Wind Cyber Consortium and Pivot Discussion

Jonathan White and Danish Saleem
National Renewable Energy Laboratory

September 27, 2022

Where we started

Workshop Convenes Experts to Evaluate the Cybersecurity of U.S. Wind Farms

July 26, 2019

Earlier this month, NREL hosted a multi-stakeholder workshop to evaluate the growing potential for cybersecurity vulnerabilities on U.S. wind farms. The workshop, "Assessing the Impact of Cybersecurity on the Nation's Wind Farms," brought together the expertise of researchers across the national lab complex, the wind energy industry, original equipment manufacturers, cybersecurity product vendors, and standards organizations.

Representatives from the national lab complex, wind industry, manufacturers, cybersecurity product vendors, and standards organizations came together at NREL's Flatirons Campus for a workshop evaluating cybersecurity vulnerabilities on U.S. wind farms. *Photo by Josh Bauer/NREL*

NREL Joins Industry in Leading Cybersecurity Threat Evaluation for the U.S. Wind Fleet

April 29, 2021

The National Renewable Energy Laboratory (NREL) and six leading industry organizations have joined forces in developing a national Wind Cybersecurity Consortium. The goal of the consortium is to improve the cybersecurity of the U.S. wind fleet through collaborative analysis, development, and information sharing.

What we accomplished

- Established multi-party NDA with “big 3” OEMs and 3 wind owner-operator
- Developed TruSTAR database for wind threat IOC data gathering and anonymization (CESER)
- Performed proactive cyber risk evaluation, such as red team/MITRE ATT&CK analysis of wind turbine controller vulnerabilities (CESER + WETO)
- Hosted ½-day virtual wind workshop in March 2022 (WETO)
- Performed mapping & cataloging of wind controller software (CESER carry over)
  - Example: NREL-developed controls advanced research turbine (CART) controller and tailoring it to DOC/NTIA software bill of material (SBOM) process standards
- Developed wind plant/turbine reference architecture along with open-source cyber simulation model (WETO new)
- Supported SNL-led Wind Weasel intrusion detection system (WETO new)
- Hosted in-person workshop in September 2022 in Washington, D.C. (WETO carry over)

Wind Cyber Consortium Feedback

Include threats to hybrid energy plants (wind + solar + storage), as well as assessing threats to turbines and the legacy “wind-only” fleet, third party devices, and the introduction of malware from tech laptops.

Take a more holistic perspective of the energy producer and utility relationship.

Assess the challenges of securing distributed energy resource management systems.

Expand scope to other power systems devices such as plant controllers, SCADA, RTUs, etc.

Lead cyber workforce development and training.

To pivot or not?

Considerations for Reshaping the Wind Cybersecurity Consortium

Charge Questions

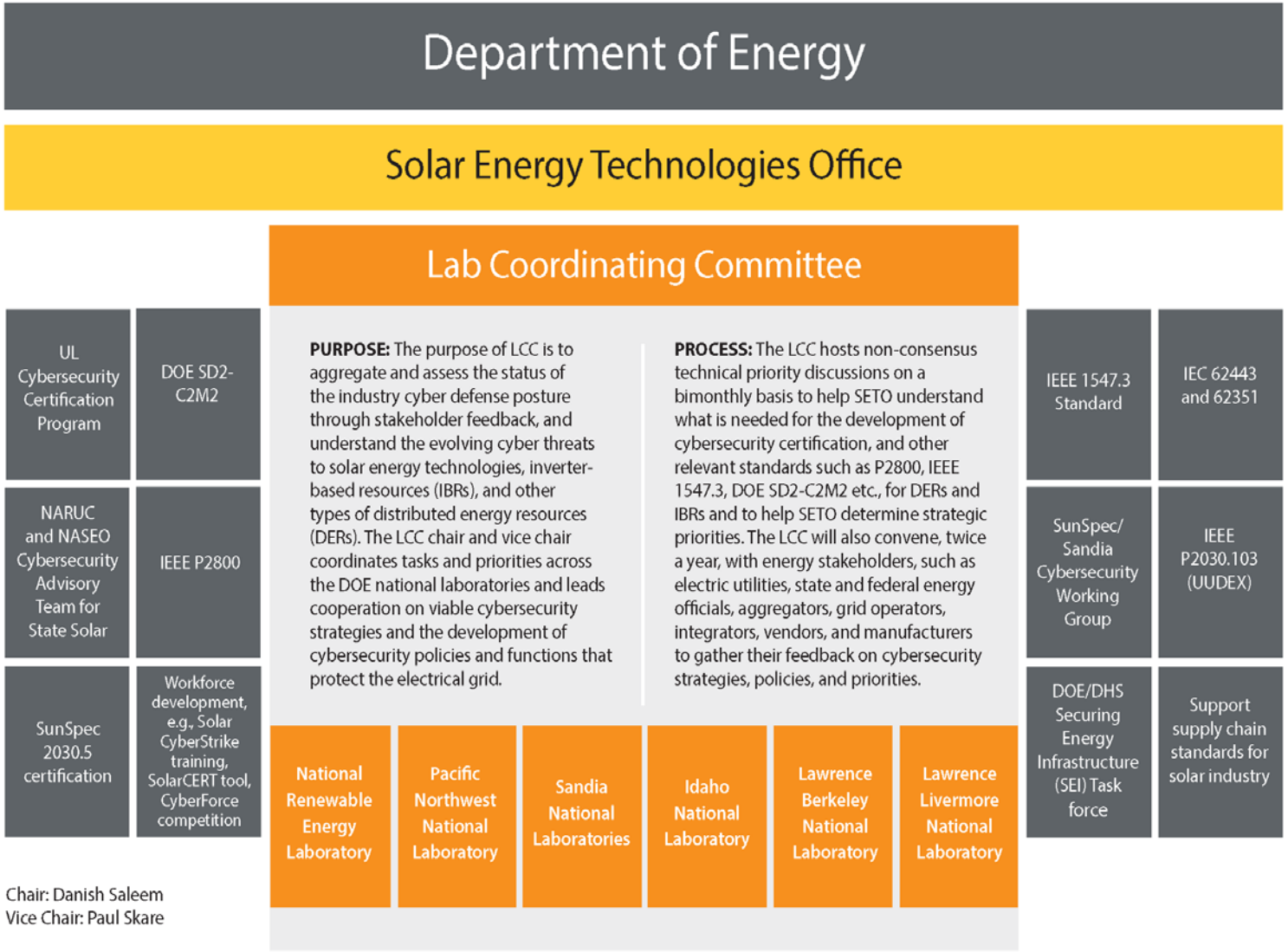
- Should we grow the wind consortium to be inclusive of wind, solar, and storage (hybrid energy systems)? Why or why not ?
- What could we achieve through consortium ? Could that be accomplished by other activities?
- What major challenges could be solved by having non-consensus discussion or debate among stakeholders ?
- What specific activities should we align under the consortium?
- How should the consortium pursue these activities?
- Where should the consortium be led and championed?
- Who should be involved in the consortium?

Solar Cybersecurity Efforts

Overview of Parallel Activities within the Solar Energy sector

Securing Solar for the Grid Program

- DOE SETO initiated Securing Solar for the Grid (S2G) program.
- The program is managed through an LCC using an Agile approach
- LCC met every 4–6 weeks to facilitate non-consensus discussion and debate on industry priorities and needs
- In fiscal year 2023, LCC plans to meet every 4–6 months with Industry Advisory Board.
- Goal is to:
  - Gather industry priorities and effectiveness feedback
  - Perform stakeholder engagement to assess industry gaps and challenges.
  - Perform continuous reprioritization evaluation.
  - Facilitate periodic informational webinars.



Team and Stakeholders

National Laboratory Point of Contacts

- **Idaho National Laboratory (INL):** Jake P. Gentle and Stephen A. Bukowski
- **Lawrence Berkeley National Laboratory (LBNL):** Sean Peisert and Daniel Arnold
- **Lawrence Livermore National Laboratory (LLNL):** Alex Campbell
- **National Renewable Energy Laboratory (NREL):** Danish Saleem and Jordan Peterson
- **Pacific Northwest National Laboratory (PNNL):** Paul Skare and Scott Mix
- **Sandia National Laboratories (Sandia):** Jay Johnson and Ifeoma Onunkwo

Industry Advisory Board Members

GE: Robby Simpson & Radhika Chaturvedi	**GridSME:** John Franzino	**UL**: Mike Slowinske & Ken Boyce	**SCE**: Rob Roel, Brian Foster & Kevin Sharp
Hitachi Energy: Steven Kunsman	**Burns & McDonell:** Ingrid Rayo	**Xanthus:** Frances Cleveland	**PJM:** Eric Hsiah
Solectria Solar: Emily Hwang	**NASEO:** Campbell Delahoyde	**NIST/NCCoE:** Jim McCarthy	**SDG&E:** Greg Smith & Cory Gerlitz
Eaton: Salam Bani Ahmed	**NCCOE:** James McCarthy	**SunSpec:** Tom Tansy	**CNK solution:** Shari Gribbin
Fortress: Gonda Lamberink & Tobias Whitney	**NERC:** Ryan Quint & Larry Collier	**SEIA:** Jeremiah Miller	**Mana Group:** Jennifer Jenkins
Operant Networks: Andrew Bartels	**SEPA:** Aaron Smallwood	**NRECA:** Emma Stewart	**NARUC:** Lynn Costantini
Kevala: Parth Pradhan	**FIU:** Arif Sarwat	**IREC: Brian Lydic**	**NERC-CIP:** Lonnie Ratliff
AT&T: Lawrence Laguardia and William Turanchik	**Iowa State University:** Manimaran Govindarasu	**ISA:** Andre Ristaino	

Focus Areas for Fiscal Year 2022

National Renewable Energy Laboratory (NREL)	• Support UL cybersecurity certification program • Support for IEEE 1547.3 cybersecurity guide • Support supply chain cybersecurity-related activities • Convene, coordinate, facilitate and lead the LCC meetings.
Pacific Northwest National Laboratory (PNNL)	• Support supply chain standards work for solar industry • Perform Secure Design Cybersecurity Capability Maturity Model (SD2-C2M2) assessments.
Idaho National Laboratory (INL)	• Support the development of Solar Cert tool • Develop Solar CyberStrike training and tool.
Sandia National Laboratories (Sandia)	• Support DHS Cyber Security Evaluation Tool (CSET) • Develop Solar CyberStrike training and tool.
Lawrence Livermore National Laboratory (LLNL)	• Support supply chain standards work for solar industry.
Lawrence Berkeley National Laboratory (LBNL)	• Support data privacy standards • Support automation standards related to DERs.

Hybrid Energy Systems

Challenges, Recent Incidents and Lessons Learned

Cybersecurity Challenges

Workforce development

Component Manufacturers

- Determine right level of security for products
- Embed security into development process
- Demonstrate validation of security to customers
- Differentiate products based on security

System Integrators

- Differentiate products and systems based on security
- Ensure purchase of secure systems and products
- Integrate with existing insecure systems
- Understand and minimize the risk of integration

Electric Utilities

- Maintaining security for legacy devices
- Lack of visibility into operating assets
- Accessibility of threat and risk information
- Lack of national or industry adopted cybersecurity requirements

Supply chain security

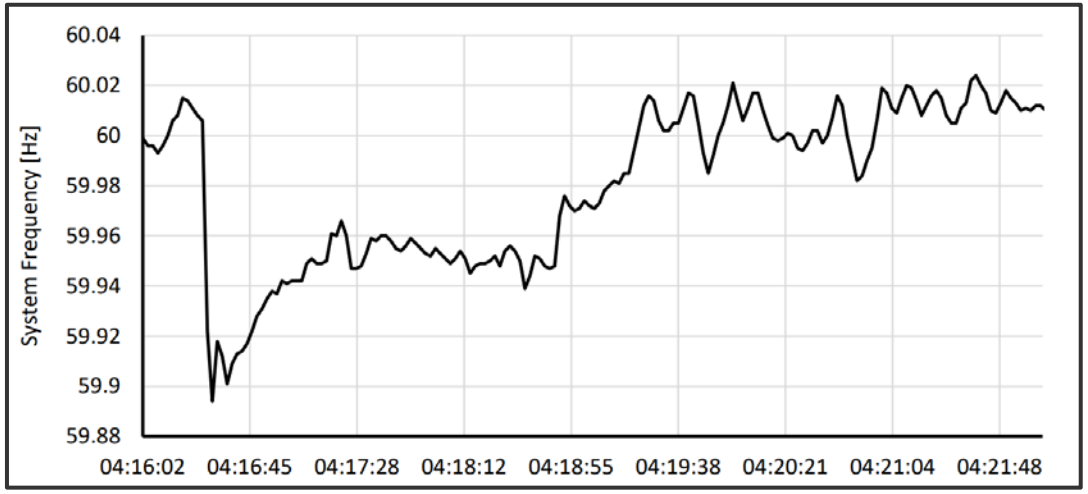
Panhandle Wind Disturbance

- Generator operators reported wind turbine icing and high windspeed cutoffs on the morning of March 22, 2022.
- Reduced wind resources were reported across the Texas panhandle.
- ERO analyzed these disturbances and the widespread reduction of inverter-based resources and summarized their findings in the *Panhandle Wind Disturbance* report.
- As a result, NERC recommended a performance-based standard for all inverter-based resources to help avoid instability, uncontrolled separation, or cascading outages.
- **The event highlighted how multiple IBRs across a geographic area failed to adhere to voltage and frequency protection requirements.**

A range of consequences from a successful cyberattack are possible in all cyber-physical energy systems, from the simple loss of power generation to the complete loss of the generating asset itself.

Overview of Disturbances from Wind Resources in the Texas Panhandle Area

Event 1	Phase to phase fault on 345 kV Gen Tie Line	Loss of 765 MW of wind resources (10 facilities)
Event 2	Phase to phase fault on 345 kV transmission circuit	Loss of 457 MW of wind resources (8 facilities)



Source: *Panhandle Wind Disturbance*. North American Electric Reliability Corporation, August 2022.

Utility Integration Scenario

Inverter or Controller

Customer or approved-vendor owns, installs, operates and maintains device

Customer owned gateway

Communicates over public internet

Potentially IEEE 2030.5

Utility Headend Server

Distribution Control Center

Through the Smart Inverter Working Group, IOUs proposed three potential methods to communicate with IBRs:
Option 1 – Customers site Inverters
Option 2 – Gateway or Inverter Energy Management Systems (EMS)
Option 3 – Collective management of customer inverters by Aggregators

NERC Guidance for DERs and IBRs

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cybersecurity for Distributed Energy Resources and DER Aggregators

NERC Security Integration and Technology Enablement Subcommittee
White Paper
August 2022

Purpose

This brief paper provides industry with information regarding activities underway to further secure the electricity ecosystem under rapid grid transformation, specifically in the area of cybersecurity efforts for distributed energy resources (DERs) and DER Aggregators. NERC is working with industry stakeholders to advance cybersecurity controls for DERs as the penetration of these resources continues to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in this area.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 6, 2019

Dear Electric Industry Vendor Community:

Re: Supply Chain Cyber Security Practices

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to develop or modify necessary Reliability Standards to address concerns that relate to supply chain risk management for industrial control system (ICS) hardware and software as well as computing and networking services associated with Bulk Electric System (BES) operations.[1] In October of 2018, FERC approved the Reliability Standards,[2] which will become effective on July 1, 2020.

This letter is intended to inform vendors to the electric utility industry of these new regulatory requirements and open a dialogue about the importance to electric utilities of working with their vendors to implement controls to manage supply chain security risks. Vendor products and services have a significant potential to impact the reliability of the BES. It is imperative that electric utilities work with their vendors to implement technical controls and processes to allow utilities to both meet their new regulatory obligations under NERC's Critical Infrastructure Protection (CIP) standards and to provide for a secure grid.

Recommended Industry Actions Moving Forward

The following are recommended actions that NERC and its stakeholders should take to support a secure electricity ecosystem with increasing levels of DERs (generation), load-side flexible resources, and DER aggregators.

1. **DER Cybersecurity Certification:** NERC and industry stakeholders should actively support DER cybersecurity certification initiatives, providing expertise related to BPS impacts of growing DERs and the introduction of the DER Aggregator. Efforts such as those pursued by UL to ensure that future DER equipment is designed, tested, and commercially installed with sufficient cybersecurity controls in place will help secure the overall electricity ecosystem. Without necessary cybersecurity controls designed in to the components and systems, security risks could be introduced and expensive and / or less effective bolt-on security measures could be necessary in the future.
2. **Cybersecurity in Distribution Interconnection Requirements:** Similar to how the Authority Governing Interconnection Requirements (AGIR) establishes necessary equipment performance specifications in IEEE 1547, the AGIR could also be responsible for establishing requirements that ensure newly interconnection DERs are equipped and operationally configured with specific cybersecurity controls in place. This will require modifications to the IEEE 1547 standard to ensure that cybersecurity is included in the standards body rather than as an informational guide (i.e., focusing on including some or all aspects of the IEEE 1547.3 guide into the main body of the IEEE 1547 standard).
3. **DER Aggregator Registration:** NERC and industry stakeholders have acknowledged that the concept of the DER Aggregator is not presently addressed in NERC registration criteria, constituting a reliability and security gap if DER Aggregators start actively controlling and operating significant amounts of DERs. In aggregate, these resources will have an impact on the bulk electric system (BES). The NERC Reliability and Security Technical Committee (RSTC) and its stakeholder groups should determine the extent of DER Aggregator participation in wholesale electricity markets today and in the future, and identify possible reliability and security risks these entities could pose if compromised. NERC will assess these reliability and security impacts and determine if the DER Aggregator should be included as a NERC Registered Entity under certain situations.
4. **Proactive Understanding of DER and DER Aggregator Cybersecurity Risks:** Industry stakeholders should actively engage in understanding the risk posed with growing levels of DERs and the introduction of DER Aggregators. Cyber security risks exist throughout the product lifecycle – equipment design, testing, commissioning, and operation. Understanding the aggregate risks posed by DERs and DER Aggregators, and how to mitigate them, will better posture the BPS for reliable operation of DERs.

Cybersecurity Focused Consortium – Why Now?

- FERC 2222 states that DER can provide transmission services if capable, typically in aggregate
- Where is the line between transmission-connected Inverter-based Resources (IBR) and distribution-connected DER?
- CAISO already supports storage systems providing ancillary services
- PUCs asking electric utilities to establish Functional Integration Program with cybersecurity requirements for DER/IBR
- PG&E, SCE and SDG&E filed for modifications to Rule 21, which allows communications capable inverter based generating facilities to comply with UL 1741SB and IEEE 1547.1
- Among Solar, rooftop and small solar in the western interconnection only is approximately 30,000 MW, representing about 65%, but none of it requires to follow NERC CIP

A national cybersecurity focused consortium can aid industry stakeholders in evaluation and validation of cybersecurity posture of their DER or IBR devices and/or systems before they are connected to the electric grid

CNN

Biden administration says solar energy has the potential to power 40% of US electricity by 2035

Nilsen, Ella. CNN.com, September 8, 2021. url

Reuters

Solar energy can account for 40% of U.S. electricity by 2035, according to DOE

Volcovici, Valeri. Reuters.com, September 8, 2021. url

NBC

Nearly half of U.S. electricity could come from solar by 2050, Biden administration

Lederman, Josh. NBC.com, September 8, 2021. url

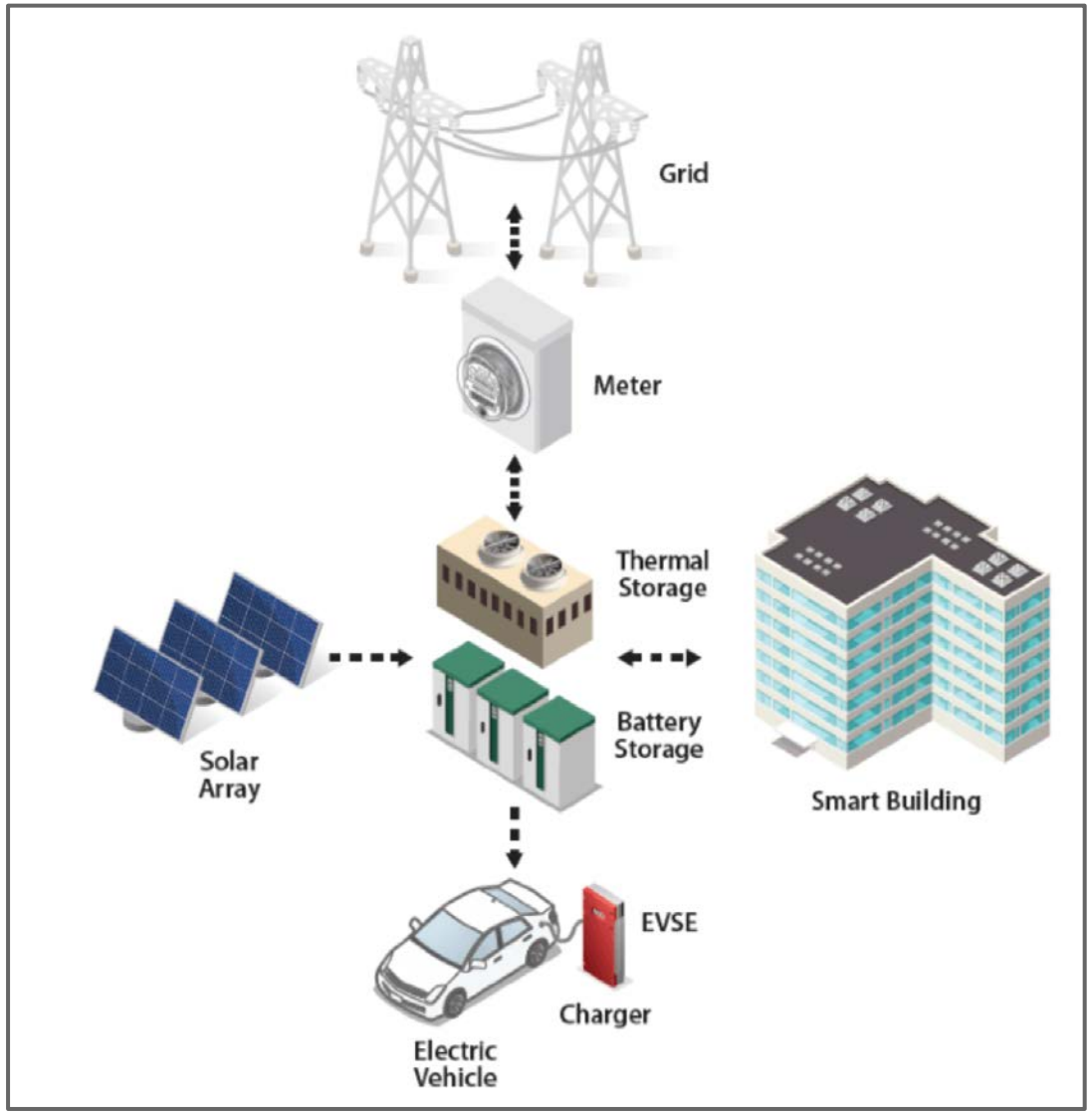
NERC

Variable-energy resources ….continue to be a significant component of new capacity

NREC Planning Committee Meeting, June 6, 2017. url

Behind-the-Meter Storage Consortium

- Focused on energy storage technologies for stationary applications less than 10 megawatt-hours
- Goal is to minimize costs and grid impacts by integrating EV charging, PV generation, and energy-efficient buildings using controllable loads.
- Consists of a multidisciplinary team to perform research on the integration of energy system technologies
- Guided by system-level thinking for research at low TRL
- Research is focused on developing new battery storage solutions that can perform at high power for excellent EV charging efficiency
- Funded by DOE VTO, NREL leads this consortium research, along with Idaho National Laboratory, Sandia National Laboratories, and Argonne National Laboratories



Charge Questions

- Should we grow the wind consortium to be inclusive of wind, solar, and storage (hybrid energy systems)? Why or why not ?
- What could we achieve through consortium ? Could that be accomplished by other activities?
- What major challenges could be solved by having non-consensus discussion or debate among stakeholders ?
- What specific activities should we align under the consortium?
- How should the consortium pursue these activities?
- Where should the consortium be led and championed?
- Who should be involved in the consortium?

Thank you

NREL/PR-5R00-84094

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Wind Energy Technologies Office and Office of Cybersecurity Energy Security and emergency Response. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NREL

Transforming ENERGY