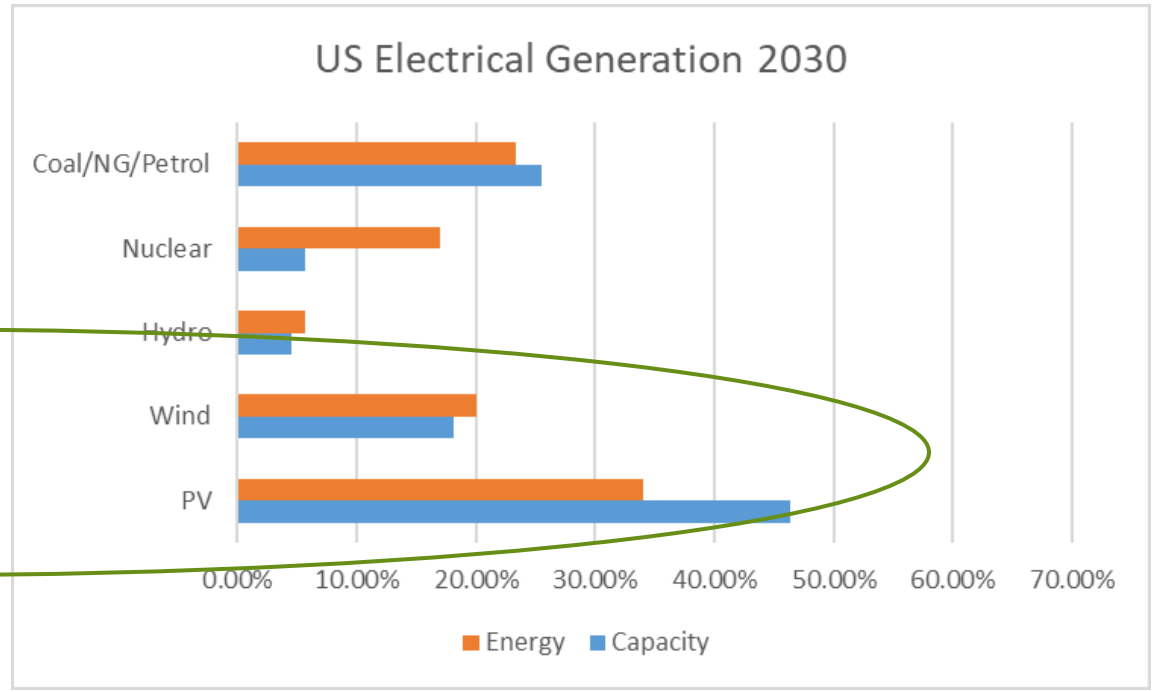
Generic Interactions between Stakeholders
Logical Interfaces of Stakeholders with DER

2021 to 2030* Capacity and Energy Production

EIA Energy and Capacity



SETO and WETO Goals



* WETO 2030 Goals and Curve Fitting to SETO 2035 Goals, with Estimated 26 million EV's sold in 2030

EIA Data 2021

Installed Electrical Generation Capacity

- Renewable (24.69%)
  - Solar (7.5%)
  - Wind (10.75%)
  - Hydro (6.44%)
- Nuclear (8.05%)
- Coal, NG, Petro (66.03%)
- Other (1.23%)

Electrical Energy Production

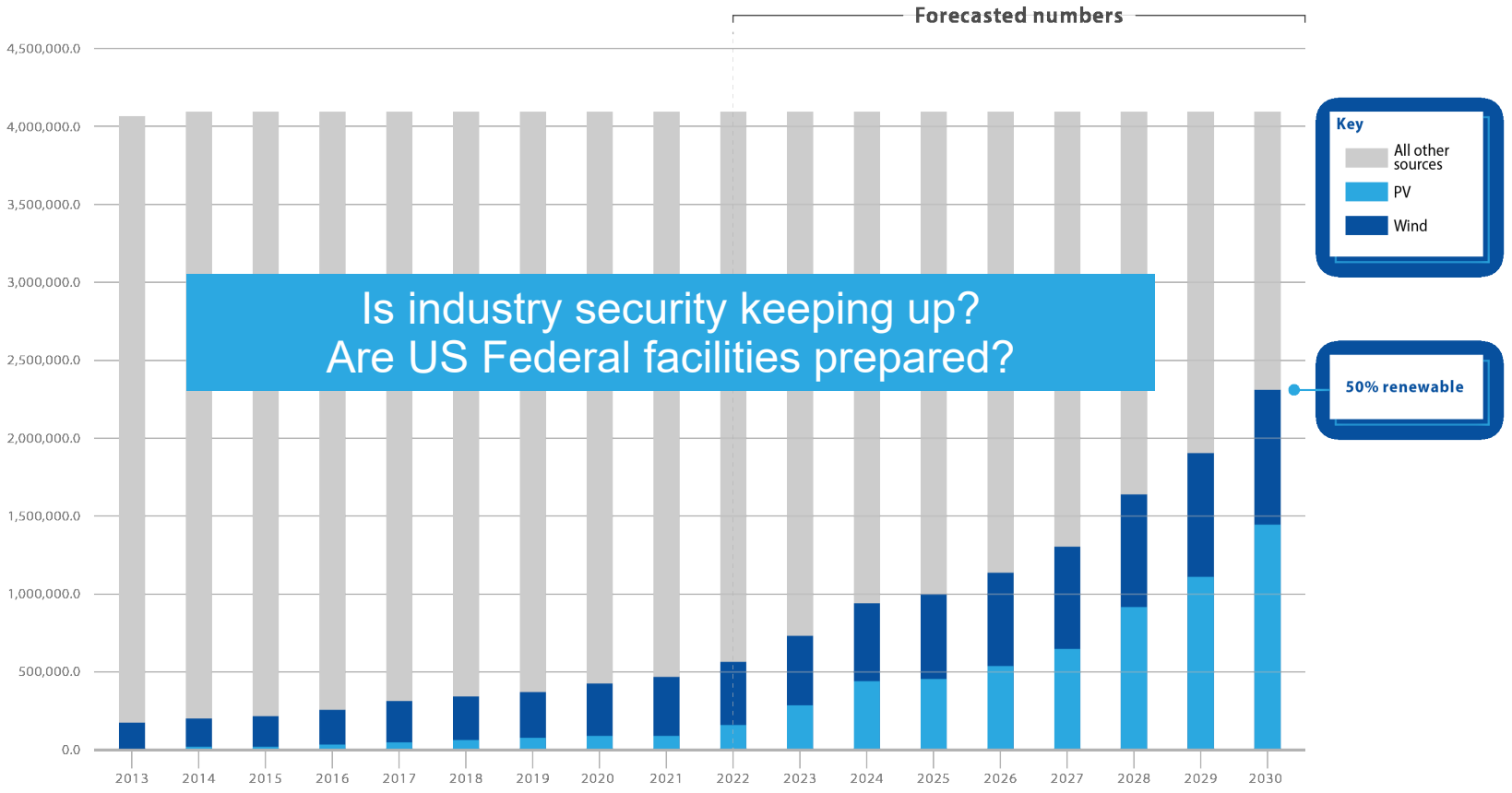
- Renewable (18.96%)
  - Solar (2.87%)
  - Wind (9.55%)
  - Hydro (6.54%)
- Nuclear (19.64%)
- Coal, NG, Petrol (60.17%)
- Other (1.23%)

From Here to There

- Solar 1000 GW installed
- 2035 – 4900 B-kWh (22.5% increase) (6-8% EV's)
- 35% Solar = 1560 B-kWh
- 20% Energy Wind Goal 2030 (920 B-kWh)
- 2030 – 1150 GW PV installed
- Average Plant size 12-20 MW
- 43k to 57k plants installed by 2030 (5.2k today or 8 to 10 times number of plants)
- 3k to 4k wind plants at 2030

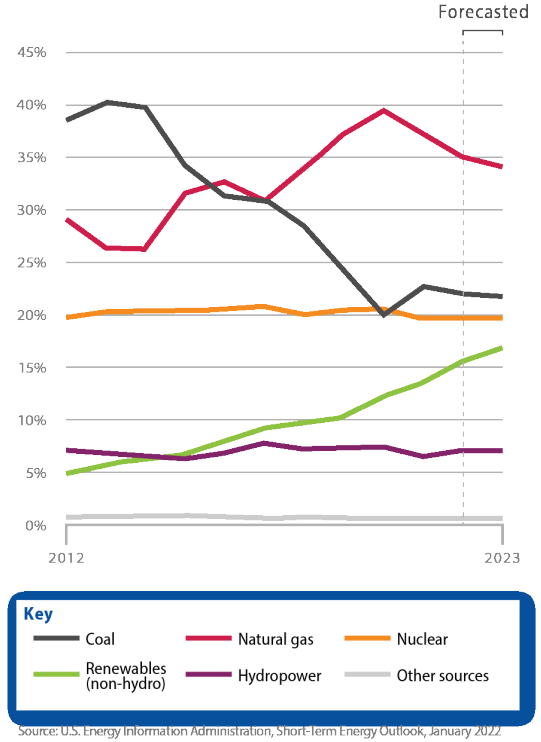
To achieve high renewable energy targets of 50% by 2030, current trends will need to grow at a much higher rate.

US Total Electrical Energy (1000's MWh)



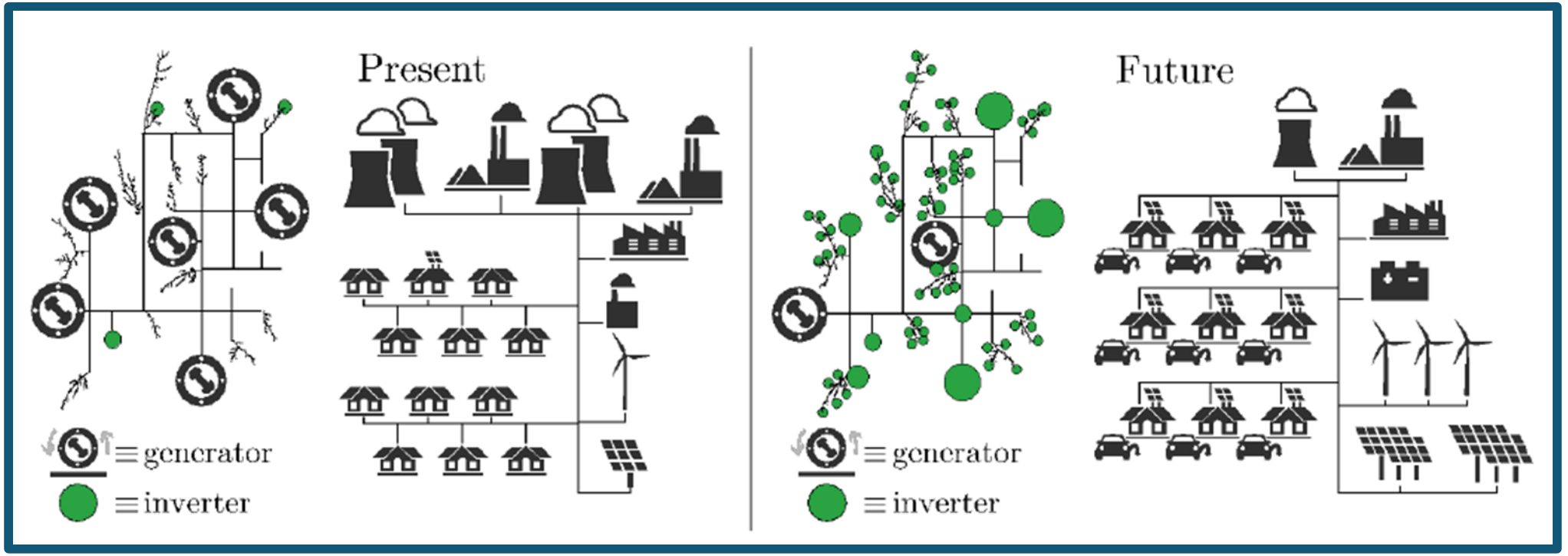
Is industry security keeping up?
Are US Federal facilities prepared?

Annual US electric power sector generation by energy source



Source: U.S. Energy Information Administration, Short-Term Energy Outlook, January 2022

Transitioning to a Hybrid then…..

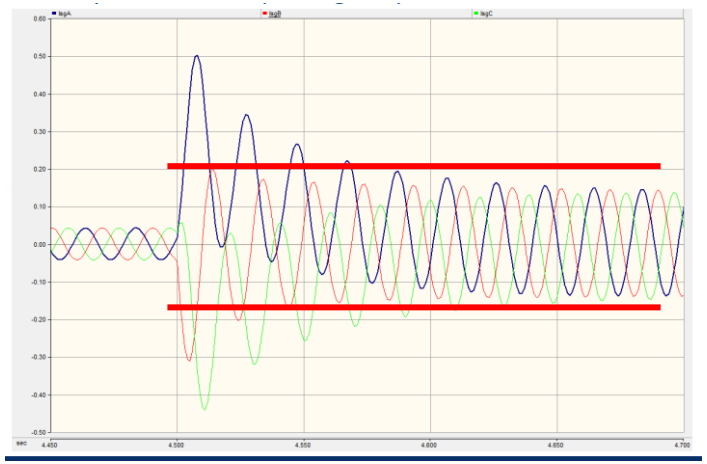


Remote, Large Scale
Thermal Systems
Nuclear, Coal, NG, Oil
Load Centers
Rotating Loads

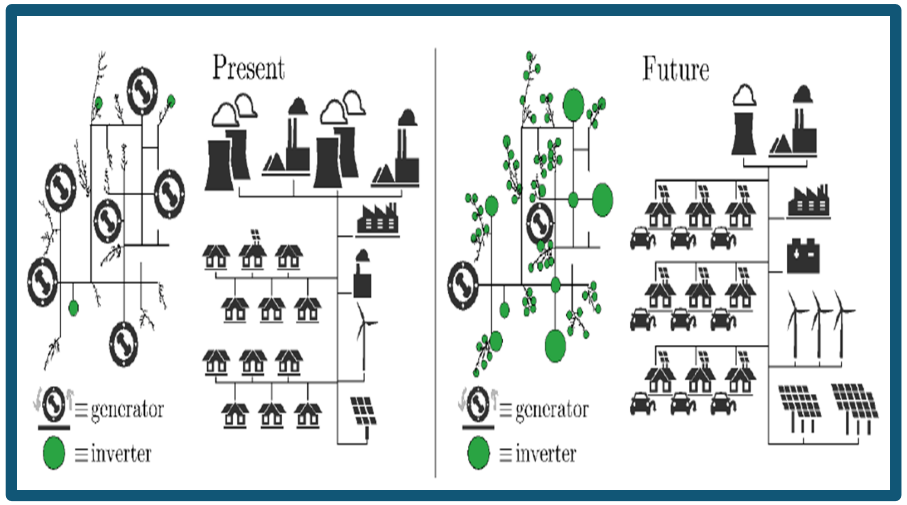
Distributed at many scales
Mostly Inverter Based
Renewable
Variable
Electrical Energy Storage
Smart Load
Bi-directional

Transition to a Carbon Free and renewable Grid:

Grid or Power Systems operations today are based upon solution and methodologies tied the physics and electrical characteristics of synchronous generators, as we transition to a carbon free renewable grid, the physics and electrical characteristics of Inverter Based Resource (IBR) are not the same as synchronous generators, ultimately eroding effectiveness of existing methodologies.

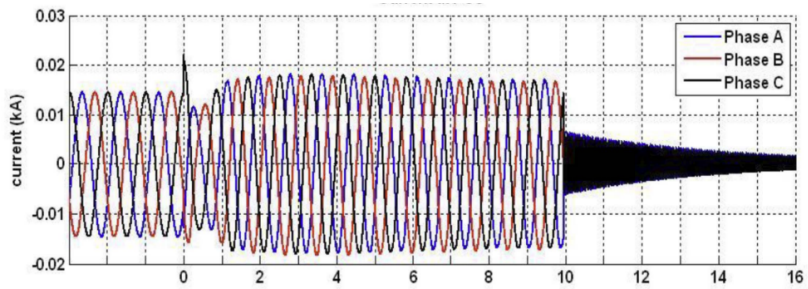


Fault current contribution by generators can be 6 to 10x



Challenge

Opportunity



Generic Model:

- Operate for 4 to 10 cycles after a fault incident even if the PCC voltage drops below 50%.
- The current is usually between 100% and 120% of the rated power of the inverter.
- The current contribution level is a function of the voltage at the terminal of the PV inverter (PCC) during a fault and thereby the type and location of the fault.

Fault current contribution by generators can be 1 to 1.2x

Sensing local and Act local
– today's protective relaying

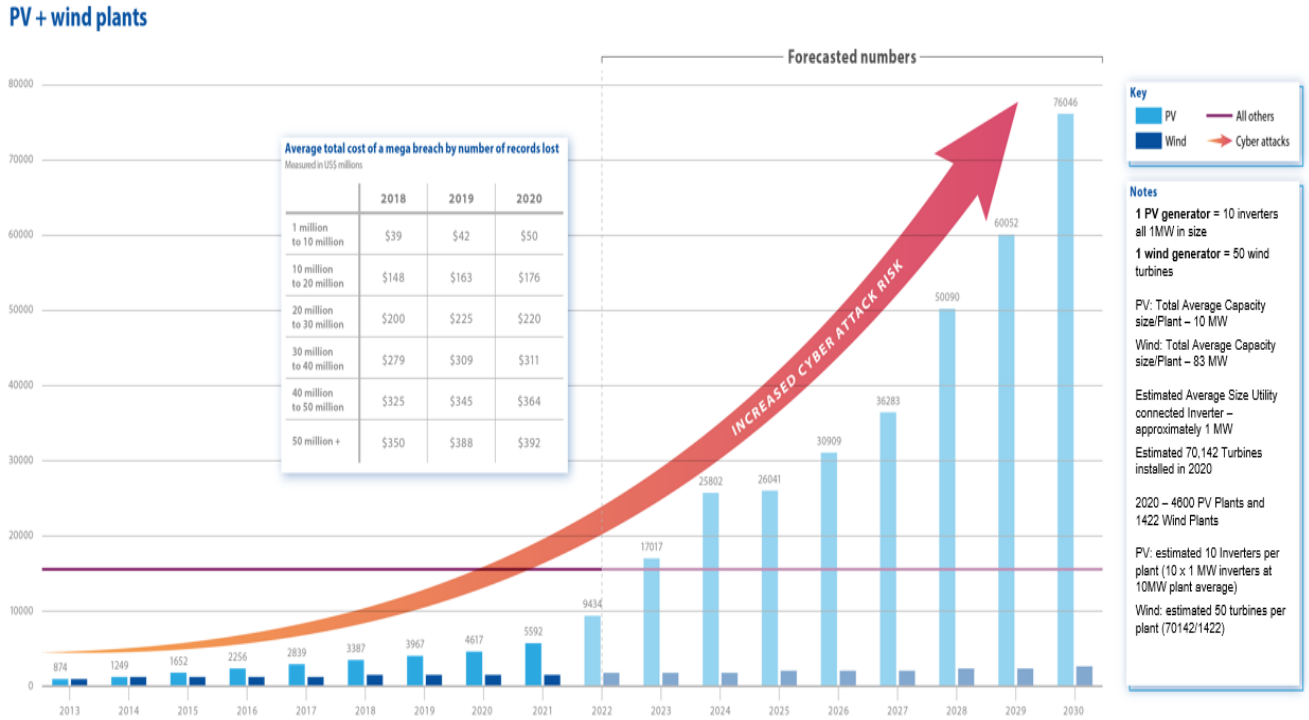
Sensing Everywhere and Act local
– tomorrow's protective relaying

The number of generator plants will increase +400%, significantly increasing the potential cyber attack space

Operational and Reliability Risk Priorities

- Operational and Cybersecurity Resilience
- Cybersecurity Threat and Risk Mitigation

The rapid and frequent evolution of technology and the cyber threat landscape brings urgency to the importance of maturing security within the renewable sector to support effective transition.



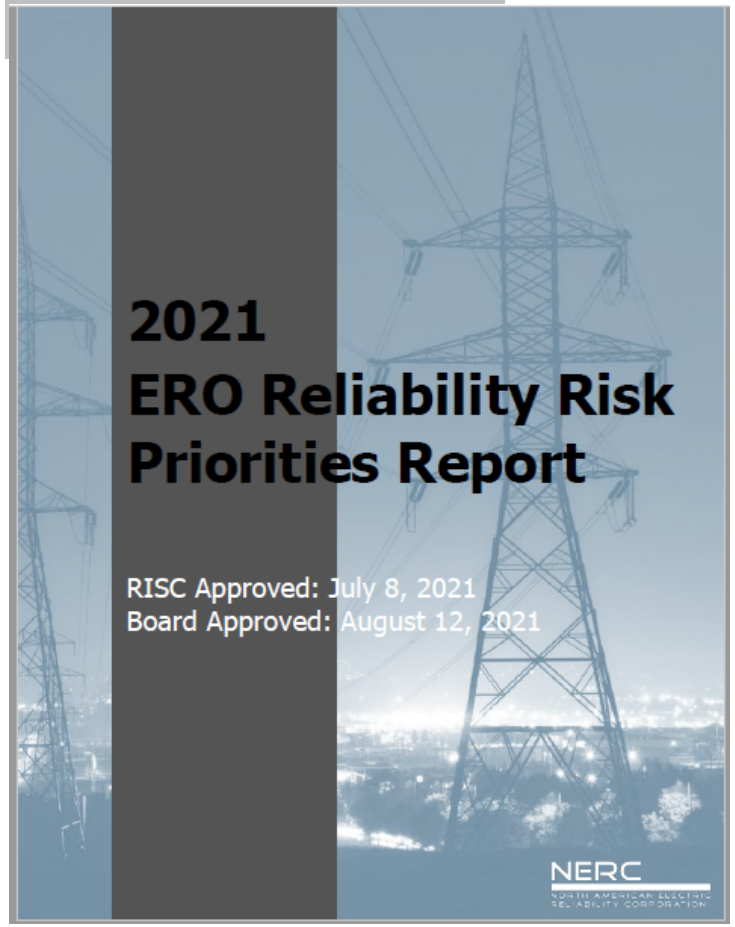
Future of DER

Changes in DER		Impact to cybersecurity
• Growth of stakeholders	→	• Increase in attack surface
• Growth of endpoints	→	• Increase in attack surface, vulnerabilities
• Electrification of loads	→	• Increase in potential impact
• Aggregation of DER	→	• Increase in potential impact
• Increasing regulation	→	• Standards more widespread
• Digitization of monitoring	→	• Explosion of data to process and store
• Digitization of control	→	• Need for resilience of critical functionality
• Distribution of control	→	• Management of roles and privileges
• Smarter inverters	→	• Increase in attack surface

Risk for the Grid

Changing Resource Mix and Cybersecurity are the highest Ranked Risks

NERC Reliability - Risk



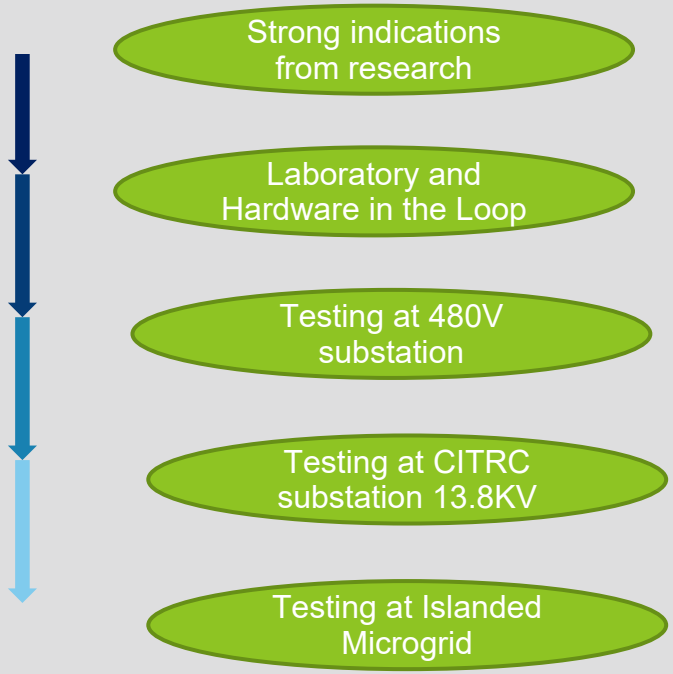
Securing the Path to Net Zero™

- Securing the Path to Net Zero™ is about identifying and solving the challenges in both technology integration and cybersecurity to achieve in paradigm.
- **Technology Integration** – Implication to utilities and grid by moving from synchronous generators to inverter-based generation
  - Data EIA vs Everyone else – ground truth LBNL DB?
  - Transmission interconnection (Energy Costs?) Motivation for large?
    - IRA and IIJA
  - Modeling
  - Protection

- **Cybersecurity** - Security through Hardware Installation, Education, and Layered Defense (SHIELD)

INL's Full capability
Concept – Lab – Field – At Scale

OE Lab Call –
Alternative Grid Operations

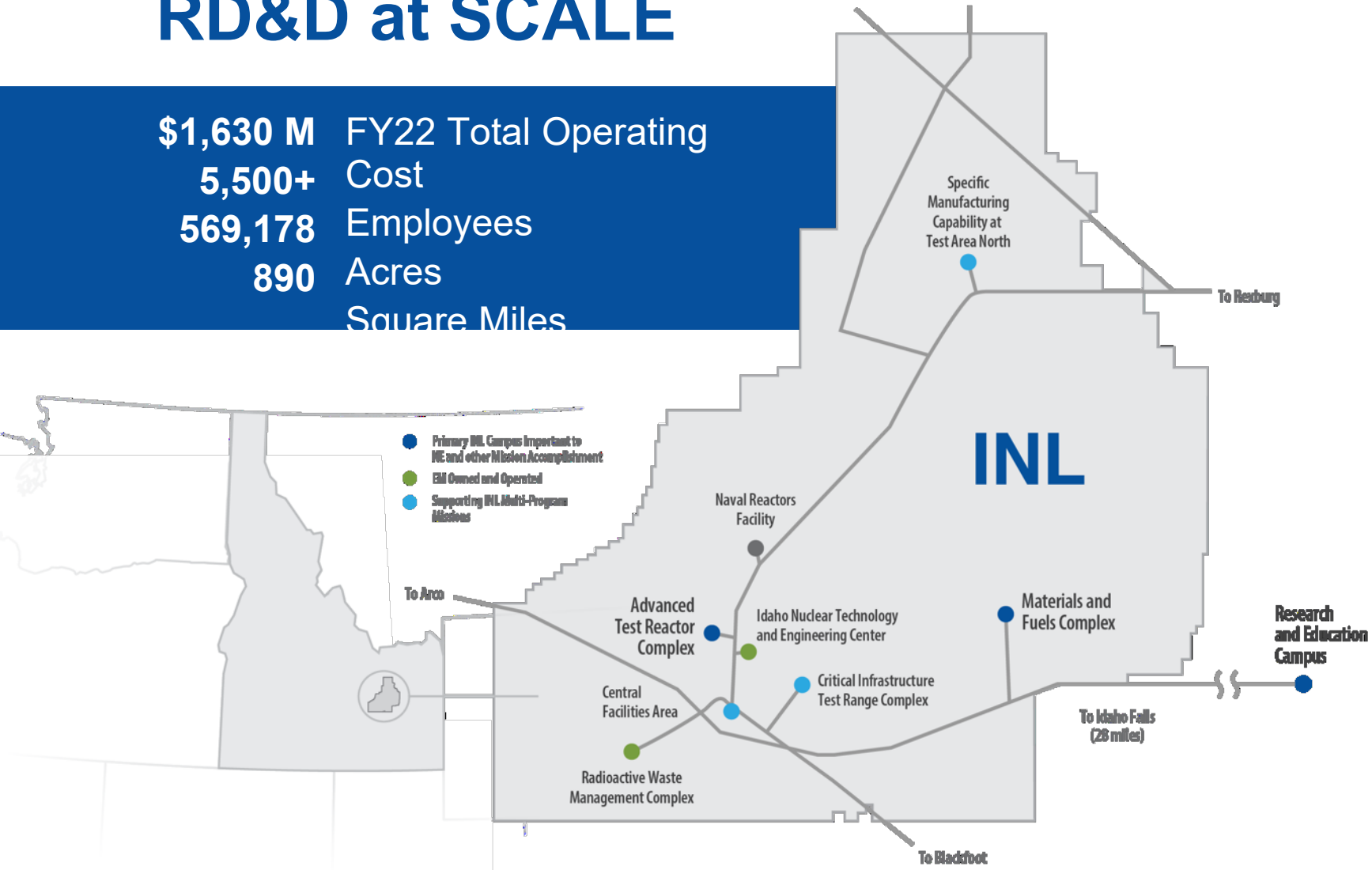


How INL is tackling these challenges through a concept-to-at-scale approach

- Area of Interest: Convergence of Technologies
  - Concept, Laboratory, Demonstration, AT SCALE
- Securing the Path to Net Zero
  - Technology and implications
  - Cybersecurity

Unique INL site, infrastructure, and facilities enable energy and security RD&D at SCALE

$1,630 M	FY22 Total Operating Cost
5,500+	Employees
569,178	Acres
890	Square Miles



4	Operating reactors
12	Hazard Category II & III non-reactor facilities/ activities
50	Radiological facilities/activities
17.	Miles railroad for shipping nuclear fuel
5 44	Miles primary roads (125 miles total)
9	Substations with interfaces to two power providers
12	Miles high-voltage transmission lines
6 3	Fire Stations

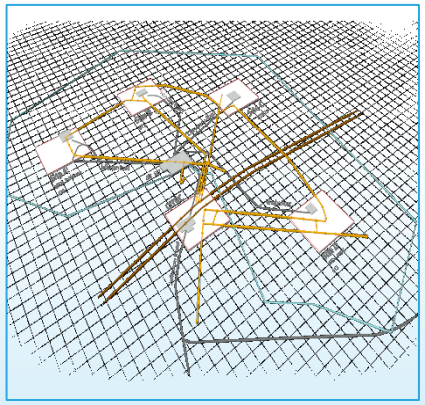
Electric Grid Test Range - Investments

Maintenance & Repair

- Reinvigorating aging infrastructure to enable a modern and scientifically instrumented grid configuration
- $23M from NE

2017

Project - Distribution



- Enabling realistic distribution technology V&V on a modern and instrumented grid; a.k.a. wagon wheel substation
- $9.8M from OE

2018

Project - Transmission

- Providing a reconfigurable transmission line for simultaneous testing of loads, generation and storage; redundant and offline
- $18.1M from OE

2019-2020

Mobile Distribution

- Mobile substation, mobile command center, mobile renewable generation and storage.
- $1.5M from OE

2021-2022

Since 2011, INL has executed over 100 tests for customers that included:

- DOE-Office of Electricity (OE)
- DOE-Energy Efficiency & Renewable Energy (EERE)
- DOE-Office of Intelligence (IN)
- Dept. of Defense
- Intelligence Community
- Vendors (manufacturers)

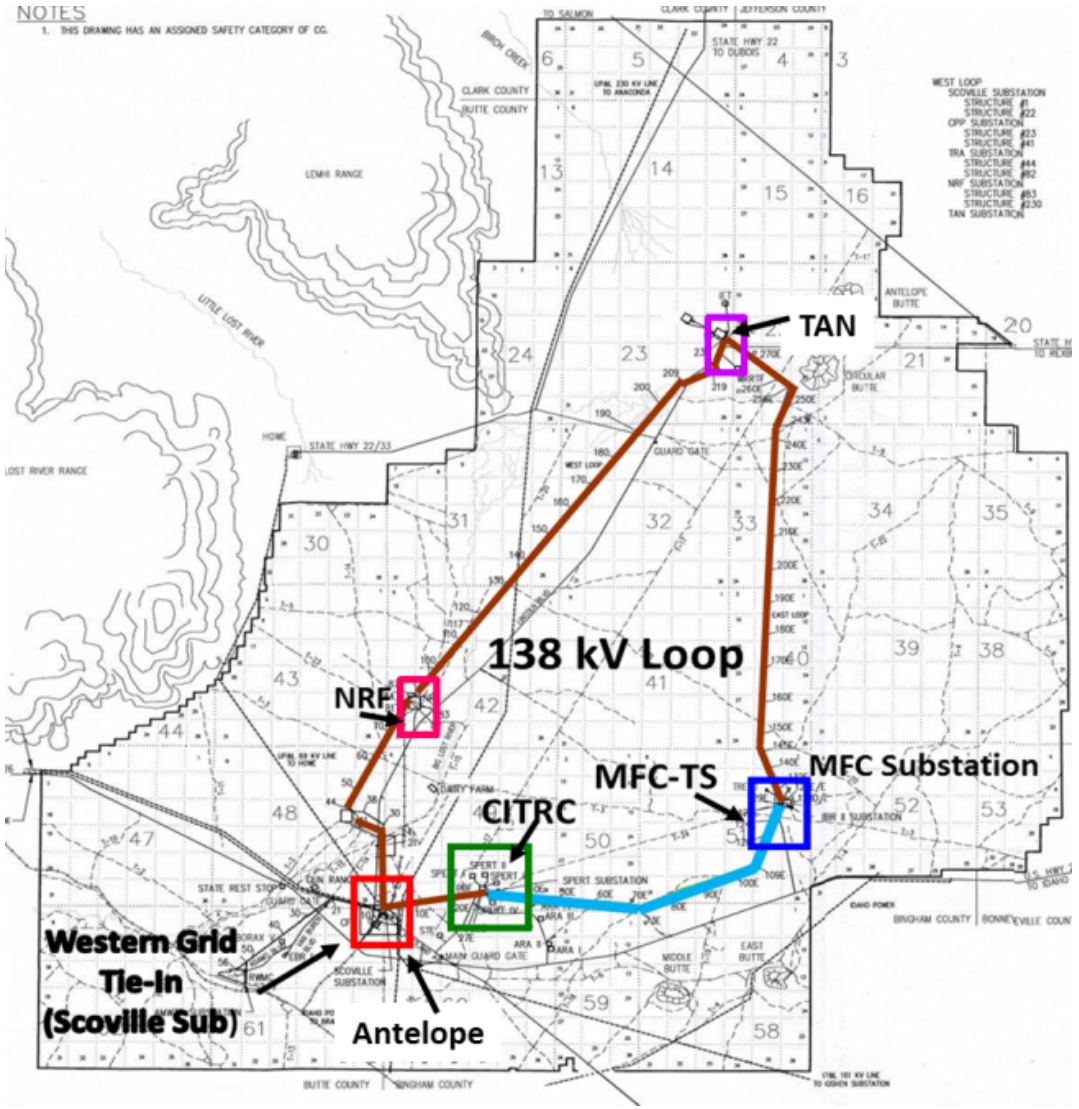
Electric Grid Test Range - Assets

Transmission – Scoville Power and Light (SPL)

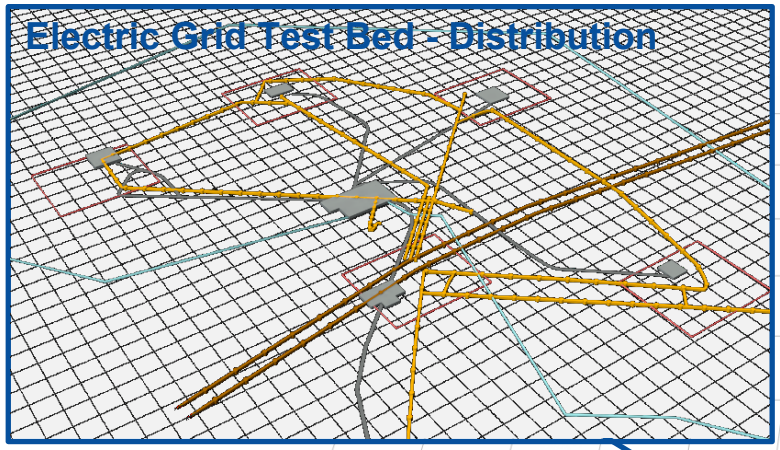
- INL owned and operated electric grid (24x7)
- 7 substations, 61 miles of 138 kV transmission line providing power for 890 square mile complex
- Full time staff; power and electrical engineers, planners
- Real-time grid monitoring and control through centralized SCADA operations center
- 3 commercial feeds at 161kV and 230kV
- Full range of environmental conditions

Distribution - Critical Infrastructure Test Range Complex (CITRC)

- Dedicated R&D substation within SPL
- Flexible distribution pads use existing equipment or customer supplied
- Power for monitoring, controlling, measuring separate from system under test
- Integrated fiber, cellular and other communications technologies
- Remote access to operations and assets under test via multiple communications mediums (including fiber connectivity)
- Ability to execute testing in isolated or configurations or integrated with SPL
- Expert staff in multi-disciplined domains



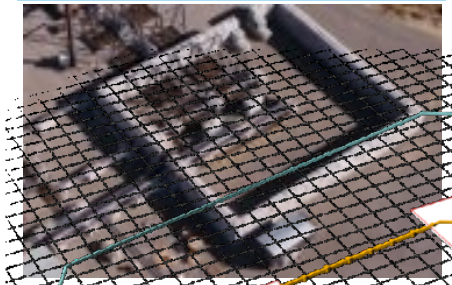
INL Site and the Electric Grid



Electric Grid Test Bed - Transmission
13-miles of transmission line between CITRC and MFC range can be isolated and is most used for testing.

Electric Grid Test Bed - Capabilities

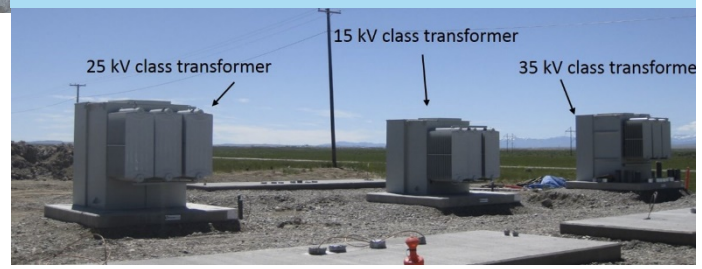
Configurable Mock Substation



Offline and Isolated Transmission

Dedicated R&D Substation

15/25/35kiloVolt Class Distribution Support



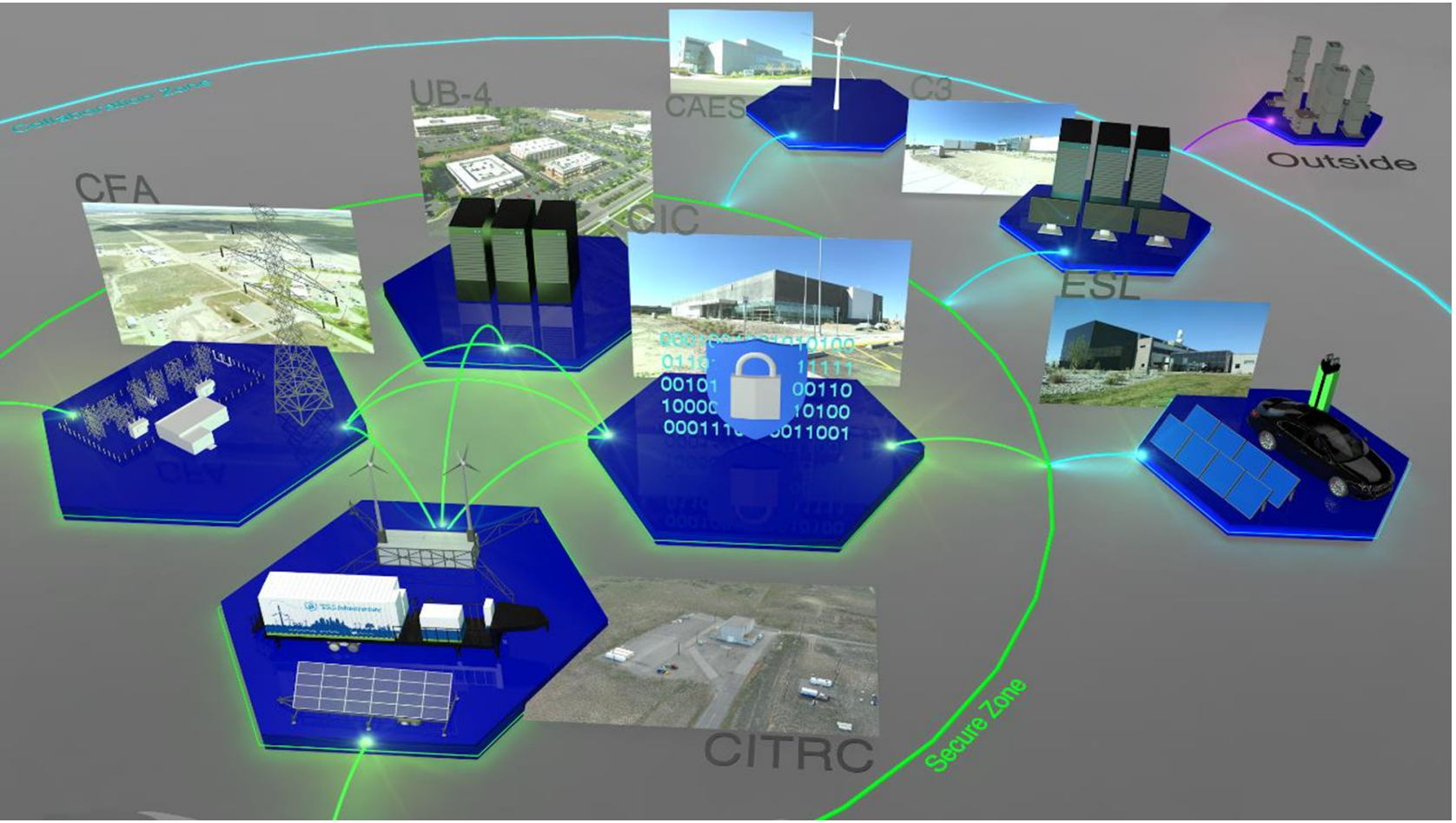
Mobile Command Center, PV Super Array, and Wind Turbines

Testing Distribution and Transmission

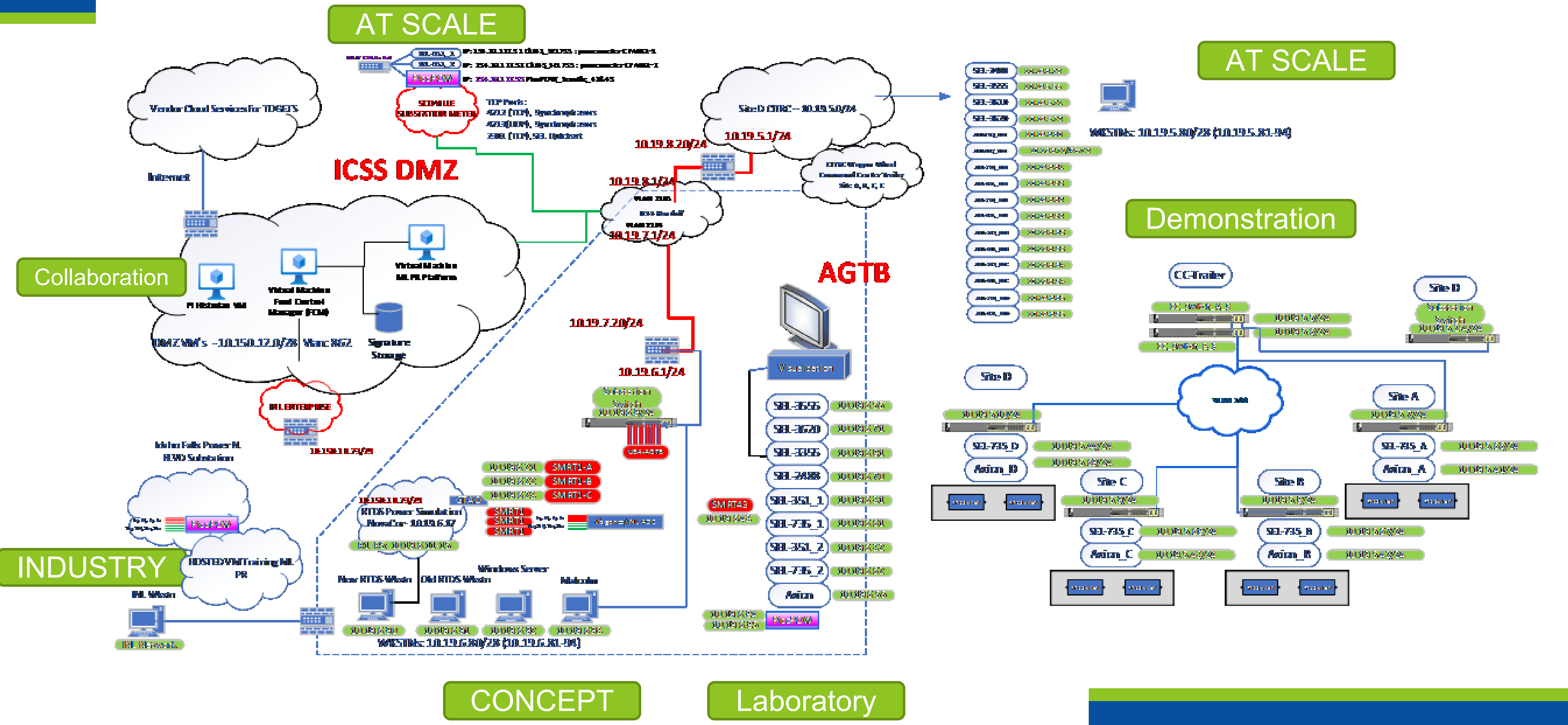
- Validate and demonstrate the effects of threats including Geo-Magnetic Disturbances (GMD) testing.
- Investigate and demonstrate the effects of certain classes of cyber exploits on critical grid operations.
- Protective relay security methodologies and product development.
- Control system cybersecurity analysis, validation and fault injection, test to fail, etc.
- Power quality and phenomenology studies associated with new equipment and system operations.
- Transmission line ice load testing.
- Interoperability (migration to new technologies).
- Risk reduction to production systems.
- Sensitive grid project work with numerous federal and state entities.
- Protection and restoration process and technologies.

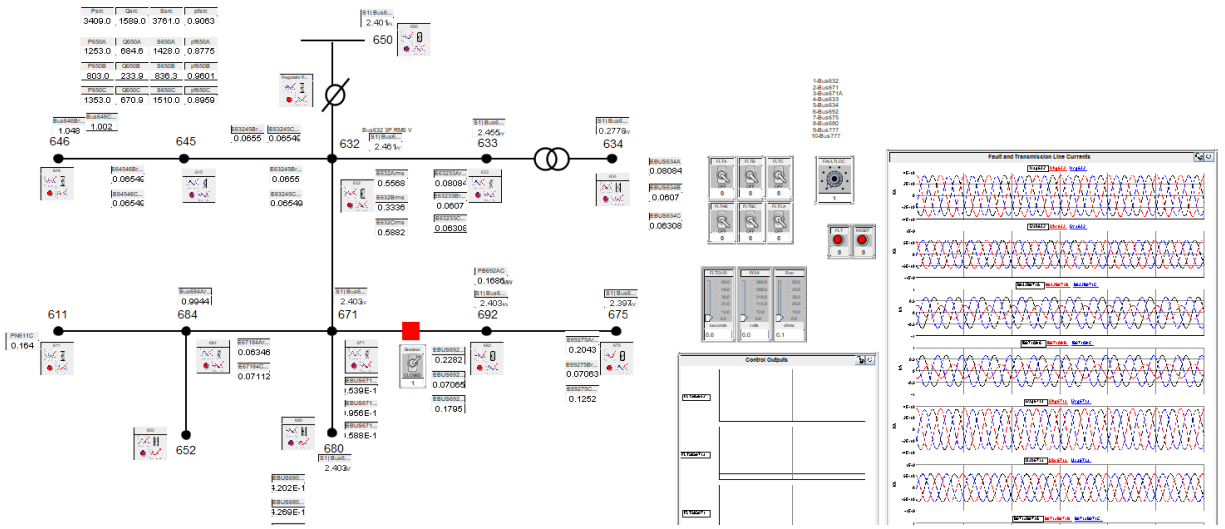
Using INL's Own CITRC Microgrid Capability

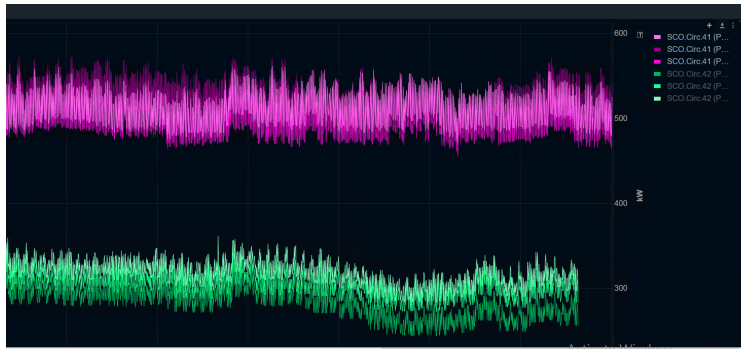
Concept ⟹ Scale; Leveraging Capabilities



- INL is continuing to develop Concept to SCALE in research surrounding the grid of the future.
- Data Networks connected from Industry, Laboratory, to Scale
- Replicating at all levels for testing and investigation
- Utility and industry Owners rarely want to invest time and assets to projects that were built to delivery energy and make money.
- INL has capability at Utility, Industry, Commercial, and Residential level for research into securing the path to net-zero.


AT SCALE
Vendor Cloud Services for TDGETS
Internet
ICSS DMZ
Collaboration
PI Historian VM
Virtual Machine
Signature Storage
DMZ VM's – 10.150.12.0/28 | Vlan: 862
INL ENTERPRISE
Site D CITRC – 10.19.5.0/24
10.19.5.1/24
10.19.8.20/24
10.19.8.1/24
10.19.7.1/24
10.19.7.20/24
10.19.6.1/24
AGTB
Visualization
SEL-3555
SEL-3620
SEL-2488
SEL-351_1
SEL-735_1
SEL-351_2
SEL-735_2
Axion
SMRT1-A
SMRT1-B
SMRT1-C
RTDS Power Simulation
Idaho Falls Power NL BLVD Substation
HOSTED VM Training ML PR
INDUSTRY
INL Wksta
INL Network
New RTDS Wksta
Old RTDS Wksta
Windows Server
Malcolm
WKSTNs: 10.19.6.80/28 (10.19.6.81-94)
AT SCALE
WKSTNs: 10.19.5.80/28 (10.19.5.81-94)
Demonstration
CC-Trailer
Site D
Site A
Site B
Site C
SEL-735_D
Axion_D
SEL-735_A
Axion_A
SEL-735_C
Axion_C
SEL-735_B
Axion_B
CONCEPT
Laboratory





RMS Voltage A:2449.87 B:2527.33 C:2444.84

CT Ratio: 6132 PT Ratio: 934.093

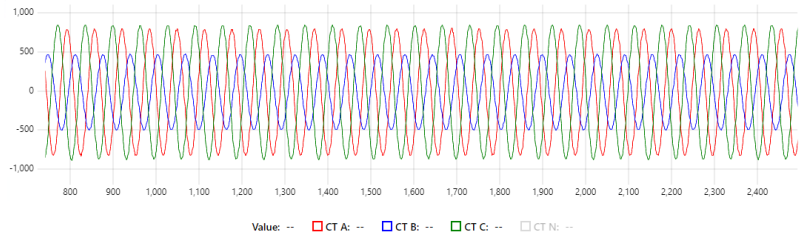
SPS: 3840 SPP: 32

AGTB Lab PPOW

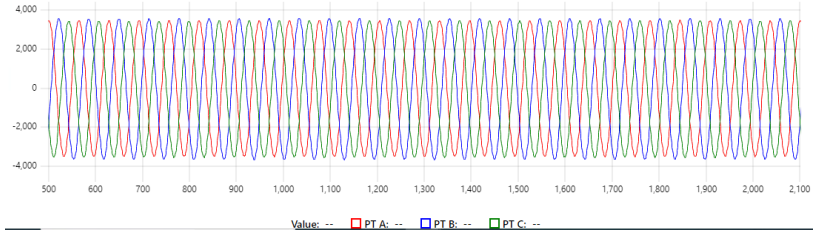
Start Stop

Messages: 9600

Current

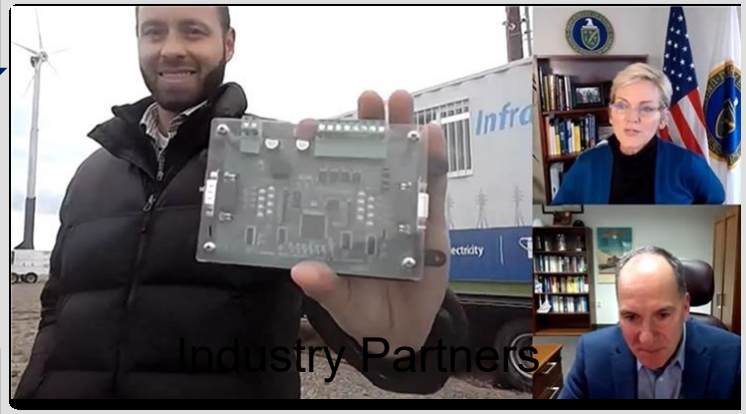


Voltage



INL's Full capability

Concept – Lab – Field – At Scale



CRADA

C3DV2

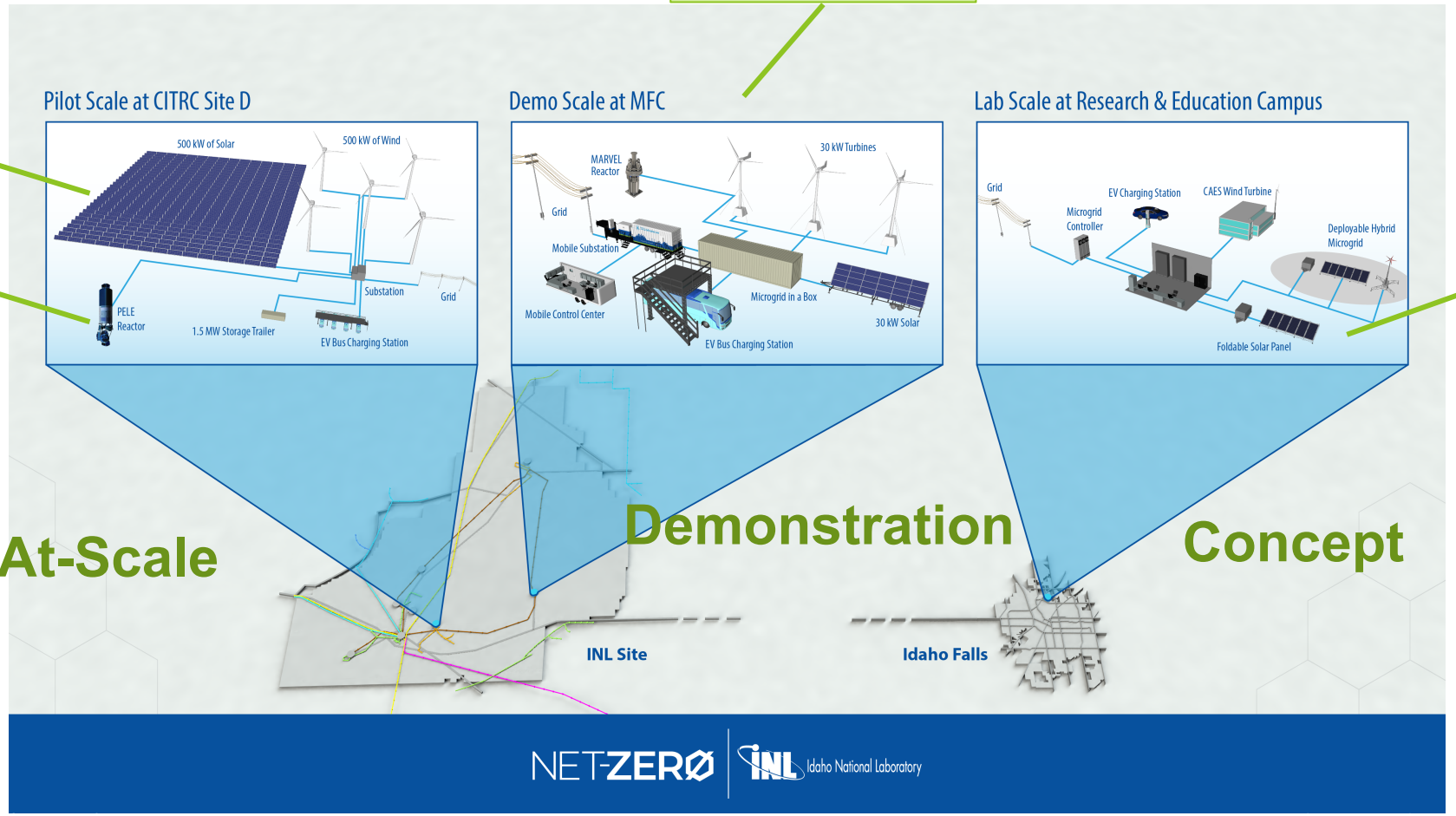
Net Zero Laboratory (NZL) Initiative

30 kW solar

500 kW solar

1MW SMR

20 kW foldable solar



Advanced Grid Test Bed : Capability

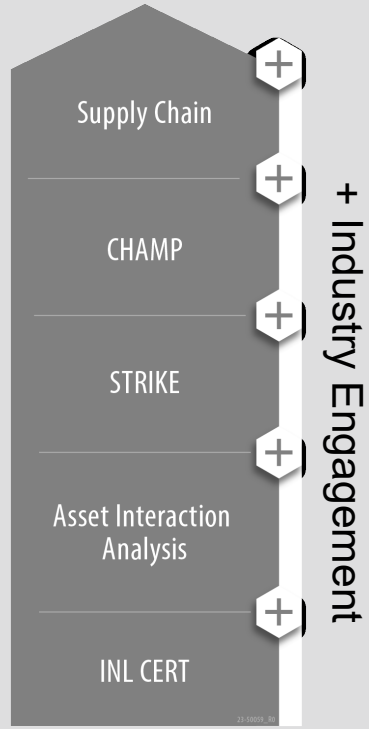
- Single device testing to integrated environments
- Simulation and Hardware in the loop
  - Example for ML PR
- Individual Inverter testing – Chroma Regenerative System and Variable DC source
- New levels of capability for collaboration for INL and Industry partners
  - DOE level issue for cybersecurity requirements
- Mobile Substation at 480V for easy of integration for commercial and industrial levels
- CITRC – Variable distribution voltages and scaling capability
- At Scale with transmission and multiple distribution substations

INL Programs

INL - Cyber SHIELD

***S**ecurity through **H**ardware **I**ntegration, **E**ducation, and **L**ayered **D**efense*

Raising the Floor on Cybersecurity for grid scale renewables



CERT Evaluation

1st

INL CERT- Tuned Assessment

CERT Evaluation

INL CERT -- Architectural Basics

3rd

2nd

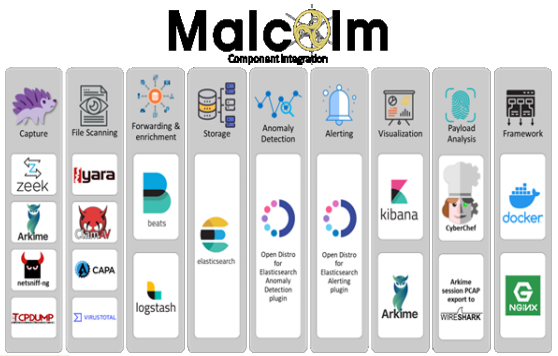
INL CERT- Tuned Assessment

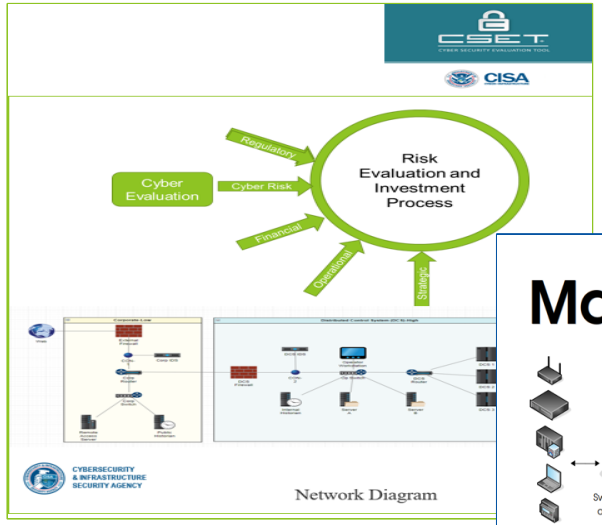
ndustry Resources

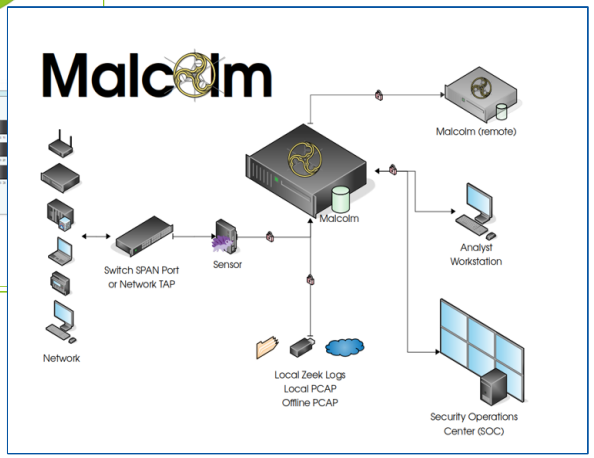
Cyber SHIELD Overview: Program Tools & Objectives

In order to support the “raise the floor” objectives, the initial focus has been deployment of three initiatives:

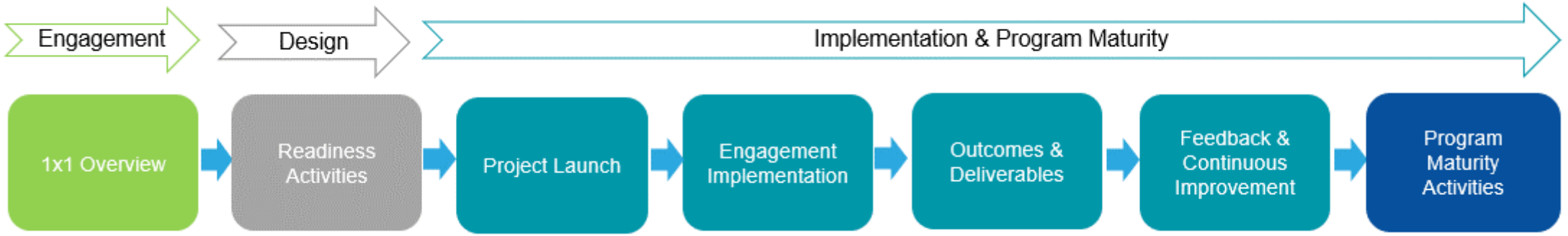
- INL Malcolm-AIA – ***Asset Interaction Analysis:*** Links assets to business processes and translates the business processes to OT devices. Supports deeper threat and vulnerability identification/analysis for user.
- INL Cyber CERT – ***Program Assessment:*** Provides entities access to a cybersecurity assessment of basic programs and capabilities along with risk-based recommendations for improving their maturity.
- INL Cyber CERT – ***Architecture Basics:*** Allows entities to plot network design and identify basic vulnerabilities in current state.







Next Steps



Looking for industry participants to get involved and leverage these resources to improve their cybersecurity maturity.

Designed to minimize level of effort from your teams (understand resources are often thin).

Partner information protection and confidentiality considerations have been integrated.

Outcomes and deliverables focused on identifying risk, mitigation activities, and prioritization.

Next Steps: Readiness

1) Partner Maturity Model
2) Partner Site Survey Questionnaire
3) Partner NDA
4) Partner SOP document for Network interaction

To discuss more or to sign up contact:

Stephen A. Bukowski at Idaho National Laboratory | stephen.bukowski@inl.gov

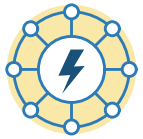
National Lab Cyber-Physical Capabilities

Current Programs and Tools

Cyber-Informed Engineering (CIE) - "engineer out" cyber risk throughout the design and operation lifecycle, rather than add cybersecurity controls later

Cybersecurity for the Operational Technology Environment (CyOTE™) - asset owners improve identification of adversarial techniques within operational technology (OT) environments

CyTRICS™ - cyber vulnerability testing, forensics, and digital subcomponent enumeration



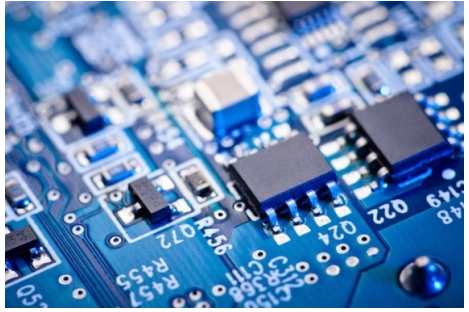
Improves cybersecurity supply chain for ICS

Uses expert testing

Identifies common-mode vulnerabilities

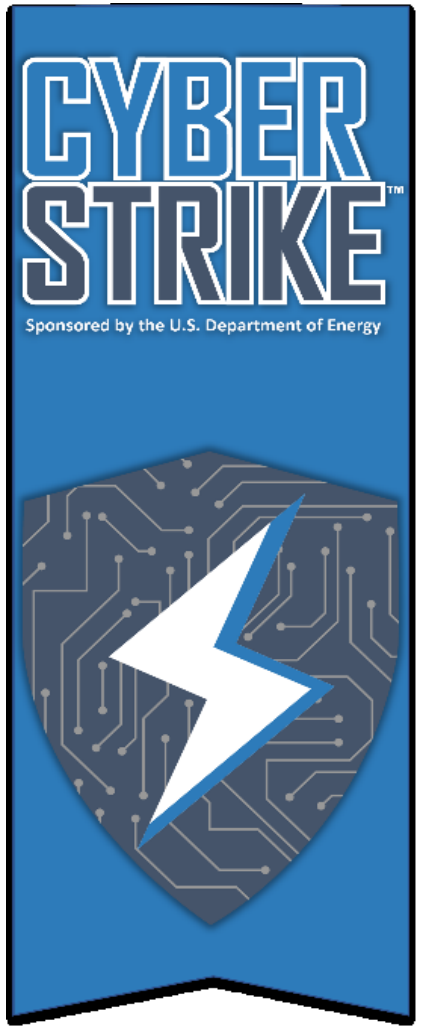
Partners with vendors and asset owners

Relationships & Continuing Engagement

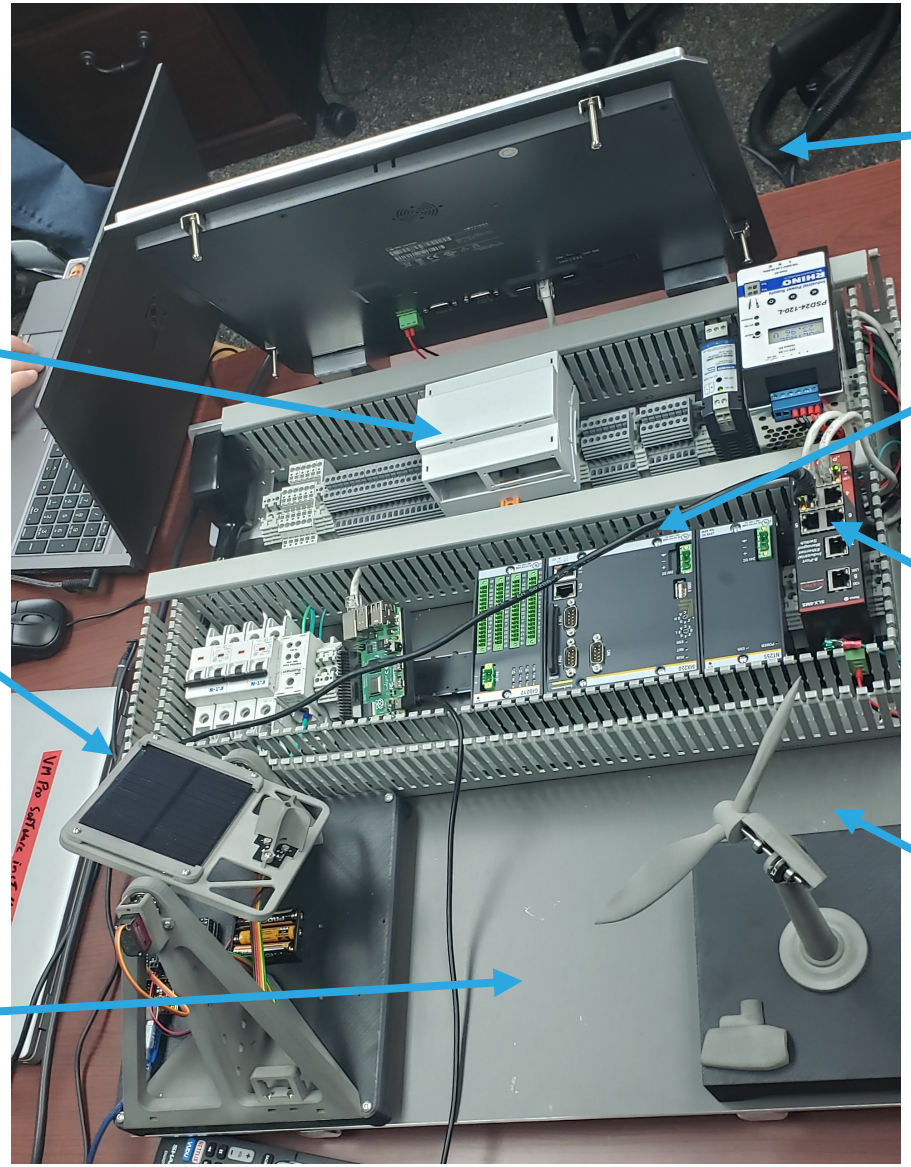


CyberStrike Storm Cloud

- The CyberStrike STORM CLOUD training workshop was designed to enhance the ability of renewable energy owners and operators to prepare for a cyber incident impacting industrial control systems with specific considerations of the architectures and limitations of renewable energy.
- This training offers participants a hands-on, simulated demonstration of relevant cyberattack vectors and training for key concepts for cybersecurity for renewable energy.



CyberStrike Storm Cloud Demo Kit



HMI

Solar “inverter” – Raspberry Pi emulator

Bachmann controller to be used for wind

Single-axis solar

Network switch for the DER system

Space for EV model

Open platform design to allow wind turbine to blow

Thank You