Land-Based Wind Reference Architecture

Zoe Dormuth, Jon Keller, Venkatesh Venkataramanan, Bryan Richardson, and Keith Schwalm

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated under Contract No. DE-AC36-08GO28308

This report is available at no cost from NREL at www.nrel.gov/publications.

Technical Report
NREL/TP-5T00-91222
September 2025

Land-Based Wind Reference Architecture

Zoe Dormuth, Jon Keller, Venkatesh Venkataramanan, Bryan Richardson, and Keith Schwalm

National Renewable Energy Laboratory

Suggested Citation
Dormuth, Zoe, Jon Keller, Venkatesh Venkataramanan, Bryan Richardson, and Keith Schwalm. 2025. *Land-Based Wind Reference Architecture*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5T00-91222. https://www.nrel.gov/docs/fy25osti/91222.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated under Contract No. DE-AC36-08GO28308

This report is available at no cost from NREL at www.nrel.gov/publications.

Technical Report
NREL/TP-5T00-91222
September 2025

15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by NREL for the U.S. Department of Energy (DOE), operated 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. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover photos (clockwise from left): Josh Bauer, NREL 61725; Visualization from the NREL Insight Center; Getty-181828180; Agata Bogucka, NREL 91683; Dennis Schroeder, NREL 51331; Werner Slocum, NREL 67842.

List of Acronyms

ARIES	Advanced Research on Integrated Energy Systems
DNP3	Distributed Network Protocol 3
DOE	Department of Energy
NREL	National Renewable Energy Laboratory
OEM	original equipment manufacturer
OS	operating system
OT	operational technology
SCADA	supervisory control and data acquisition
TMW	Triangle MicroWorks
VLAN	virtual local area network
VM	virtual machine
WETO	Wind Energy Technologies Office
WTG	wind turbine generator

Executive Summary

This report summarizes the final deliverables for the Land-Based Wind Reference Architecture project funded by the U.S. Department of Energy's Wind Energy Technologies Office. The project's objective was to further refine the existing wind power plant reference architecture, originally developed by Idaho National Laboratory and Sandia National Laboratories, by expanding the wind turbine generator into a high-fidelity reference architecture that encompasses the full range of the turbine's components. Additional details regarding the wind turbine system and how it integrates with a wind power plant were researched and are reflected in the reference architecture. With this additional information, researchers can understand how the components and devices in a wind turbine function and how a wind turbine integrates into a wind power plant so they can perform cybersecurity evaluations on the system. The communication and control systems were the focus of this reference architecture to understand the cybersecurity posture of a wind turbine and power plant. The information technology and operational technology systems perspective is integral to improving the cybersecurity posture because it is the starting point for understanding, from an integrated systems standpoint, how to safely design and deploy wind energy in the power grid. A holistic wind power plant and turbine reference architecture and simulation were developed and were placed in an open-source repository for further research efforts.

Table of Contents

List of Figures

List of Tables

1 Combined Wind Power Plant and Turbine Reference Architecture

This project expanded on the wind turbine generators (WTGs), which are illustrated as white boxes in the bottom of the wind power plant control network reference architecture in Figure 1. The wind power plant control network was developed during the Wind Cyber Hardening project performed by Sandia National Laboratories and Idaho National Laboratory (Johnson 2021). The wind turbine reference architecture is illustrated in the wind turbine network on the right side of Figure 1. The wind turbine reference architecture was developed by the National Renewable Energy Laboratory (NREL) and was integrated into the existing wind power plant reference architecture. The wind turbine is connected to the wind power plant via a supervisory control and data acquisition (SCADA) network. The turbine is divided into three sections: tower base, nacelle, and hub and blades. This report provides details about the components and connections in each part of the turbine and how the wind turbine network connects and communicates to the wind power plant control network.

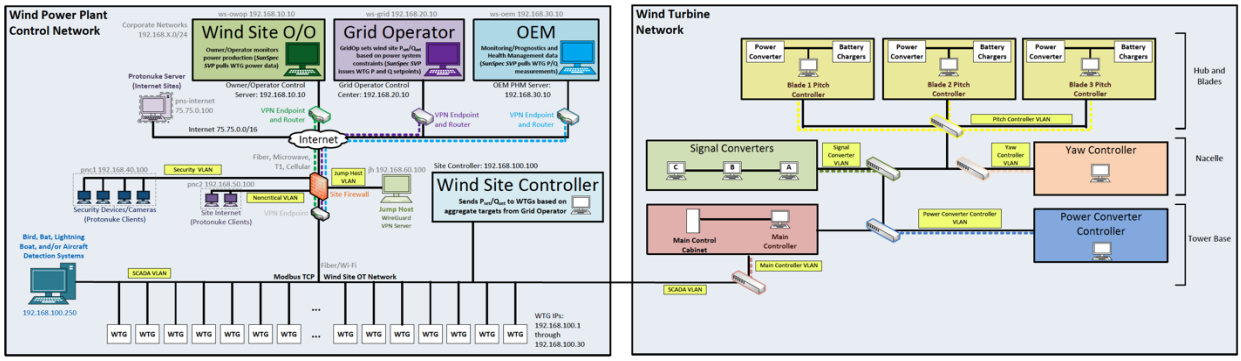

Figure 1. Combined wind power plant and turbine reference architecture

1.1 Wind Power Plant Reference Architecture

The wind power plant reference architecture shown in Figure 2 contains a wind site owner/operator, grid operator, original equipment manufacturer (OEM), and wind site controller. The wind site owner/operator, grid operator, and OEM access the wind power plant network through virtual private networks. Within the wind power plant control network, virtual local area networks (VLANs) are used to segment the network. A jump host is the gateway to the remote wind power plant network. The protonuke servers and clients represent internet sites and security devices/cameras. The protonuke devices can generate communication traffic for HTTP, HTTPS, SSH, and SMTP protocols. The SCADA VLAN connects the wind turbines and wind site controller and enables communication between the plant and turbines.

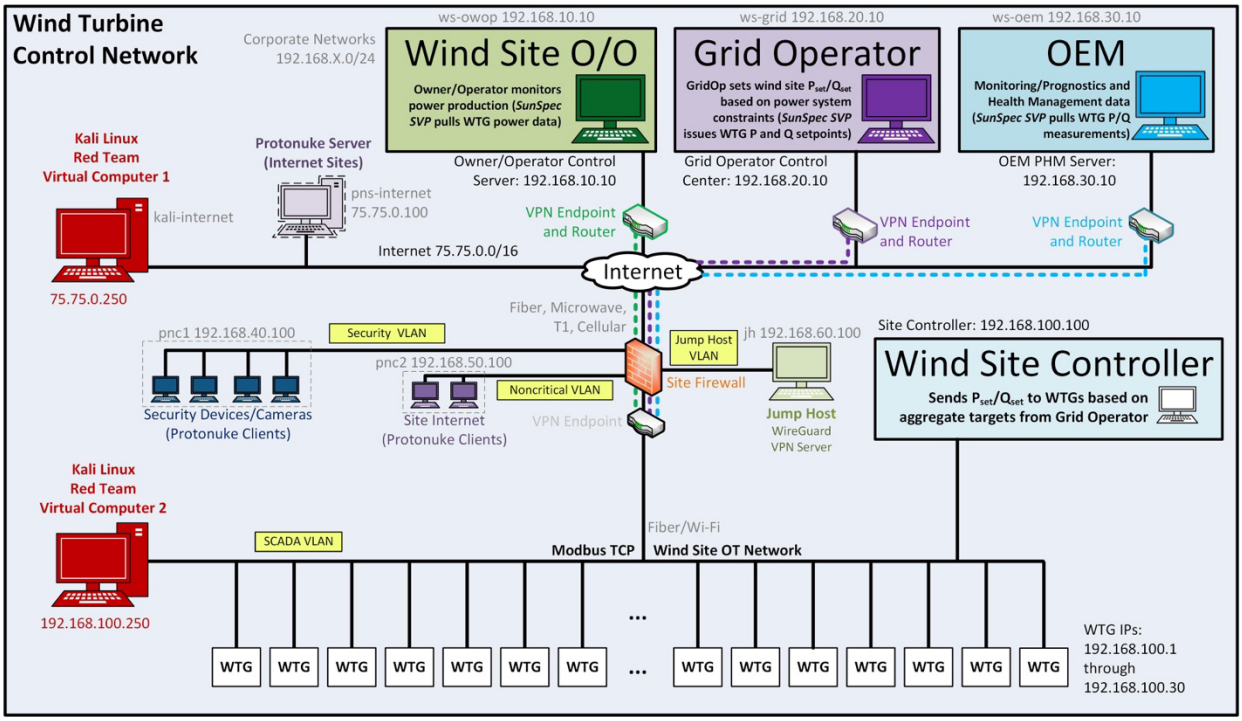

Figure 2. Wind power plant reference architecture

1.2 Wind Turbine Reference Architecture

The wind turbine reference architecture shown in Figure 3 connects to the wind power plant reference architecture through the SCADA VLAN. This reference architecture was developed by reviewing the components in a wind turbine and analyzing the function of each component and how it communicates with other components in the wind turbine and power plant. Wind power systems subject matter experts at NREL were involved in this process to understand the critical components in a wind turbine. A wind site controller in the wind power plant is used to communicate to each turbine. Within the turbine, there are multiple VLANs to segment the network for each turbine component. The tower base contains the main controller, which sits in the main control cabinet, and the power converter controller. The nacelle contains the yaw controller and signal converters, which represent multiple devices such as auxiliary controls, anemometer, sensors, and protection systems. The hub and blades contain three pitch controllers that are connected to their own power converter and battery chargers, which provide backup power for control.

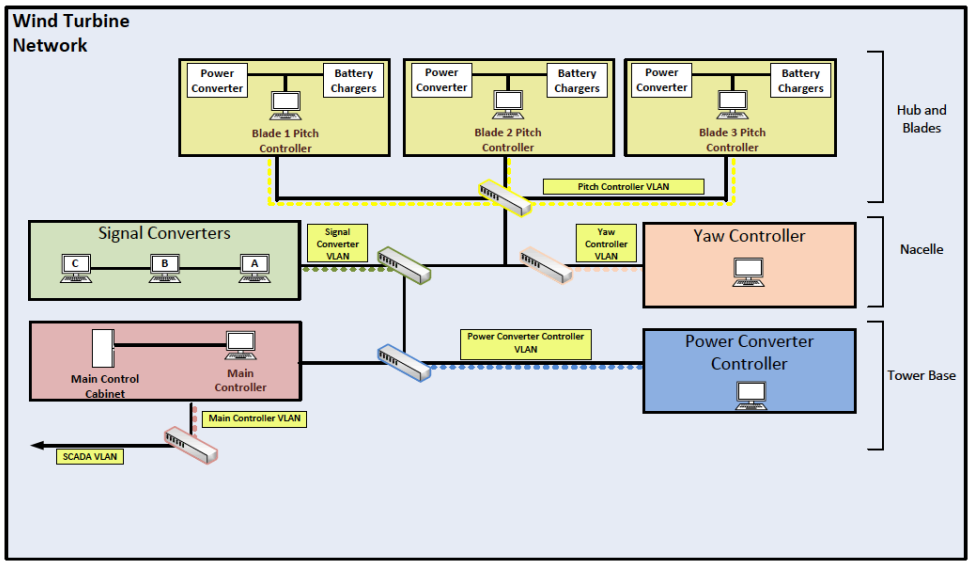

Figure 3. Wind turbine reference architecture

Each component communicates by receiving input and output from the other devices within the turbine and wind site controller. Table 1 describes each device, its purpose, and its communication procedures.

Table 1. Wind Turbine Reference Architecture Devices

Device	Description	Communication
Main controller	• Receives cut-in and cut-out wind speeds from the power module • Receives wind speed and direction from the Modbus module • Determines if the turbine blades should be feathered based on how the wind speed compares to cut-in and cut-out values	• Receives current yaw from the Modbus module; determines if the yaw set point should be adjusted based on the wind direction and current yaw • Distributed Network Protocol 3 (DNP3) provides a binary output point for activating turbine emergency stop mode • Input/output publishes power output from the power module to the other HELICS federates (which represent other components in the simulation)
Power converter controller (module within main controller)	• Receives wind speed, direction, temperature, and pressure from the Modbus module the in main turbine controller	• Receives emergency stop message from DNP3 module and skips power calculations if emergency stop is active
Signal converter (anemometer)	• Replays historical weather data captured from NREL Flatirons Campus turbine at 1-second intervals	• Modbus makes weather data available via input registers
Yaw controller	• Adjusts yaw based on the yaw set point. Uses an error of 4% to determine if adjustment is still needed. Adjusts yaw by 0.1 degree per second	• Yaw set point is received from the main controller via Modbus • Current yaw is made available via Modbus
Pitch controllers	• Periodically queries the signal converter for wind speed, direction, temperature, and pressure conditions • Periodically queries the yaw controller for current yaw	• Receives feather commands from the main controller

2 Simulation

A simulation for the wind turbine reference architecture was developed and integrated into the existing simulation for the wind power plant reference architecture. The design and tools required to deploy the wind power plant reference architecture were used to develop the wind turbine simulation. Additionally, a visualization for the reference architectures was added to improve user experience.

2.1 Open-Source Code

The simulation is open source to allow further research to be performed using the developed reference architecture and simulation. The files needed to run the simulation are hosted in GitHub repositories, listed in Table 2.

The required tools to deploy the simulation are listed below:

- phenix
- minimega
- Storage backend
- Continuous integration/continuous development workflow
- Configuration files, virtual machine (VM) images, and injects
- The repositories listed in Table 2 contain instructions and source code to deploy the wind power plant and turbine reference architecture simulations.

Table 2. Open-Source Repositories

Name	Description
Wind power plant with turbine architecture	https://github.com/patsec/wind-turbine
OT-sim with the controller modules	https://github.com/patsec/ot-sim
Wind turbine phenix application	https://github.com/sandia-minimega/phenix-apps

2.2 Wind Power Plant and Turbine Simulation

The combined wind power plant and turbine simulation illustrated in Figure 4 shows phenix's visualization output for the topology, configuration, and scenario files needed to deploy the combined simulation. There are 30 wind turbines deployed and each communicates to the wind site controller over the SCADA VLAN. The existing wind power plant reference architecture simulation was used to develop and deploy the wind turbine reference architecture simulation shown in detail in Section 2.3 of this report. The visualization can be challenging to read in the nodal output, and further efforts to improve the visualization are explained in Section 2.5.

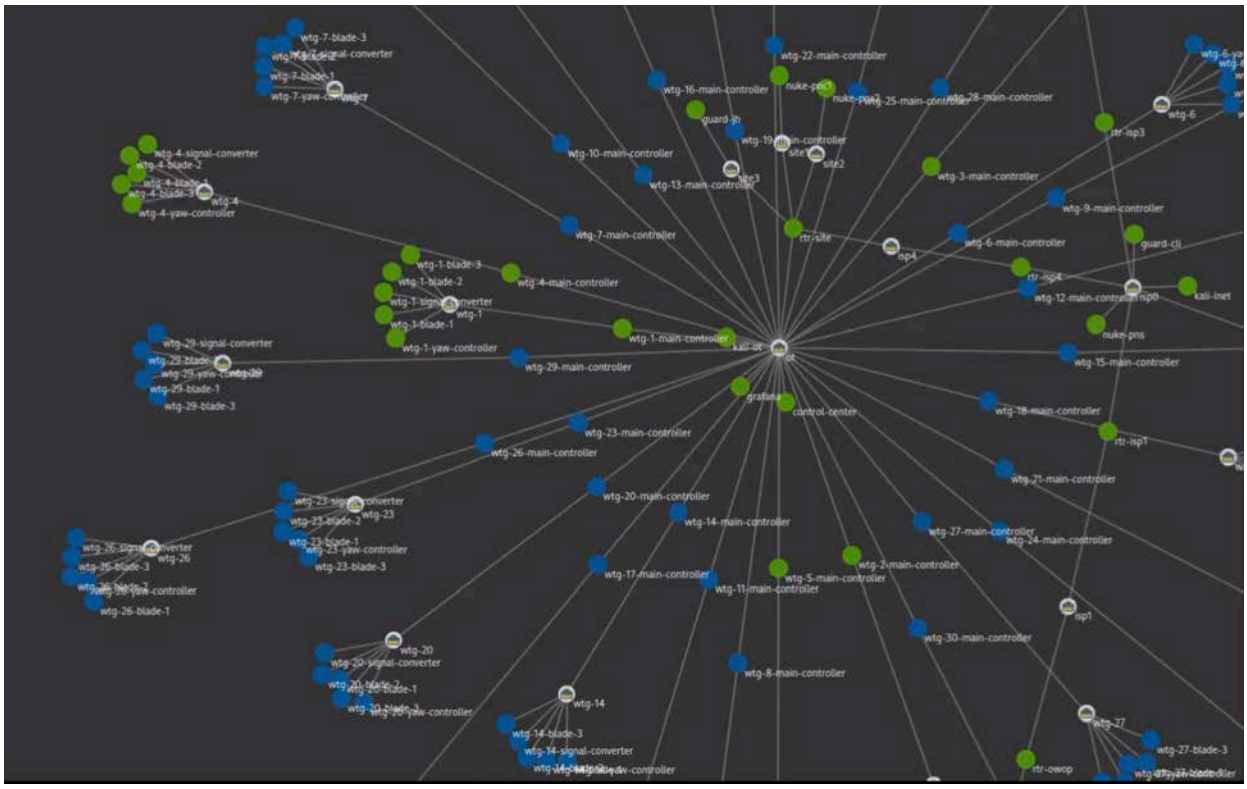

Figure 4. Combined wind power plant and turbine phenix simulation

The following is a list of the components specific to the wind power plant simulation:

- Wind Entities
  - ws-owop
    - Owner-Operator node
    - Windows operating system (OS)
    - control-center qcow2 image
  - ws-grid
    - Grid Operator node
    - Windows OS
    - control-center qcow2 image
  - ws-oem
    - OEM Operator node
    - Windows OS
    - control-center qcow2 image
  - wind-site-controller
    - Wind Site Controller node
    - Windows OS
    - control-center qcow2 image
- Red Team Machines
  - Kali-ot
    - Kali VM for operational technology (OT) environment

        - Linux OS
        - Kali qcow2 image
    - Kali-inet
        - Kali VM for IT environment
        - Linux OS
        - Kali qcow2 image
- Security Cameras/Devices and Site Internet
    - nuke-pnc1/nuke-pnc2
        - Protonuke Client nodes
        - Linux OS
        - protonuke qcow2 image
- Internet Sites
    - nuke-pns
    - Protonuke Server node
    - Linux OS
    - protonuke qcow2 image
- Jumphost
    - guard-jh
        - WireGuard Jump Host node
        - Linux OS
        - wireguard qcow2 image
    - guard-cli
        - WireGuard Jump Host Command Line Interface node
        - Linux OS
        - wireguard qcow2 image.

2.3 Wind Turbine Simulation

The wind turbine simulation produced by phenix in a nodal visualization, as shown in Figure 5. There are six nodes, or VMs, that represents the devices in a wind turbine. These are listed below. The main controller contains a module that represents the power converter controller.

Wind turbine simulation devices:

- wtg1-main-controller (contains power converter module)
- wtg1-signal-converter
- wtg1-yaw-controller
- wtg1-blade-1
- wtg2-blade-2
- wtg3-blade-3.

In addition, there are two routers. One represents the connection of the wind turbine, the WTG box, to the OT network to communicate with the wind power plant. A second router is for the turbine network and segments the devices that are in the wind turbine.

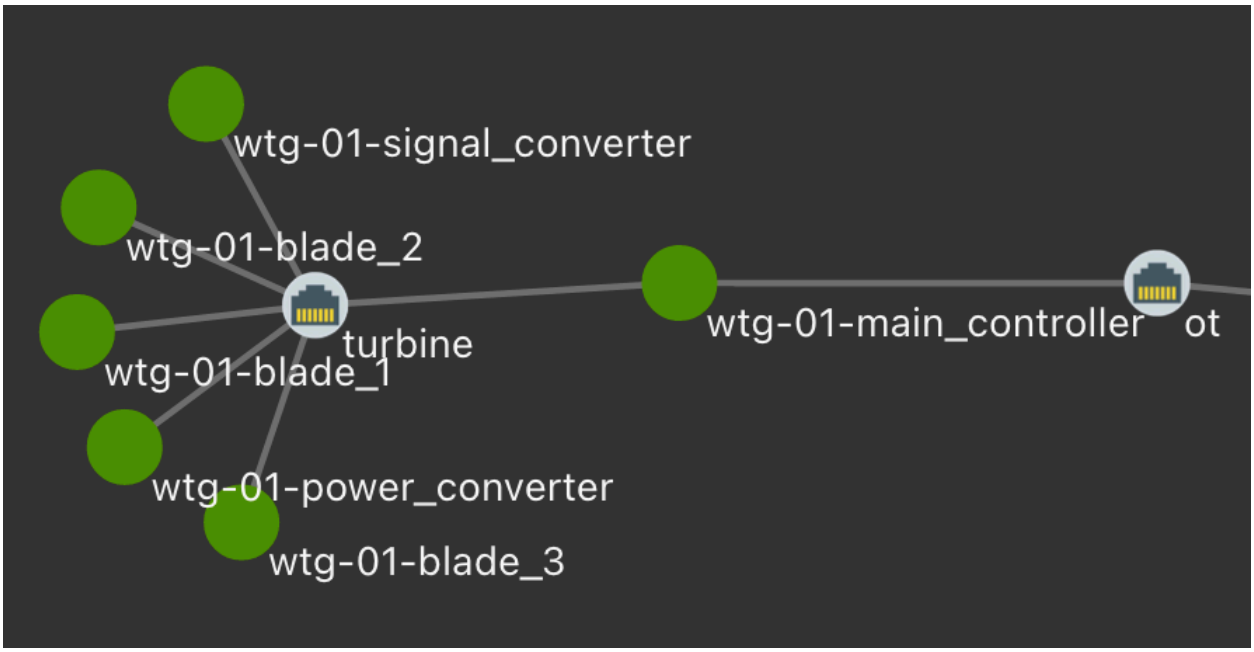

Figure 5. Wind turbine phenix simulation

The wind turbine simulation developed custom logic to process inputs and produce outputs to send to various devices in the turbine. This logic was developed using fundamental wind turbine physics and control data. Figure 6 shows the logic for each device of the wind turbine and how they communicate to the wind turbine main controller.

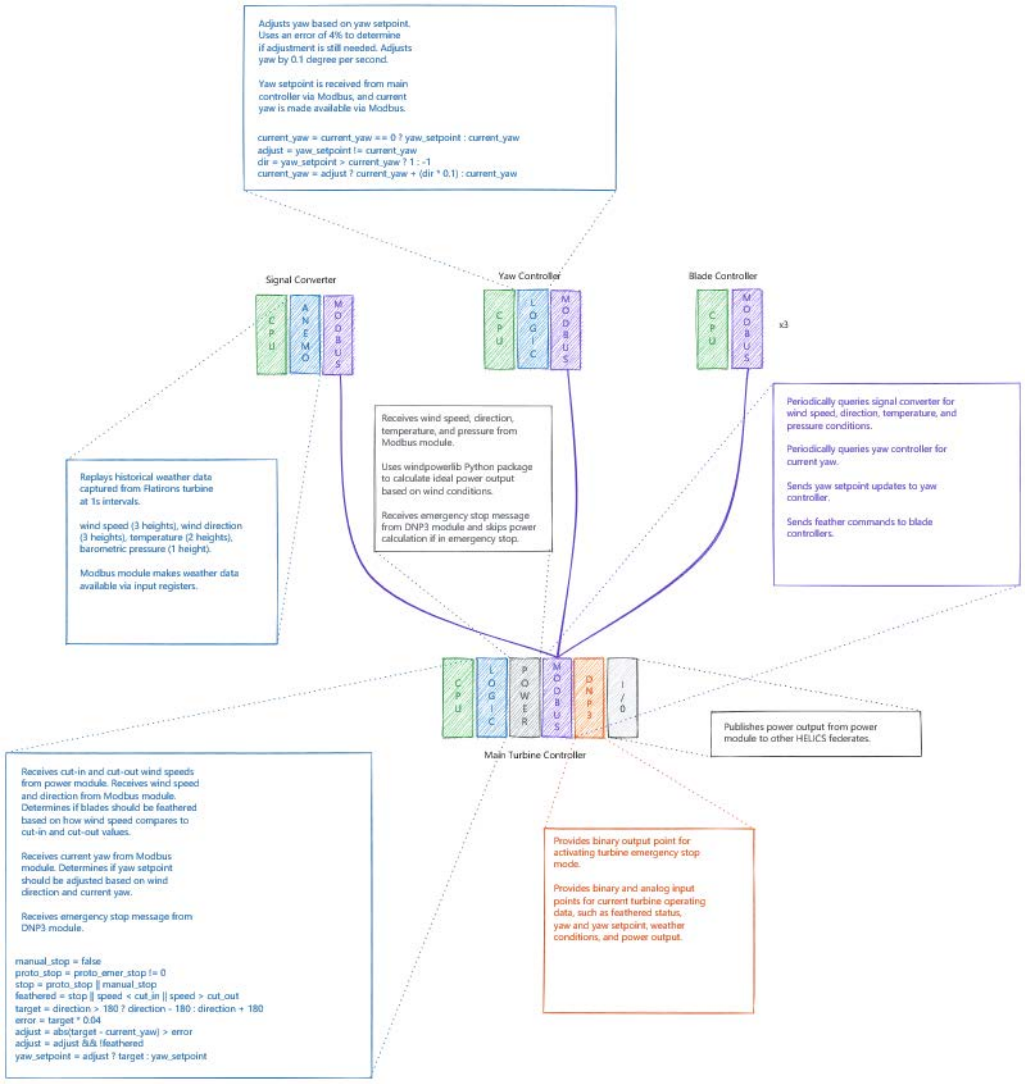

Figure 6. Wind turbine simulation logic

2.4 Network Communications

A SCADA VLAN connects the turbine, or WTG, to the wind site OT network through the SCADA VLAN using a Modbus protocol. The wind power plant SCADA network is controlled through a human-machine interface. This can be either from the control panel or from a remote computer via SCADA.

The wind site controller has a module for Modbus and DNP3. The Modbus protocol module periodically queries the signal converter for wind speed, direction, temperature, and pressure conditions. It also periodically queries the yaw controller for the current yaw. It sends yaw set point updates to the yaw controller and feather commands to pitch controllers.

The DNP3 protocol module is used to provide a binary output point for activity turbine emergency stop mode. It also provides binary and analog input points for current turbine

operating data, such as feathered status, yaw and yaw set points, weather conditions, and power output.

2.5 Visualization

The visualization for the reference architecture simulations was enhanced to provide the users a better understanding of the simulation. The visualizations from the phenix tool provide a nodal representation of the simulation that can be a challenge to interpret. The visualization enhancements include an application to show control center data and a user-friendly dashboard that shows a wind turbine and its data.

Triangle MicroWorks (TMW) is an application that supports software libraries for industry standard communication protocols and testing and simulation tools to validate devices and networks, and a SCADA data gateway. The TMW Distributed Test Manager was used to simulate SCADA communications and visualize the data communication in the simulation. Figure 7 shows point type data that represent wind turbine values such as wind speed, blade pitch, and other data that are read and written to different devices in the wind turbine. An example is the binary inputs point type value in the first row, which is set to 0 to shut down the turbine. A corresponding analog inputs point type in the third row has a value of 92.9 to represent a pitch angle of 90 degrees, which shows that the turbine is at rest.

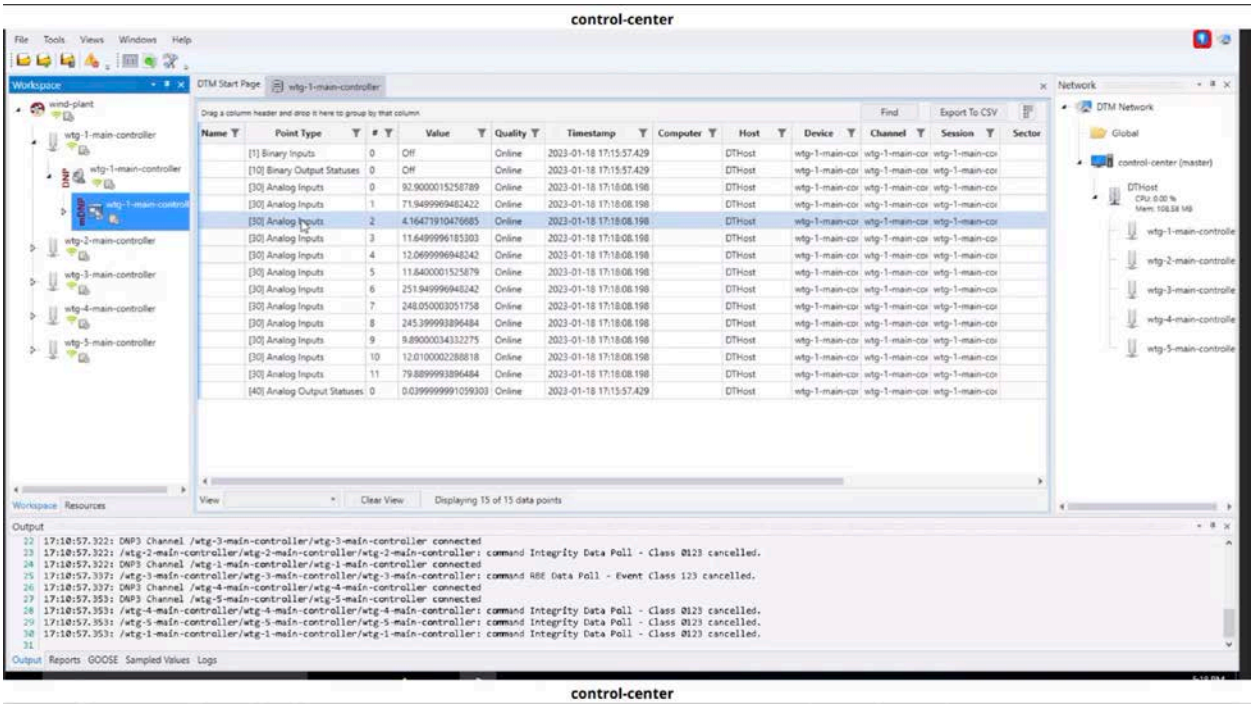

Figure 7. Triangle MicroWorks control center

Figure 8 shows a user-friendly dashboard created using the Grafana application to illustrate a wind turbine with input and output data. The data points include power output, feathered value, wind direction, wind speed, temperature, yaw current, yaw set point, and pressure. The wind turbine will spin when producing power and will be stopped when not producing power. This dashboard can scale up to the number of turbines in the simulation, and the user can click on each turbine to see its specific values.

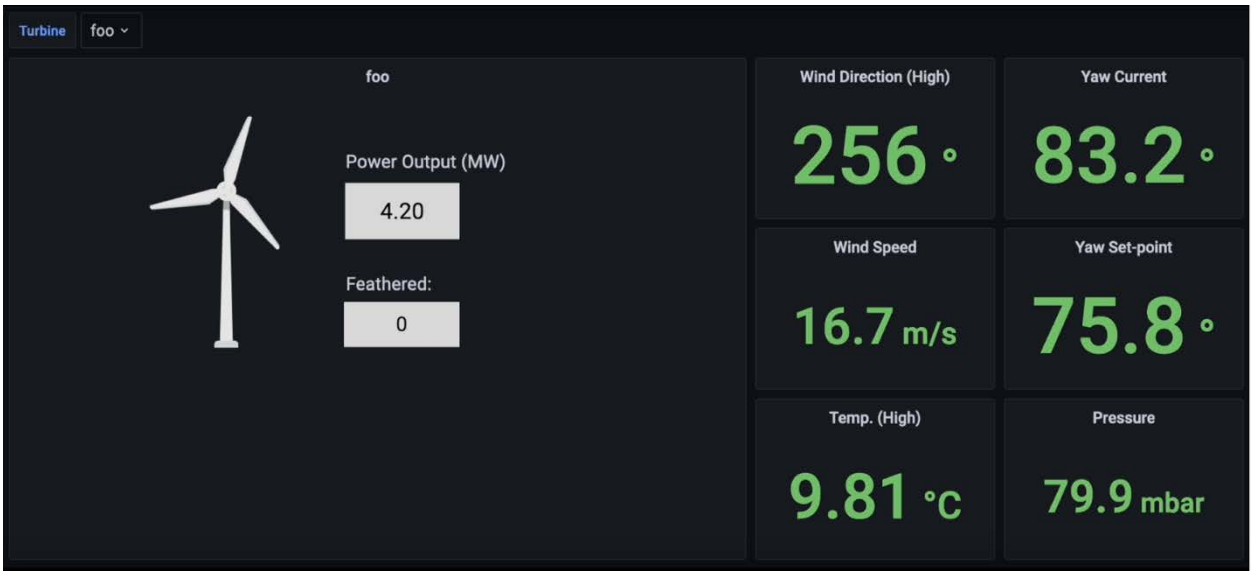

Figure 8. Simulation dashboard visualization

3 ARIES Cyber Range Demo

The wind power plant reference architecture simulation and accompanying visualization was integrated into the Advanced Research on Integrated Energy Systems (ARIES) Cyber Range demonstration, which was first showcased at the NREL FY23 Cyber Resilience Symposium. The purpose of this demonstration was to showcase current and previous ARIES project work at NREL and collaborations across the U.S. Department of Energy's (DOE's) national laboratories. The reference architecture simulation was a part of this large demonstration, and further details can be found on the NREL website. The reference architecture simulation represented a generation asset as a wind power plant. It was incorporated to simulate a cyber adversary sending a malicious command to perform an emergency shutdown of all turbines at a wind power plant and to illustrate the impact on the power grid for a wind power plant generation loss.

The wind power plant reference architecture simulation was used to represent an independent power producer on the generation side of the electric grid. It includes 30 high-fidelity virtual wind turbines implemented as OT-sim devices (six for each turbine), a plant control center, and remote connections to site owner/operator and OEM networks (Patria Security 2021). Also included is a Grafana VM used as the site controller in the demo scenario that collects turbine data from elastic search and displays status information in a dashboard. The visualization portion was supported by DOE's Wind Energy Technologies Office (WETO) in the wind reference architecture project. In addition, there is a network connection from the site router to an internet VLAN, which is shared by all three topologies in the larger demonstration (generation, transmission, and distribution). This shared internet connection is also where the owner/operator and OEM connections are made.

Topology

The wind power plant topology was created using previous work funded by WETO for the Wind Cyber Hardening project. The PowerWorld save case was developed based on the 2000-bus synthetic grid model created by Texas A&M University and modified to include 30 wind turbine generator models connected to bus 2100 in the model (Electric Grid Test Case Repository 2016).

Modifications were made to support the demonstration environment including:

- Removed unused nodes: protonuke client/server, Kali, HIDS/NIDS/SOAR, SIEM
- Upgraded low-fidelity wind turbine generator VMs to use multi-controller models. This work leveraged this project, the Wind Reference Architecture project led by NREL, and funding from WETO that developed OT-sim based higher-fidelity wind turbine models.

Scenario

- The wind plant scenario includes the phenix user apps listed in Table 3.

Table 3. Wind Plant Scenario Phenix User App Descriptions

Name	Description
tmw	Generates configuration files for Triangle MicroWorks Distributed Test Manager, zips them up, and injects the zip into a specified node.
vrouter*	Generates configuration files for specified virtual routers and injects the configuration into the corresponding nodes. Specifically for this scenario, the vrouter app configures the IPsec tunnel between the wind plant and transmission utility's demilitarized zone (DMZ)
wind-turbine	Generates XML configuration files for all virtual wind turbines (OT-sim devices) and injects the file into the respective nodes.

* Indicates a default or core phenix app

The wind plant and turbine reference architecture efforts were utilized to demonstrate a generation asset in a wider power grid, potential cyberattacks, and the consequences of those attacks. Figure 9 shows the visualization that was created for this demonstration. The figure to the left shows 30 wind turbines running as expected, and the figure to the right shows 30 wind turbines shut off and not generating power due to the cyber adversary sending an emergency stop command to each turbine.

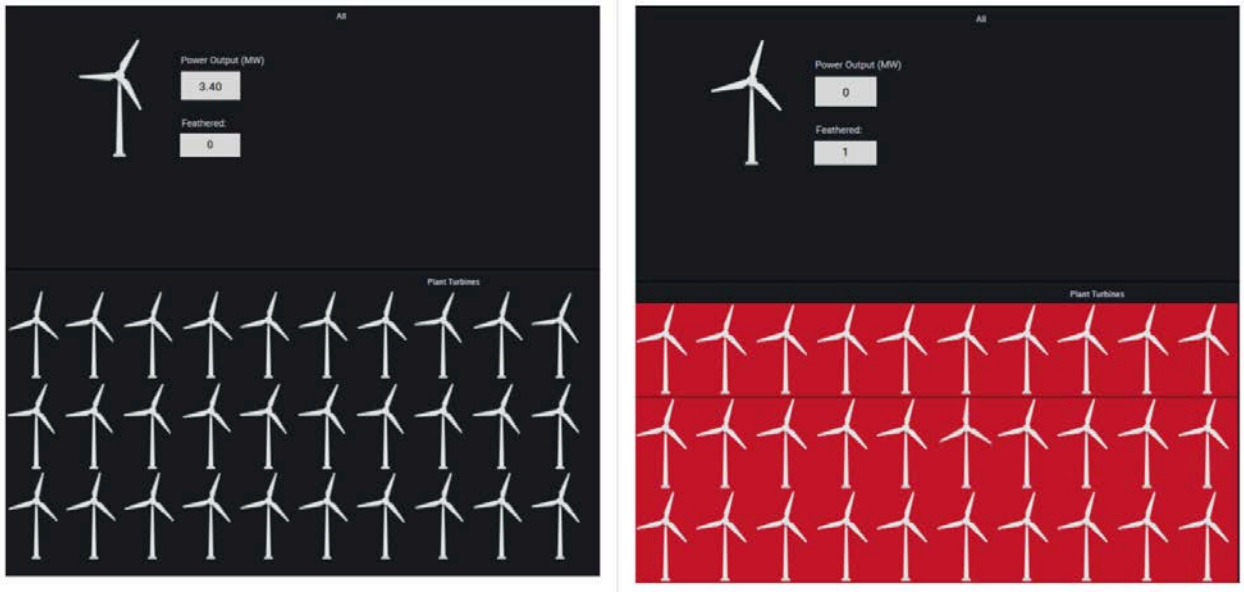

Figure 9. Wind power plant demo visualization

4 Future Work

One motivation for developing a combined wind power plant and turbine reference architecture was to have a tool to use in future research efforts. Reference architectures serve as a starting point for designing systems, and in the cybersecurity domain, they provide a starting point for developing security implementations (Martin et al. 2022). The shift in focus and resources toward achieving a clean, modern, and efficient power grid imposes cybersecurity implications for new technology integrations. It is important to study the effect of installing modern grid technology and expanding the energy footprint to rely increasingly on clean energy. Research focused on evaluating the cybersecurity posture of renewable technology will better secure and increase the reliability of the power grid.

The Renewable Energy and Storage Cybersecurity Research project, funded by DOE's Office of Cybersecurity, Energy Security, and Emergency Response, plans to develop a blended reference architecture suite that includes wind, solar, and energy storage systems. The combined wind power plant and turbine reference architecture will be integrated into this suite of reference architectures to model a hybrid energy system. This will support the study of the interconnection of hybrid energy assets in multiple configurations of varying sizes on the wider power grid. The reference architecture simulations are deployed in the ARIES Cyber Range (NREL n.d.). An emulation library hosts the configuration, topology, and scenario files needed for users to create custom experimental environments and to deploy the reference architecture simulations.

The Offshore Wind Cybersecurity project funded by WETO will research offshore wind energy and transmission networks as well as their connections to the power grid. The wind power plant and turbine reference architectures will provide a starting point to compare offshore wind turbine infrastructures to land-based architectures. The standards for cybersecurity, wind energy infrastructure, and interconnections to the grid will be applied to the reference architectures to understand potential gaps in standards and frameworks. The development of a reference architecture will be used to perform cybersecurity assessments and scenarios to demonstrate solutions to improve the security posture of offshore wind energy.

References

Electric Grid Test Case Repository. 2016. "ACTIVSg2000: 2000-bus synthetic grid on footprint of Texas." https://electricgrids.engr.tamu.edu/electric-grid-test-cases/activsg2000/.

Johnson, Jay. 2021. "E10 – Hardening Wind Energy Systems from Cyber Threats." Presented at the 2021 Wind Program Peer Review Report and Presentation meeting, Virtual, August 2–5, 2021. https://www.energy.gov/sites/default/files/2021-10/fy21peerreview-gridintegration-snl-johnson2.pdf.

Martin, Maurice, Samuel Chanoski, Steve Granda, and Steven Kunsman. 2022. "Reference Architectures as a Means of Influencing ICS Security Outcomes." This publication was produced for the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response by the Technical Project Team of the Security Energy Infrastructure Executive Task Force. https://inl.gov/wp-content/uploads/2022/04/SEI-ETF-Reference-Architecture-for-EEOT.pdf.

National Renewable Energy Laboratory. No date. "Advanced Research on Integrated Energy Systems Cyber Range." https://www.nrel.gov/security-resilience/cyber-range.html.

Patria Security, LLC. 2021. "Operational Technology (OT) Simulator." https://ot-sim.patsec.dev/.