Renewable Energy and Storage Cybersecurity Research (RESCue) Pilot Final Report

Danish Saleem, Charles MaGill, Venkatesh Venkataramanan, Zoe Dormuth, Adarsh Hasandka, and Emily Waligoske

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5T00-89921
September 2024

Renewable Energy and Storage Cybersecurity Research (RESCue) Pilot Final Report

Danish Saleem, Charles MaGill, Venkatesh Venkataramanan, Zoe Dormuth, Adarsh Hasandka, and Emily Waligoske

National Renewable Energy Laboratory

Suggested Citation

Saleem, Danish, Charles Magill, Venkatesh Venkataramanan, Zoe Dormuth, Adarsh Hasandka, and Emily Waligoske. 2024. *Renewable Energy and Storage Cybersecurity Research (RESCue) Pilot Final Report*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5T00-89921. https://www.nrel.gov/docs/fy24osti/89921.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5T00-89921
September 2024

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

NOTICE

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 the U.S. Department of Energy Office of Energy Office of Cybersecurity, Energy Security, and Emergency Response. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Acknowledgments

Project Renewable Energy and Storage Cybersecurity Research (RESCue) and this report were made possible through the collaborative efforts of the RESCue consortium members, including:

- Vestas
- GE Vernova
- Siemens-Gamesa
- Orsted
- Berkshire Hathaway Energy
- Idaho National Laboratory (INL).

The project team expresses its gratitude to all RESCue consortium members, including the renewable energy companies and asset owners, for their active participation, knowledge sharing, and commitment to advancing the cybersecurity of hybrid renewable energy systems. Their collective efforts and willingness to collaborate have been crucial in addressing the evolving cyber threats facing the renewable energy sector.

The team would also like to acknowledge the invaluable contributions of Sandia National Laboratories and INL. The expertise and insights provided by the cybersecurity experts at these national laboratories were instrumental in shaping the blended reference architectures and the cyber-resilient design framework. The National Renewable Energy Laboratory (NREL) served as the project lead and coordinated the consortium activities.

The Project RESCue team would like to express their sincere gratitude to the U.S. Department of Energy's Cybersecurity Energy Security and Emergency Response office for their support and funding of this important initiative. The team is particularly appreciative of the guidance and involvement of the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy's Solar Energy Technologies Office and the Wind Energy Technologies Office.

The Project RESCue team and the report also benefited from the invaluable feedback and participation of the 45 industry stakeholders who attended the in-person meeting in February 2024. The Project RESCue pilot's success is a testament to the power of public-private partnerships and the dedication of all the individuals and organizations involved. The team looks forward to continuing this collaborative journey toward a more secure and resilient renewable energy future.

List of Acronyms

BESS	battery energy storage system
DMZ	demilitarized zone
IBR	inverter-based resource
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
NDA	nondisclosure agreement
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OEM	original equipment manufacturer
OT	operational technology
PV	photovoltaic
RESCue	Renewable Energy and Storage Cybersecurity Research
SCADA	supervisory control and data acquisition
SGU	single generating unit

Executive Summary

Project Renewable Energy and Storage Cybersecurity Research (RESCue) is a collaborative effort aimed at securing the rapidly growing deployment of transmission-connected hybrid renewable energy systems, consisting of a combination of wind, solar, and/or energy storage equipment, against escalating cyber threats. This project brings together major original equipment manufacturers (OEMs) of wind, solar, and energy storage, along with major asset owners and national laboratories, to collectively identify cyber threats, assess risks, and develop robust cybersecurity strategies and solutions.

The RESCue consortium has made significant progress in several key areas. The consortium has actively sought to expand its reach and diversify its membership, welcoming new members from the renewable energy industry and government agencies, further enriching the collective knowledge and capabilities of the group. The project team has worked on two primary research thrusts in its first year: (1) the development of reference architectures for hybrid renewable energy systems, and (2) a cyber-resilient design framework that quantifies the cyber resilience of the design and a companion application guide.

The development of hybrid reference architectures has provided comprehensive blueprints for the secure design and integration of hybrid renewable energy systems, accounting for their unique characteristics and interdependencies. Additionally, the National Renewable Energy Laboratory (NREL) has created a cyber-resilient design framework that integrates cybersecurity considerations from the start of the system life cycle, ensuring security is “baked in” from the initial design phase.

Looking ahead, the RESCue consortium is exploring exciting opportunities, such as expanding international collaboration, developing industry-specific guidelines and standards, investigating emerging technologies, and fostering stronger public-private partnerships. By capitalizing on these opportunities and continuing to grow its membership, the consortium aims to solidify its position as a leading force in securing hybrid renewable energy systems, ensuring the sustainable and resilient operation of these critical infrastructures.

Table of Contents

List of Figures

1 Introduction and Value Proposition

With over 3,000 utilities and hundreds of thousands of transmission lines and distribution feeders, there will inevitably be a wide range of designs for the electric grid in 2030. Of increasing interest is the combination of renewable resources (such as wind, solar) combined with energy storage to make them dispatchable, which is often referred to as ‘hybrid renewable energy system’. These constitute a growing share of the electricity mix in the United States (U.S Energy Information Administration n.d.). These hybrid systems have a wide range of configurations i.e., co-located vs. independent, virtual power plants, full vs. partial hybrids, etc., with specific cybersecurity challenges such as rapid communication between sub-components, rapid communication between hybrid system and grid, increased attack surface, interoperability of legacy and new equipment, and potential use of third-party components with unsecure supply chain (U.S. DOE 2021). With the aim to support the secure development of hybrid renewable energy systems inclusive of wind, solar, and energy storage, U.S. Department of Energy’s Cybersecurity, Energy Security, and Emergency Response office launched the pilot of Project Renewable Energy and Storage Cybersecurity Research (RESCue)—a multi-laboratory effort, led by the National Renewable Energy Laboratory, to analyze and address cybersecurity concerns for hybrid energy systems that include wind, solar, and energy storage.

Project RESCue aims to secure the rapidly growing deployment of transmission-connected hybrid renewable energy systems, including a combination of wind, solar, and energy storage, against escalating cyber threats. The project expands on wind cybersecurity consortium (Office of Energy Efficiency & Renewable Energy 2021), previously funded by DOE, to include solar and energy storage and invites original equipment manufacturers (OEMs) and owner-operators with renewable energy portfolios to share insights and feedback. It offers a collaborative platform where original equipment manufacturers (OEMs) of wind, solar, and energy storage, along with asset owners of renewable energy portfolios and national laboratories, can work together to identify cyber threats, assess risks, and develop effective cybersecurity strategies and solutions. This platform welcomes all OEMs and asset owners in the renewable energy sector, encouraging a diverse range of partners to participate and contribute their expertise.

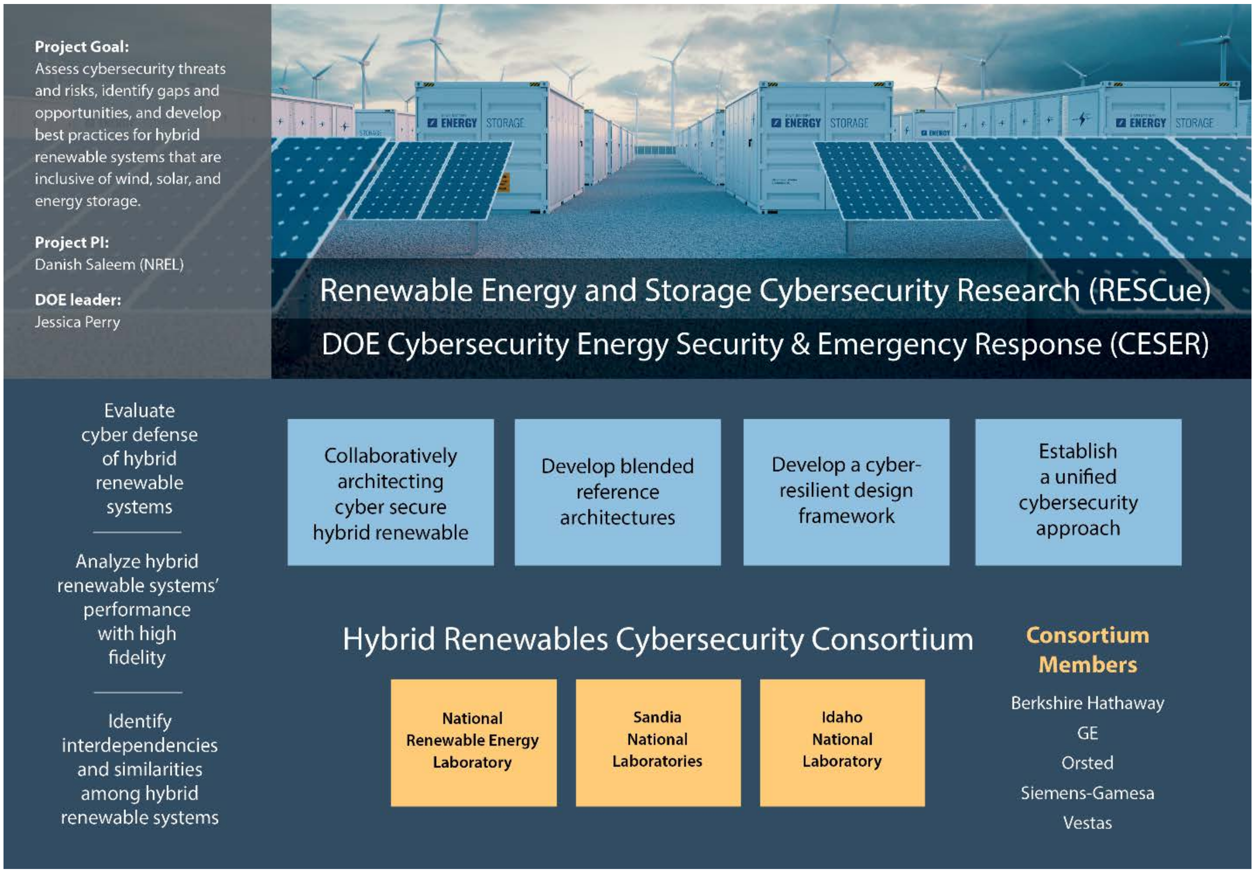
Project RESCue supports efforts in achieving strategic objective 4.4 of the White House’s National Cybersecurity Strategy (The White House 2023), that focuses on securing clean energy future, and underscores the importance of this initiative. During the pilot year, the following four major objectives were addressed:

- Establish consortium comprising of stakeholders from the wind, solar and energy storage industries to establish an ecosystem of information sharing and actionable intelligence gathering that could be used for improving the cybersecurity of hybrid renewable systems.
- Create a cyber-resilient design framework for hybrid renewable systems which considers design philosophies, design aspects, and design metrics.
- Develop modular reference architectures, such as cyber-physical models, for the common modes of installations of hybrid renewable systems such as for wind, solar and energy storage.
- Host an in-person workshop to share perspectives on the strengths and weaknesses, to help identify potential pathways for achieving robust cybersecurity defenses and

responses, and to provide viewpoint on what areas of publicly funded research and development would have the highest value for hybrid renewable energy systems.

Among these objectives, the project team has concentrated on following two primary research thrusts:

- Developing reference architectures for hybrid renewable energy systems
- Developing a cyber-resilient design framework that quantifies the cyber resilience of the design, accompanied by an application guide to aid implementation.



Project Goal: Assess cybersecurity threats and risks, identify gaps and opportunities, and develop best practices for hybrid renewable systems that are inclusive of wind, solar, and energy storage.

Project PI: Danish Saleem (NREL)

DOE leader: Jessica Perry

Renewable Energy and Storage Cybersecurity Research (RESCue)

DOE Cybersecurity Energy Security & Emergency Response (CESER)

Evaluate cyber defense of hybrid renewable systems

Analyze hybrid renewable systems' performance with high fidelity

Identify interdependencies and similarities among hybrid renewable systems

Collaboratively architecting cyber secure hybrid renewable

Develop blended reference architectures

Develop a cyber-resilient design framework

Establish a unified cybersecurity approach

Hybrid Renewables Cybersecurity Consortium

National Renewable Energy Laboratory

Sandia National Laboratories

Idaho National Laboratory

Consortium Members

Berkshire Hathaway

GE

Orsted

Siemens-Gamesa

Vestas

Figure 1. Overview of RESCue consortium—Source Anthony Castellano, NREL

Project RESCue helped foster collaborations with global industry leaders because they lend essential real-world insights into the most pressing gaps and threats. The current OEMs such as Vestas, GE, and Siemens-Gamesa supply a significant portion of the global offshore/onshore wind turbine market (Wilson, Adam. 2023). In terms of asset owners, Berkshire Hathaway Energy is one of the largest investor-owned utility in the United States with a significant clean power portfolio. The project team also had multiple discussions with SolarEdge, Enphase and Tesla to invite them for joining the RESCue consortium. As per Wood McKenzie Power and Renewables report released at the end of 2022 (Wood McKenzie 2022), these three OEMs, and prospective consortium members, cover more than 92% of the inverter market in the U.S. residential solar industry (US Residential Solar Inverter Market).

	2018	2019	2020	2021	2022
Enphase	19.3%	25.0%	41.4%	45.1%	44.7%
SolarEdge Technologies	51.6%	59.5%	51.3%	45.7%	43.0%
Tesla Energy	0.0%	0.0%	0.0%	3.6%	5.0%
SMA	3.9%	2.2%	2.3%	1.4%	3.3%
Delta Electronics	5.6%	2.4%	1.9%	2.1%	1.4%
APSystems	0.5%	0.8%	0.7%	0.5%	0.5%
Hoymiles	0.0%	0.0%	0.1%	0.2%	0.5%
Generac	0.0%	0.1%	0.2%	0.4%	0.4%
ABB	3.1%	0.5%	0.1%	0.1%	0.3%
LG Electronics	0.0%	0.0%	0.1%	0.3%	0.2%
All Others	16.0%	9.5%	1.9%	0.6%	0.6%

As the energy sector transitions toward a clean energy future with increasing integration of distributed energy resources and inverter-based resources (IBRs), new potential for cyber vulnerabilities is being introduced. Legacy software, interconnected devices, and unfettered supply chains pose significant cybersecurity risks that could lead to disruptions and compromise critical infrastructure. Project RESCue addresses these challenges through regular discussion and collaboration among consortium members and performing focused research and development to develop common cybersecurity solutions that could be quickly and easily deployed. By investing in Project RESCue, stakeholders can collectively strengthen the cybersecurity posture of hybrid renewable energy systems, safeguard critical assets, and enable a secure transition to a clean energy future, aligning with the National Cybersecurity Strategy’s objectives.

1.1 Impact of Project RESCue

Project RESCue hosted an in-person meeting in February 2024 in Washington, D.C., to share findings on the unique cybersecurity challenges faced by hybrid renewable energy systems. The meeting aimed to present research and development progress within Project RESCue, identify strategies for robust cybersecurity defenses, promote coordination for resilience and basic cyber hygiene, and gather industry feedback.

This meeting was attended by 45 industry stakeholders representing a wide array of expertise. Participants included subject matter experts from major wind and solar OEMs like Vestas, Siemens Gamesa, and GE, as well as asset owners such as NextEra Energy and Avangrid Renewables and operation and maintenance providers like EDF Renewables.

The meeting featured a panel presentation with participants from wind and solar OEMs, asset owner-operators like Berkshire Hathaway Energy, and national laboratory representatives from the National Renewable Energy Laboratory (NREL) and Idaho National Laboratory (INL). Discussions centered around current challenges facing the renewable energy industry, as well as specific challenges to the hybrid renewable energy systems industry. The meeting also served as a platform to identify future research directions aimed at improving the cybersecurity posture for the entire industry.

A comprehensive workshop report summarizing the key takeaways and findings from this meeting has been compiled and is available for further reference (https://www.nrel.gov/docs/fy24osti/90220.pdf).

The consortium has actively sought to expand its reach and diversify its membership base. Over the past year, five additional renewable energy companies and one international government agency participated in the consortium meetings (on a non-NDA basis, with their NDAs still being processed) bringing fresh perspectives and expertise.

The influx of new members has enhanced the consortium’s collective knowledge and capabilities, fostered the cross-pollination of ideas, and enabled more comprehensive and multidisciplinary approaches to cybersecurity issues.

As the consortium moves forward, several exciting opportunities for future work and growth have emerged:

- Expanding international collaboration: Establishing partnerships with international organizations and consortia to facilitate global knowledge sharing and align on best practices for securing hybrid renewable energy systems across different regions and regulatory environments.
- Developing industry-specific guidelines and standards: Leveraging the consortium’s collective expertise to develop industry-specific guidelines, standards, and certification frameworks tailored to the unique requirements of hybrid renewable energy systems.
- Exploring emerging technologies: Investigating the cybersecurity implications of emerging technologies, such as distributed energy resources, smart grid systems, and advanced control systems, to stay ahead of potential threats and ensure the resilience of hybrid renewable energy infrastructures. These are also being addressed by several other Cybersecurity Energy Security and Emergency Response programs, and it is important that these efforts inform each other.
- Fostering public-private partnerships: Strengthening collaborations with government agencies and regulatory bodies to align cybersecurity efforts, share threat intelligence, and develop comprehensive policies and initiatives to safeguard critical energy infrastructures.

By capitalizing on these opportunities and continuing to expand its membership base, the RESCue consortium can further solidify its position as a leading force in securing hybrid renewable energy systems, ensuring the sustainable and resilient operation of these vital infrastructures.

2 RESCue Consortium Structure

As stated earlier, Project RESCue convenes diverse experts to advance cybersecurity research for distributed energy and hybrid renewable energy systems to strategically meet renewable sector cybersecurity needs while enabling innovation and adoption. Figure 2 shows an overview of how partners are added to the consortium. The last step in the process is the nondisclosure agreement (NDA). In the context of Project RESCue, the NDA refers to an agreement that governs the sharing of sensitive information among RESCue partners but does not preclude participation in the collaborative work itself. The NDA structure is particularly important to facilitating open discussions between entities that are typically placed in a competitive environment and ensuring that the consortium works for the betterment of the sector as a whole. The NDA discussions have informed several of the research priorities for the project and have resulted in the production of a classified report for the members of the consortium, informing them of the cyber threat landscape for the sector. In addition, the discussions from the annual workshop have also resulted in a report summarizing future research and development needs for the sector (https://www.nrel.gov/docs/fy24osti/90220.pdf).

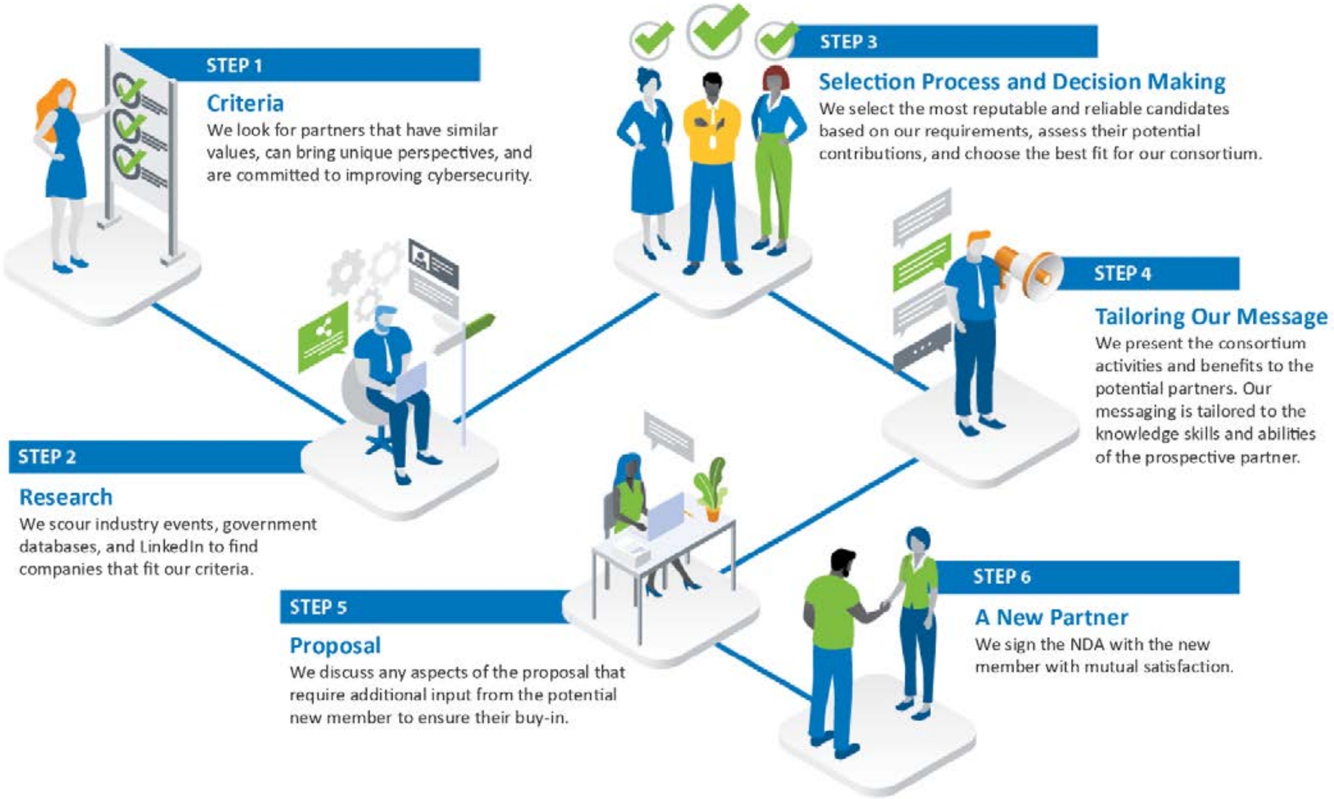

STEP 1
Criteria
We look for partners that have similar values, can bring unique perspectives, and are committed to improving cybersecurity.
STEP 2
Research
We scour industry events, government databases, and LinkedIn to find companies that fit our criteria.
STEP 3
Selection Process and Decision Making
We select the most reputable and reliable candidates based on our requirements, assess their potential contributions, and choose the best fit for our consortium.
STEP 4
Tailoring Our Message
We present the consortium activities and benefits to the potential partners. Our messaging is tailored to the knowledge skills and abilities of the prospective partner.
STEP 5
Proposal
We discuss any aspects of the proposal that require additional input from the potential new member to ensure their buy-in.
STEP 6
A New Partner
We sign the NDA with the new member with mutual satisfaction.

Figure 2. Steps to add partners to the consortium

Through a coordinated consortium, the project leverages advanced research and development to:

- Identify the common cybersecurity fundamentals for hybrid renewable energy systems
- Develop blended reference architectures that enable baselining of cyber risk and operation from a shared understanding of the cybersecurity posture
- Develop a cyber-resilient design framework capable of quantifying the cyber resilience of a particular hybrid renewable energy system design
- Establish best practices, guidelines, and tools for improving cybersecurity across the hybrid renewable energy ecosystem, from design to operations
- Foster public-private collaboration, knowledge sharing, and coordinated response planning to collectively defend critical energy infrastructure.

2.1 Identification of Common Cyber Fundamentals for Utility-Owned IBR Systems

IBRs are crucial components in various utility systems, especially in renewable energy generation such as solar wind power and energy storage. Ensuring the cybersecurity of these resources is paramount to maintaining the integrity, availability, and confidentiality of data related to the energy grid. Listed below are some common cybersecurity fundamentals applicable to different utility-owned IBRs. These were determined and agreed upon by RESCue consortium members during virtual and in-person discussions over the last one year. These cybersecurity fundamentals are supported by several key standards and frameworks, including:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST 2024)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations (NIST 2020)
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC): ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection—Information security controls. (ISO and IEC 2022)
- NIST SP 800-161: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST 2022)
- North American Electric Reliability Corporation: Critical Infrastructure Protection Reliability Standards (North American Electric Reliability Corporation. n.d.)
- The International Society of Automation (ISA) and International Electrotechnical Commission (IEC): ISA/IEC 62443 Series of Standards
- DOE Office of Cybersecurity, Energy Security, and Emergency Response: Cybersecurity Capability and Maturity Model (C2M2) (DOE Office of Cybersecurity, Energy Security, and Emergency Response 2022)
- Institute of Electrical and Electronics Engineers (IEEE) Standards Association: 1547-2018: IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. (IEEE Standards Association 2018).

These documents provide comprehensive guidance and best practices for implementing robust cybersecurity measures across various aspects of utility-owned IBR systems.

2.1.1 Access control and authentication

- Multifactor authentication: Multifactor authentication requires additional verification beyond a simple username and password to access IBR systems. This can include fingerprint scanners, security tokens, or one-time codes.
- Least-privilege principle: Granting users only the access level required for their specific role minimizes the potential damage caused by compromised credentials.
- Regular password rotation: Enforcing frequent password changes helps maintain the security of IBR systems.
- Implementing robust access control mechanisms, such as role-based access control and multifactor authentication, ensures that only authorized personnel can access and manage the IBR systems.

- Establishing secure communication channels and encrypted protocols for remote access and maintenance activities.

2.1.2 Data security

- Encrypting sensitive data both at rest and in transit. Utilize encryption protocols to protect data transmission between IBRs and other components of the utility system. This ensures that data exchanged between IBRs, and control systems cannot be intercepted or tampered with by unauthorized entities.
- Data backups: Regularly backing up critical data ensures its availability in case of system outages or cyberattacks.
- Data loss prevention: Data loss prevention solutions can help prevent sensitive information from being accidentally or intentionally shared outside the organization.

2.1.3 Network security

- Firewalls: Firewalls act as barriers between IBR systems and the internet, filtering incoming and outgoing traffic based on predefined security rules.
- Intrusion detection/prevention systems: These systems monitor network activity for suspicious behavior and can take actions to block potential attacks.
- Regular security patching: Keeping IBR systems and software up to date with the latest security patches helps address known vulnerabilities.
- Network segmentation: Segmenting IBR networks from other operational networks and the internet help minimize the attack surface and potential lateral movement of threats.

2.1.4 Firmware and software updates

- Ensure that firmware and software updates for IBRs are obtained from trusted sources and are thoroughly tested and validated before deployment.
- Patch management: Maintain an effective patch management process to promptly address security vulnerabilities in IBR software and firmware. Regularly update IBR systems with patches and security updates to mitigate the risk of exploitation by cyber threats.
- Implement secure update processes, including digital signatures and integrity checks, to prevent unauthorized modifications.

2.1.5 Secure configuration management

- Establish and maintain secure configurations for IBRs, including disabling unnecessary services, ports, and protocols
- Implement configuration management processes to ensure that changes are properly reviewed, tested, and documented.

2.1.6 Logging and monitoring

- Enable comprehensive logging and monitoring capabilities for IBRs to detect and respond to potential security incidents or anomalous behavior
- Integrate logs with centralized security information and event management systems for analysis and correlation.

2.1.7 Incident response

- Security incident and event management: Security information and event management tools aggregate data from various security sources to provide a centralized view of potential security incidents.
- Developing and testing predefined plans for responding to security incidents helps organizations minimize damage and restore normal operations quickly. This should include procedures for containment, eradication, and recovery.
- Ensure that backup and recovery mechanisms are in place to restore IBR systems to a known good state in the event of a security breach or failure.
- Regular security awareness training: Educating employees about cybersecurity best practices can help them identify and avoid social engineering attacks and phishing attempts.
- Identifying roles and responsibilities for various stakeholders helps to ensure a coordinated incident response.

2.1.8 Supply chain risk management

- Assess and manage supply chain risks associated with IBRs, including thorough vetting of vendors, secure software development practices, and vulnerability management processes
- Implement stringent cybersecurity requirements in vendor contracts and partnerships to ensure that IBR suppliers adhere to industry best practices and security standards.

2.1.9 Security awareness and training

- Provide regular security awareness training to personnel involved in the operation and maintenance of IBRs, covering topics such as cyber threats, secure practices, and incident reporting procedures
- Educate employees about common cyber threats, phishing attacks, and best practices for securely managing IBR systems to mitigate the risk of human error and insider threats
- Foster a culture of security awareness and promoting the adoption of secure behaviors throughout the organization.

2.1.10 Additional considerations

- Defense in depth security: A layered security approach is vital. This involves combining various security measures like access control, network segmentation, and intrusion detection to create a comprehensive defense against cyberattacks.
- Physical security of inverters: Physical access to inverters should be restricted and monitored to prevent unauthorized tampering.
- Compliance with regulations: Utility-owned IBRs might be subject to specific industry regulations regarding cybersecurity for inverter-based systems.
- Standards and best practices: Developing cybersecurity standards, recommendations, and best practices for IBRs ensures secure design and deployment.
- Certification and testing: Implementing cybersecurity certification testing procedures helps identify gaps and mandate secure features at the device, network, and system levels.
- Collaborative efforts: Participate in stakeholder committees and working groups to advance cybersecurity guidelines and share knowledge across the industry.

- Continuous improvement: Stay informed of cybersecurity developments and updating practices to address dynamic threats and evolving industry needs.

3 Hybrid Reference Architectures

The RESCue consortium's effort to develop reference architectures for hybrid renewable energy systems has yielded a comprehensive set of architectural diagrams that explicitly define the interdependencies and similarities among various system configurations. These reference architectures help guide stakeholders in the secure design, deployment, and operation of hybrid systems while accounting for their unique characteristics and integration challenges.

Sandia National Laboratories played a crucial role in the development of blended reference architectures. Their team of experts contributed extensive knowledge and experience in cybersecurity for energy systems, focusing on identifying and mitigating potential cyber risks and vulnerabilities. Their work was seamlessly integrated into the consortium's efforts, ensuring that the reference architectures incorporated robust security measures from the ground up.

The blended reference architectures have received positive feedback from consortium members. Industry partners have appreciated the comprehensive approach, the attention to detail, and the consideration given to real-world operational challenges. Other feedback has commended the architectures' modularity and scalability, enabling further research and adaptation into emerging technologies.

To validate the effectiveness of the blended reference architectures, the research teams conducted several demonstrations across different environments and system configurations. The feedback from these demonstrations has been valuable in highlighting areas for refinement and confirming the architectures' applicability in practical settings.

3.1 Approach

The hybrid energy systems considered in this effort consist of more than one generation asset and some amount of energy storage, which are co-located behind a single point of interconnection. They are operated and/or coordinated to appear as a single resource to a system operator and incorporate controls to manage the output across multiple resources to the system owner (Hybrid Resources Task Force 2022). Project RESCue developed reference architectures for the common modes of installations for the three types of hybrid renewable energy systems: wind turbine and wind plant systems, PV installations and PV power plants, and battery energy storage systems (BESS).

The team performed a survey of existing hybrid energy systems to understand the existing state of hybrid power plant design and configuration, information and operational technology (OT) device communication, and cybersecurity solutions integration between solar, wind, and BESS. Understanding and enumerating the hybrid energy system devices, interconnections, and hybrid energy market was imperative to creating accurate, representational reference architectures.

The reference architectures are designed to be modular to support multiple configurations of varying scales of renewable energy assets to study their effects on the wider power grid. The architectures consist of modular components, including stand-alone power plants, renewable energy generating units, and communication models. The team also created a reference architecture template and comprehensive list of components and protocols to design and understand different hybrid renewable energy systems.

The components in the reference architectures are divided into functional, technological, and cybersecurity devices. Functional devices include the main components in the systems such as solar arrays, power converters, and battery management systems. Technological devices are the components that support digital communication and data collection such as data servers, monitoring systems, and cloud services. Cybersecurity devices are security solutions such as intrusion detection systems, hardened network taps, and firewalls. It is important to consider all three types of components, as they exist in and serve different roles in a hybrid energy power plant.

The communication between the components in the energy systems is complicated and can vary depending on the design and configuration of the system. The reference architecture components are connected via blue or red lines. Blue lines denote digital communication, and red lines denote power connections. The list of components expands upon the types of communication protocols each component could support. Using the reference architecture diagrams and the list of components will allow users to understand what each device does and how it can be connected and communicate with other devices in the system.

3.2 Hybrid Reference Architecture Templates

Hybrid power plants are designed and configured in multiple ways depending on the existing infrastructure, use case, and energy market. Each template assumes the generating assets are in the same geographical location. This effort focuses on fully integrated, co-located, and supplemental configurations (Petersen et al. 2018).

A fully integrated hybrid renewable energy system integrates all assets into operating as a single power plant from the grid’s perspective (Figure 3). All assets have individual points of connection and are connected to the same substation. The substation is the point of interconnection between the hybrid renewable energy plant and the grid. A global hybrid power plant controller aggregates individual assets. The point of common coupling is usually DC-coupled. Assets may be wind, solar, or BESS.

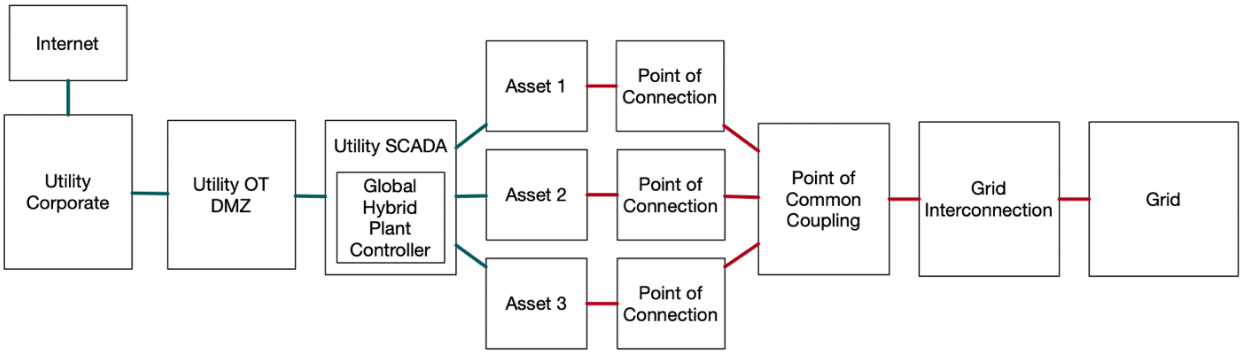


Figure 3. Fully integrated hybrid renewable energy system template

SCADA = supervisory control and data acquisition; DMZ = demilitarized zone

A co-located hybrid renewable energy system (Figure 4) has assets that operate more independently and have their own set of components such as inverters, controllers, and connection infrastructure. Each asset may be designed, configured, and operated (bid into markets) more independently. The point of common coupling may be AC- or DC-coupled. An energy management system will aggregate each asset's controller data to determine operational decisions; however, a main power plant controller would not be present, as the systems operate more independently. Assets may be wind, solar, or BESS.

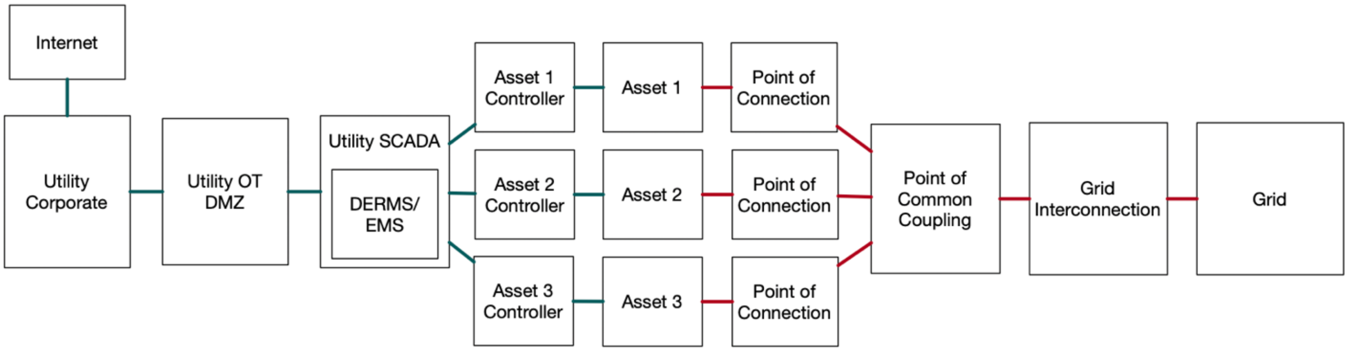


Figure 4. Co-located hybrid renewable energy system template

DERMS = distributed energy resource management system; EMS = energy management system

The supplemental hybrid reference architecture template in Figure 5 illustrates a configuration in which Asset 1 is the main generational asset. Asset 1 is commonly seen as a wind asset, and Asset 2 and/or 3 may be solar and/or BESS. Assets 2 and 3 act as supplemental or supportive assets and must leverage the existing power conversion equipment in Asset 1. One controller is in Asset 1; the controller must contain functionality to control all assets. If the combination of Assets 1, 2, and 3 are scaled to multiple systems in the configuration below, additional control components must be added to the system.

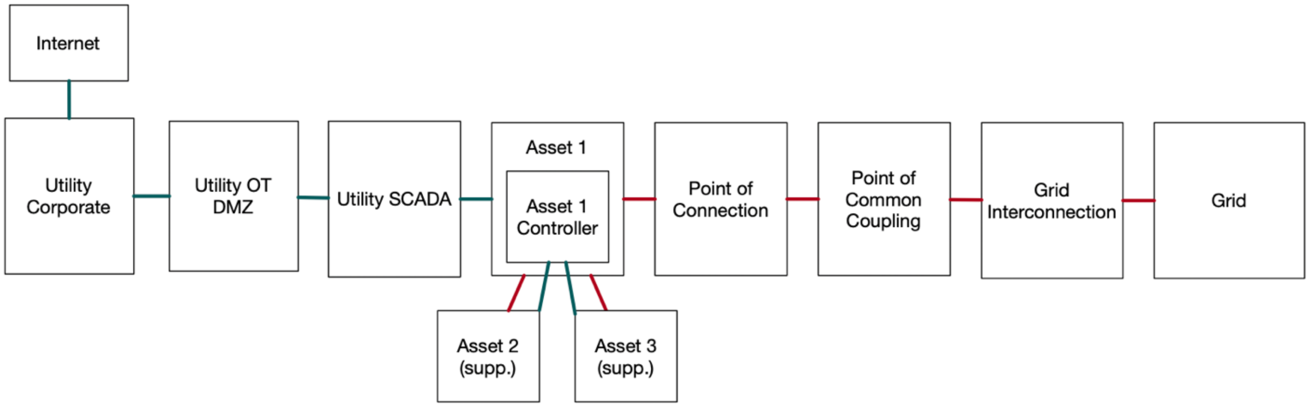


Figure 5. Supplemental hybrid renewable energy system template

3.3 Reference Architecture Diagrams

The consortium developed seven reference architectures, including hybrid renewable energy system, wind, solar, and BESS power plants, and wind, solar, and BESS single generating units (SGUs). The power plant reference architectures for hybrid and renewable energy assets are designed to be stand-alone. The SGU reference architectures are modular to allow for integration into the three templates outlined in the previous section.

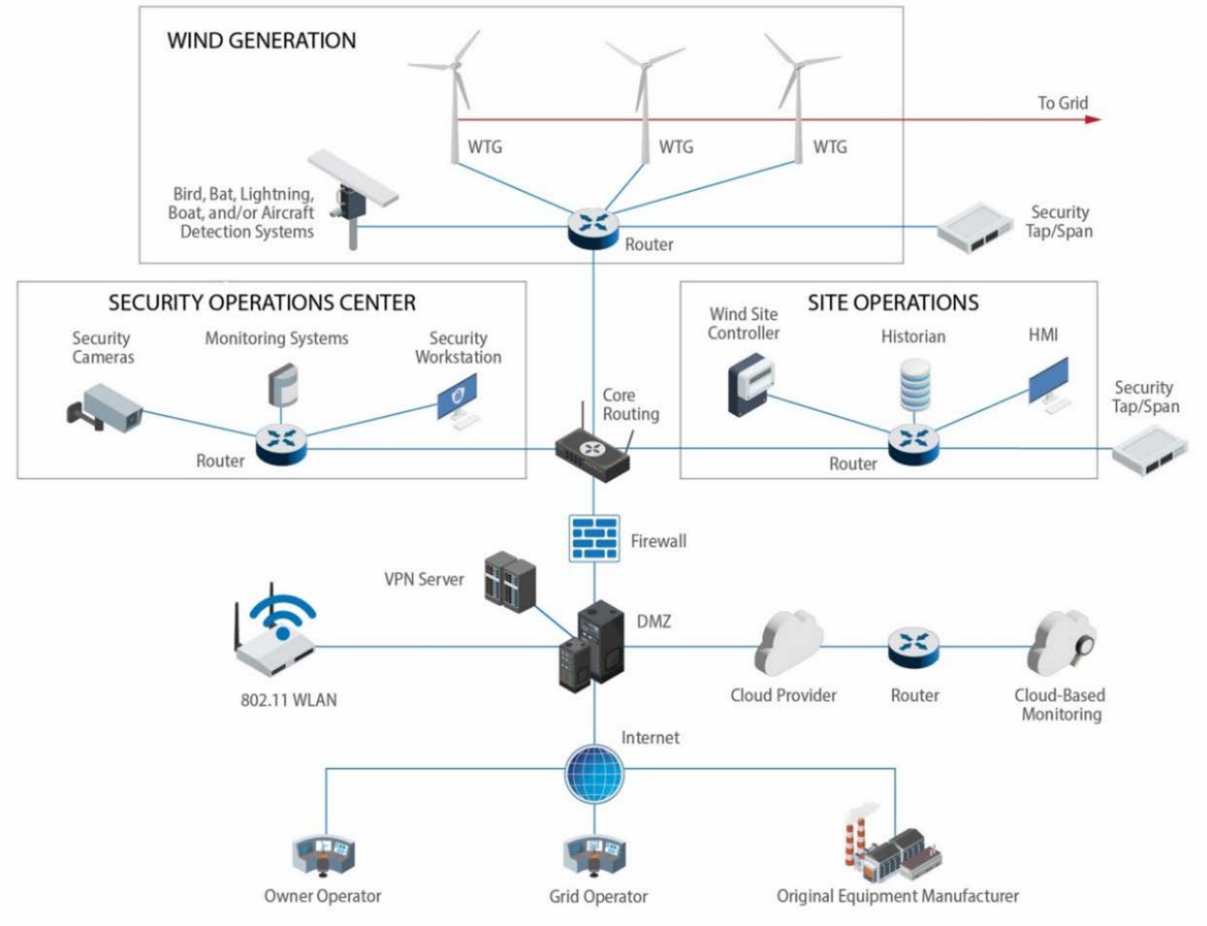


Figure 6. Wind power plant reference architecture

The wind power plant and SGU, in this case representing a wind turbine, were derived from SNL's and INL's wind cyber-hardening project and NREL's wind turbine reference architecture project (Johnson et al. 2023). These existing reference architectures were modified to capture the integration details seen in hybrid power plants.

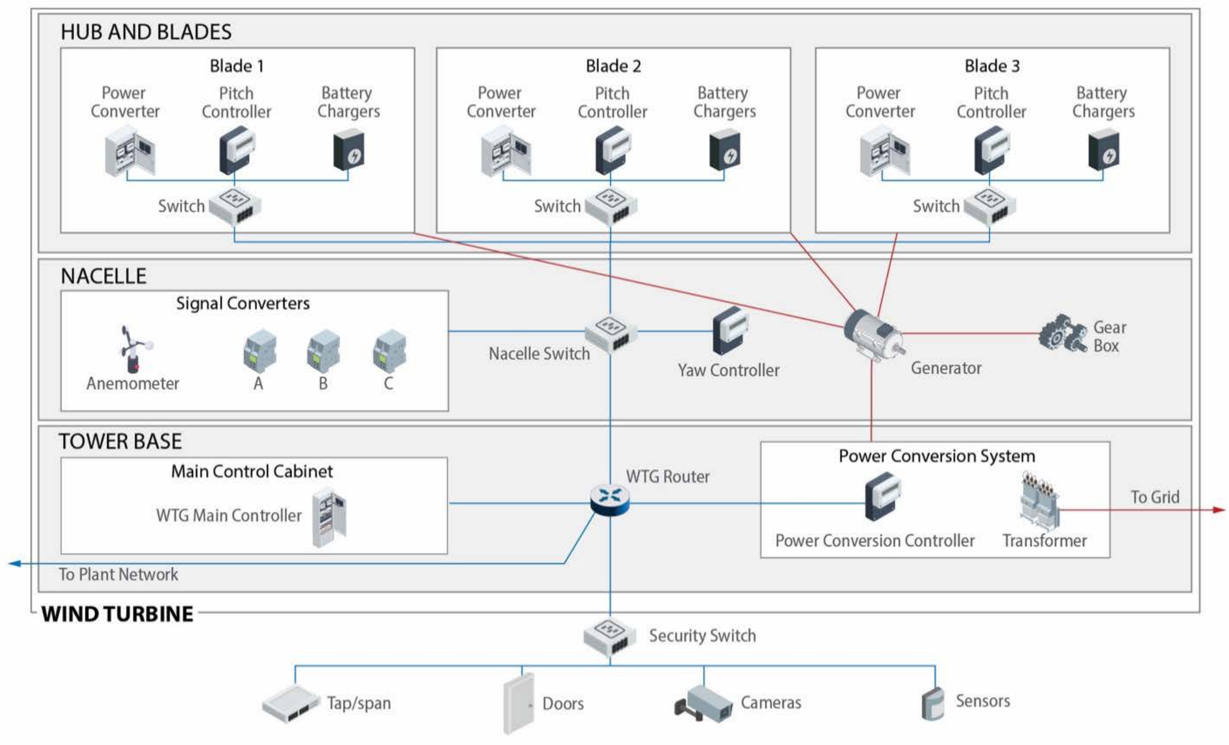


Figure 7. Wind turbine reference architectures

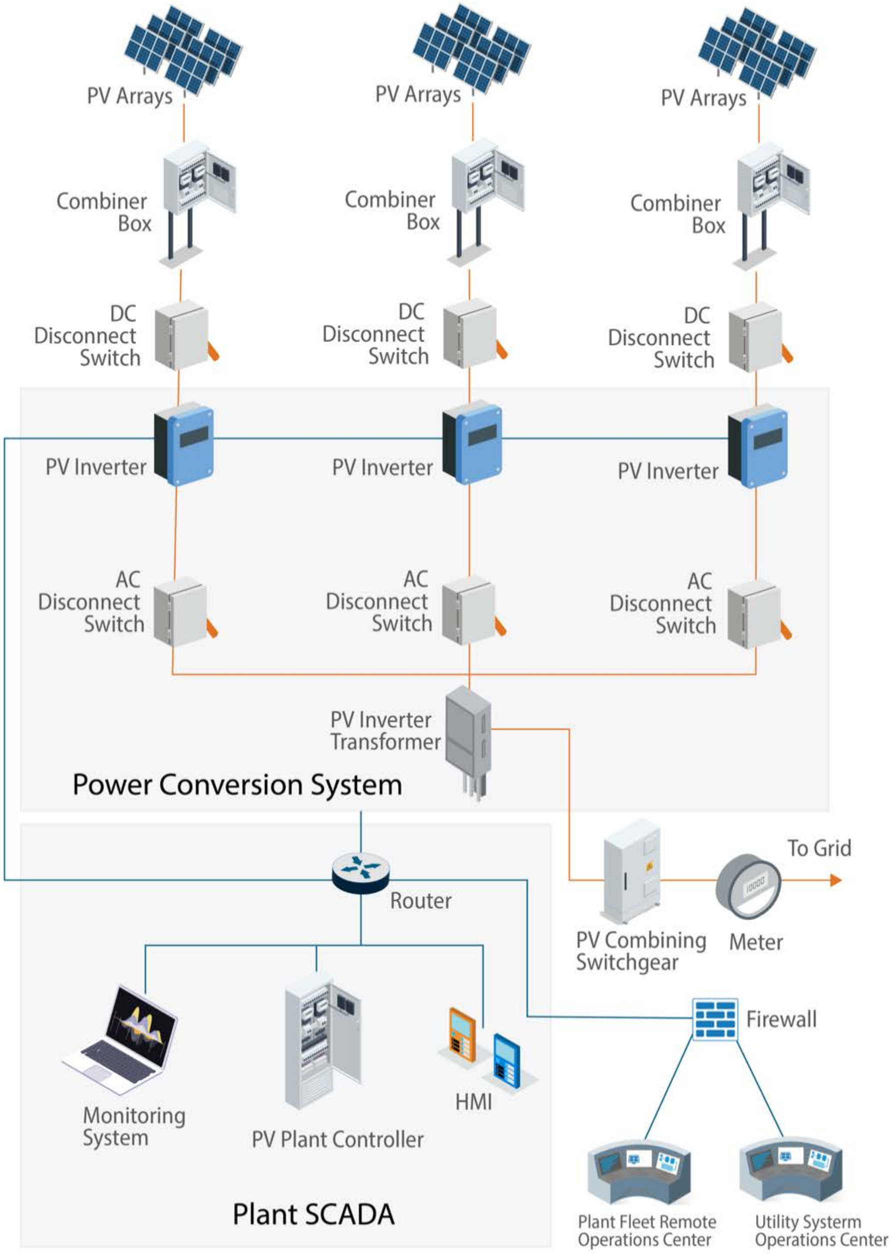


Figure 8. Solar power plant reference architectures

The solar power plant reference architecture illustrates how a solar PV plant SCADA system hosting a controller, monitoring systems, and human machine interface communicates to the PV inverters, power conversion system, grid infrastructure, and operations centers. The solar asset SGU is designed to be placed in a hybrid system between the plant network, which will be hosting a global plant controller or a PV controller and the grid.

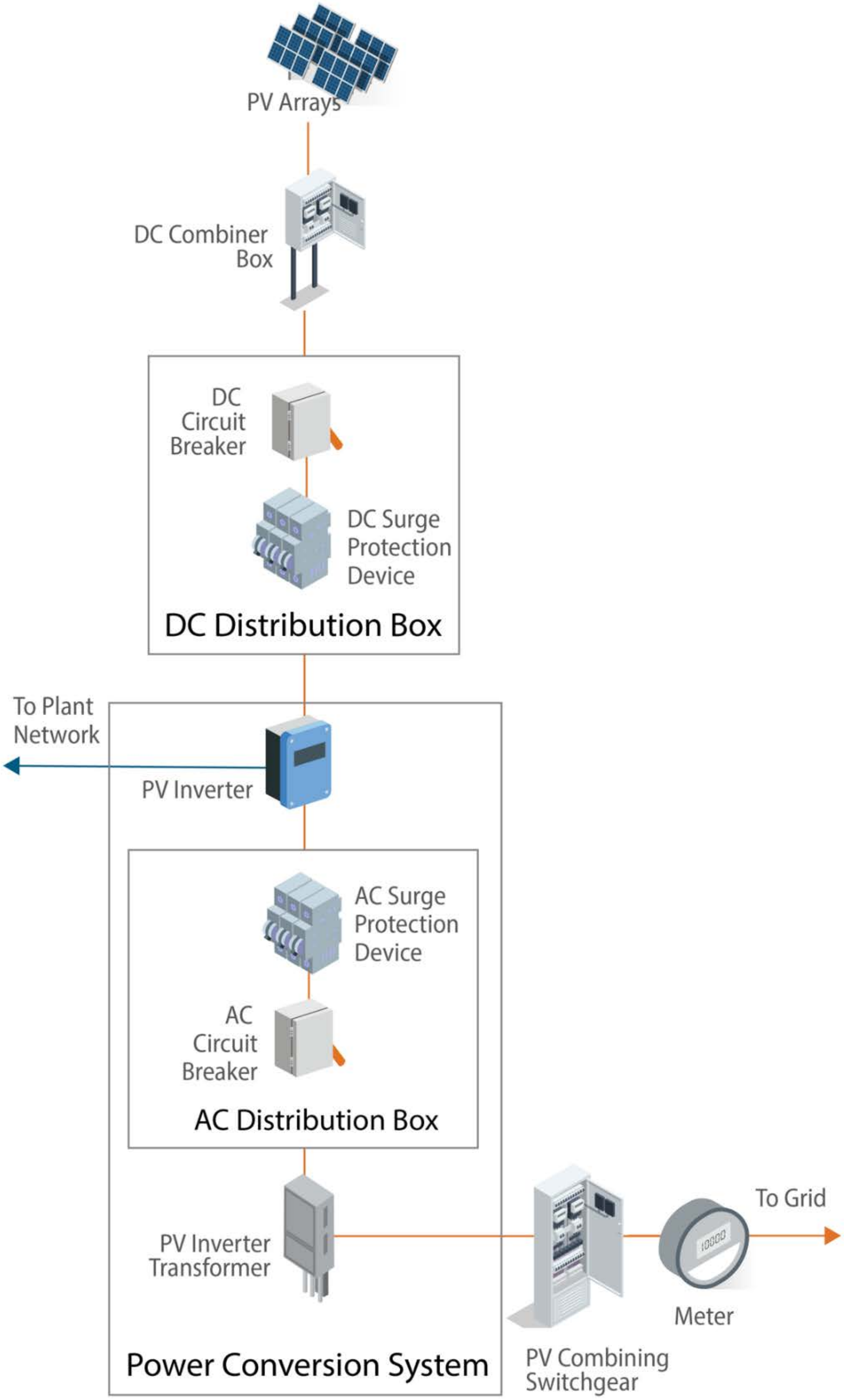


Figure 9. Solar single generating unit reference architecture

The BESS plant and SGU include an environmental control system, which is unique to energy storage. Concerns exist over DC arcs and the safety of battery storage, due to the safety hazards with the materials. A battery management system is unique to this infrastructure, as it controls the battery modules and sends the data to a battery controller and/or energy management system. The BESS power plant is a stand-alone design to be operated more independently, whereas the SGU is designed to be integrated into a hybrid plant as a supplemental or integrated asset.

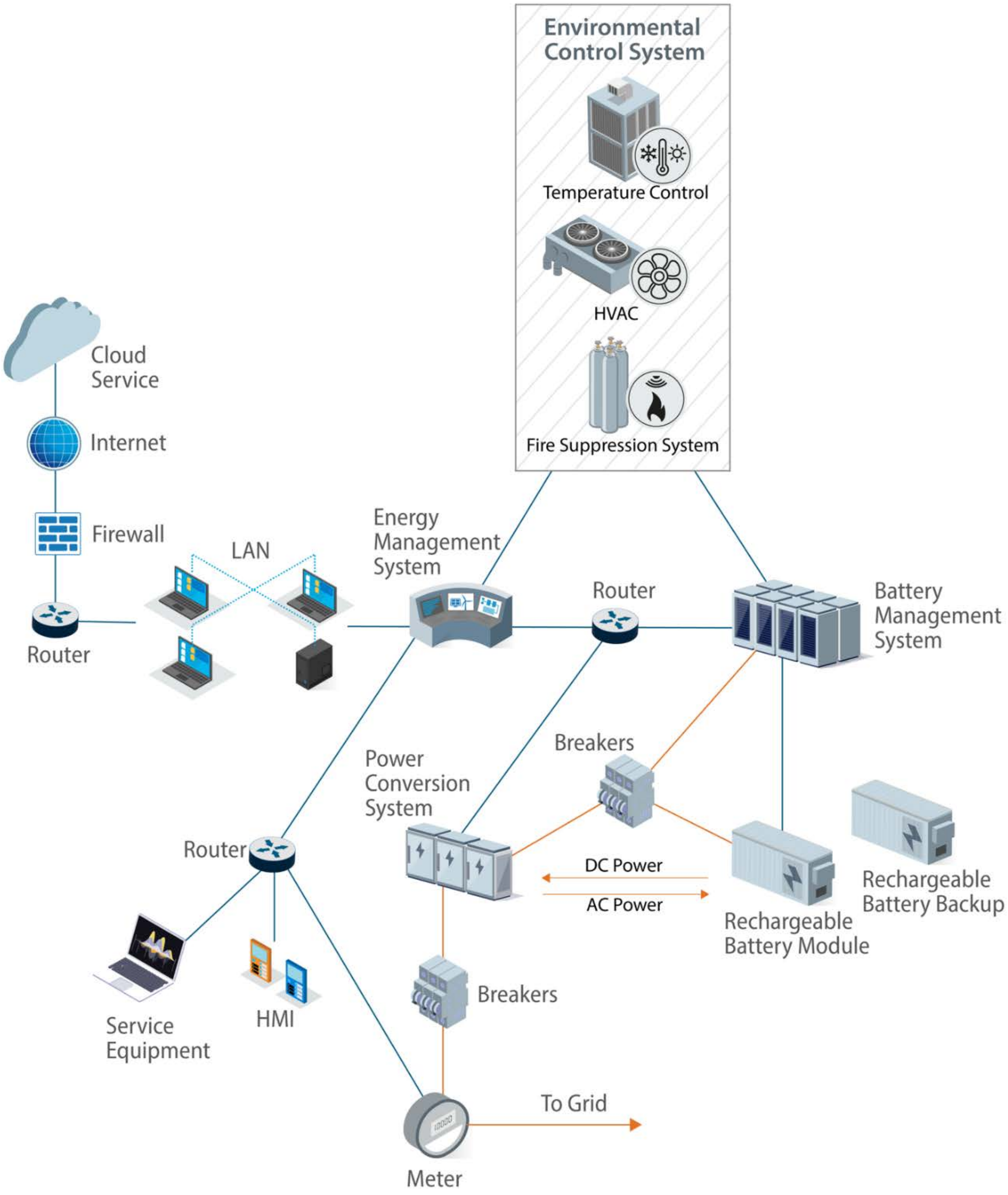


Figure 10. BESS plant reference architectures

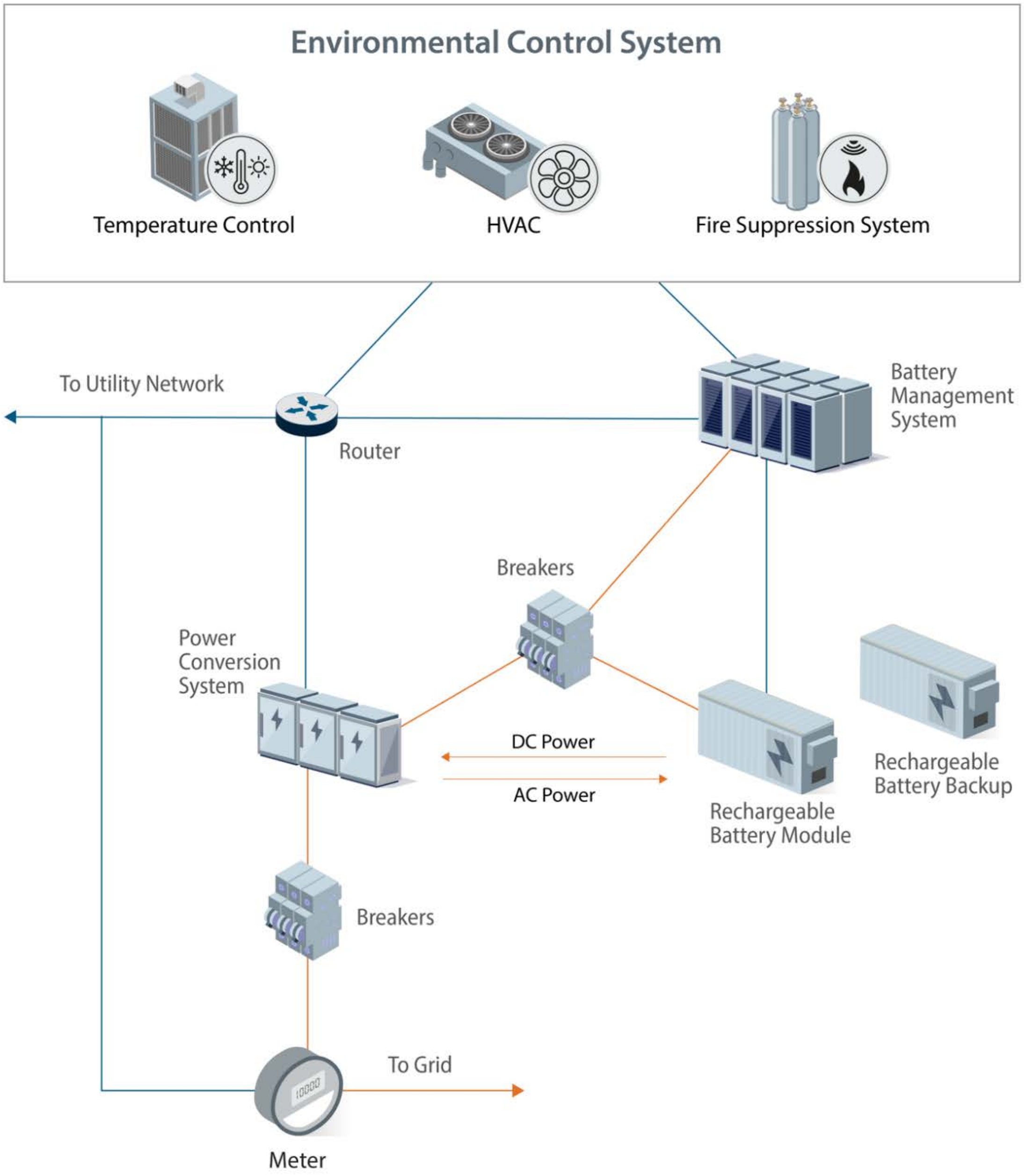


Figure 11. BESS single generating unit reference architectures

The hybrid power plant reference architecture illustrates the utility network and devices that aggregate, analyze, and inform system owners and operators of the status of the hybrid power plant. This power plant shows a version of a co-located hybrid power plant, as each system has its own controller that sends data to an energy management system and a main controller.

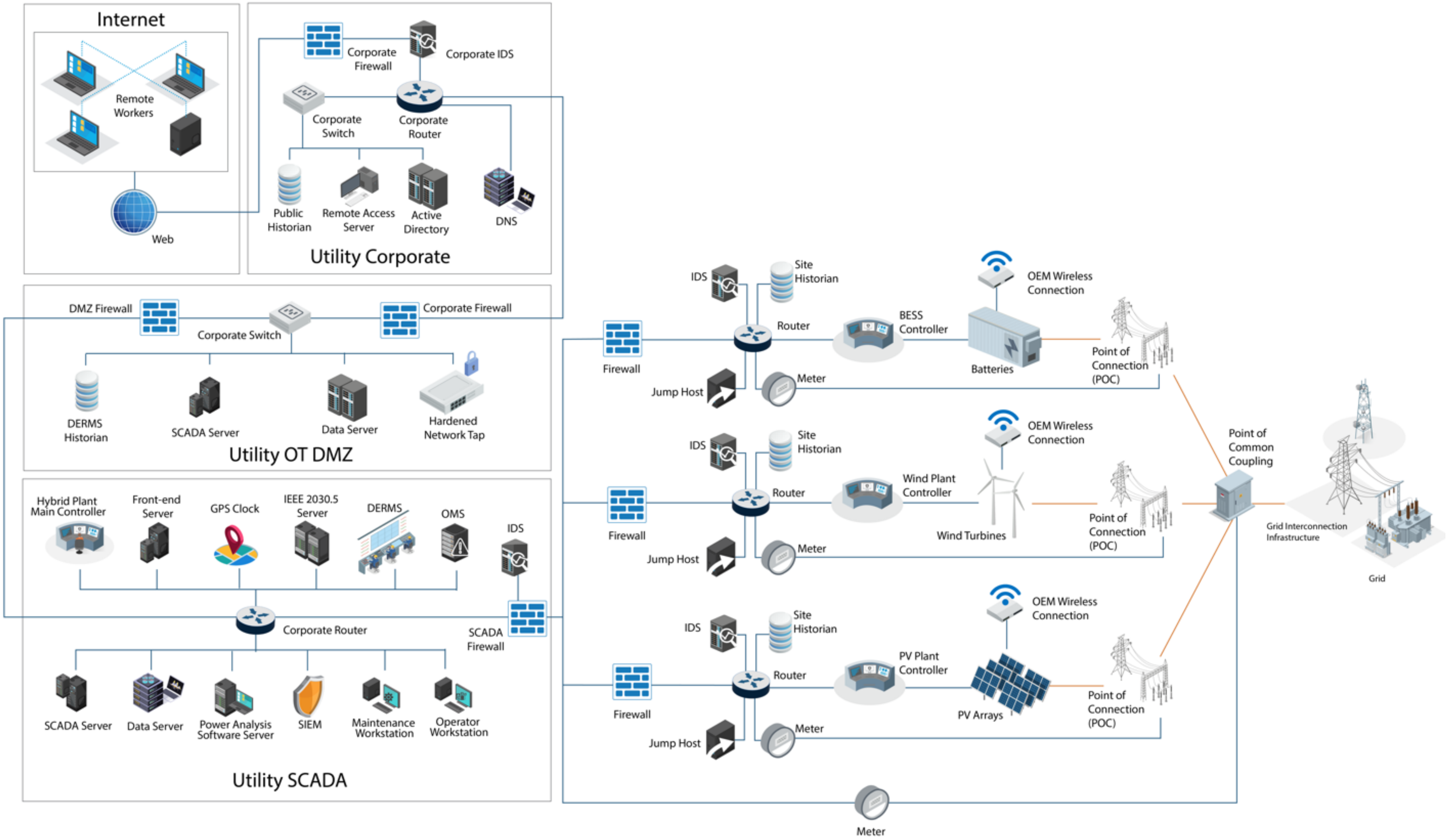


Figure 12. Hybrid co-located power plant reference architecture

The uniqueness of solar, wind, and BESS contribute to identifying how each system would integrate into a hybrid power plant. Each generating asset requires specific infrastructure that may or may not be able to be shared. The hybrid reference architecture and templates help distinguish different designs and configurations of assets and digital components.

3.4 List of Components

Every device, system, and component represented in the reference architecture diagrams was enumerated into a main list that includes a description and the communication protocols each may support. This list is intended to provide additional information about the reference architectures and enable the user to create customized architectures for their specific use case.

3.5 Simulation Model

The simulation model was developed by building on an existing standard power system model and developing a simple emulated system topology to deploy the developed reference architecture and evaluate various resilience scenarios. A system topology and scenario description in the form of configuration files for phenix were developed for deployment and demonstration on the NREL Cyber Range. The standard power model selected on which to build these scenarios was an IEEE 13Bus model running in OpenDSS, with the addition of storage elements and other such devices as dictated by the reference architecture or scenario. Emulated OT-Sim devices were configured to represent specific power system elements in accordance with both the source IEEE model and the designed reference architecture.

3.6 RESCue Consortium Feedback

NREL and SNL presented the blended reference architectures to the RESCue consortium members to gather industry feedback and facilitate discussion. Key topics included the integration and positioning of cybersecurity solutions, comparisons to other hybrid energy power plants, and the methods for remote access by vendors and OEMs.

A primary challenge in developing the reference architectures was determining the positioning of cybersecurity solutions for securing hybrid energy power plants. The discussion focused on whether to place a local security operations center (SOC) on-site or off-site and explored the use of security-as-a-service products, such as hardened network taps provided by OT cybersecurity vendors. The conversation also analyzed the attack surface of hybrid renewable energy systems. It was noted that read-only cybersecurity solutions, which depend on third-party cloud services for data analysis, do not increase the attack surface and benefit from the cloud's larger compute power for analysis. However, monitoring Internet-of-Things devices, such as temperature sensors in BESS, presents challenges, as these out-of-band network devices might not be within the SOC's direct monitoring capabilities.

The RESCue consortium compared hybrid power plants, including those using hydrogen and storage assets, with the hybrid renewable energy architectures presented. Development of tools for sizing generation assets, planning capacity, and optimizing schedules was highlighted to support the design and configuration of hybrid energy systems. These systems can operate independently, providing all necessary power, or serve as supplemental generating assets to improve existing energy sources. As a result, various configuration possibilities with hybrid renewable architecture templates and single generating units for wind, solar, and BESS to represent different configurations of generating assets in current and future hybrid power plants were developed.

Remote access to hybrid renewable energy systems for both stand-alone plants and hybrid plants was another discussion point. Direct remote access by vendors and OEMs for wind, solar, and BESS is typically achieved through cellular modems or wireless access. However, vendors expressed reluctance to use jump hosts and utility-provided security for system access.

The presentation of the hybrid reference architecture work to the RESCue consortium demonstrated that reference architectures are essential to designing and studying hybrid renewable energy systems to improve efficiency and security of the energy transformation. In response to the RESCue consortium feedback, hardened security network taps were incorporated throughout the reference architectures and wireless communication points were added for OEMs to connect directly to their renewable energy assets.

4 Cyber-Resilient Design Framework

Cyber resilience is essential for the reliable operation of critical energy systems. To address this need, the consortium developed a cyber-resilient design framework. This framework is a tool for system designers to use when considering the cyber resilience of their system from the initial design phase. It provides a structured approach to integrating cybersecurity considerations throughout the entire system life cycle, ensuring that security is baked in from the start rather than treated as an afterthought.

The development of the cyber-resilient design framework consisted of several steps, shown below, each addressing a critical aspect of securing hybrid renewable systems.

4.1 Identifying Key Challenges in the Design of Hybrid Systems

The consortium employed a comprehensive, multifaceted approach to thoroughly examine the unique challenges and operational requirements inherent in the design of hybrid systems. This systematic process involved a combination of literature review, expert consultation, and in-depth analysis of real-world case studies. Through this rigorous investigation, eight distinct challenges were identified, each with its own specific implications for the design, operation, and maintenance of hybrid systems. These identified challenges were then validated and refined through feedback and input from the diverse expertise within the RESCue consortium, ensuring a comprehensive understanding of the complexities involved in hybrid system design.

4.2 Identifying Existing Design Best Practices and Design Parameters for Hybrid Systems

Recognizing the limited availability of specific guidance tailored to the unique complexities of hybrid systems, the consortium conducted a comprehensive review of existing frameworks, standards, and best practices. This in-depth analysis focused on identifying relevant principles and approaches for incorporating cyber resilience into the architectural design of cyber-physical systems, with a particular emphasis on their applicability to hybrid energy systems. Key resources included NIST's Cyber Resilience Engineering Framework (CREF), which provides a structured approach to managing cybersecurity risks throughout the system life cycle; the U.S. Department of Energy's Cyber-Informed Engineering (CIE) initiative, which promotes the integration of cybersecurity considerations into the engineering design process; and the Cybersecurity and Infrastructure Security Agency's Secure by Design principles, which advocate for building security into products and systems from the earliest stages of development. These three frameworks were adapted to derive a cyber-resilient design framework for hybrid energy systems by deriving principles that are directly applicable to address the challenges from Step 1. Based on these principles, the consortium formulated a set of design "aspects," tangible parameters of the hybrid energy system on which the system designer makes decisions. The overall design framework is shown in Figure 13.

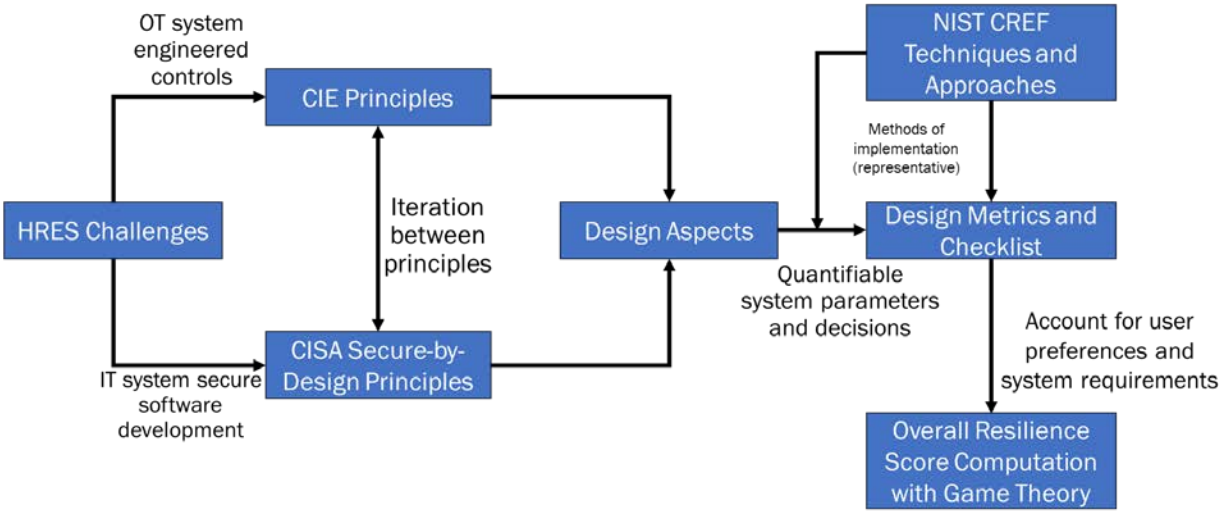

OT system engineered controls
CIE Principles
NIST CREF Techniques and Approaches
Methods of implementation (representative)
Iteration between principles
HRES Challenges
Design Aspects
Design Metrics and Checklist
Quantifiable system parameters and decisions
Account for user preferences and system requirements
CISA Secure-by-Design Principles
IT system secure software development
Overall Resilience Score Computation with Game Theory

Figure 13. Proposed cyber-resilient design framework for hybrid renewable energy systems (HRES).

NIST CREF = National Institute of Standards and Technology Cyber Resiliency Engineering Framework

4.3 A Methodology to Quantify the Cyber Resilience of a Particular Design

The consortium undertook an extensive evaluation of various methodologies for quantifying cyber resilience and assessed existing approaches for their suitability in capturing the nuanced and context-dependent nature of cyber resilience, which can vary significantly between different systems and stakeholders. Recognizing the need for a flexible and customizable approach that could accommodate the unique preferences and priorities of system designers and users, a novel game-theoretic methodology was developed. This methodology leverages the principles of game theory to model the strategic interactions between system defenders and potential attackers, allowing for a quantitative assessment of the system's resilience under various attack scenarios. The game-theoretic approach provides a framework for evaluating the effectiveness of different defense strategies, identifying vulnerabilities, and optimizing resource allocation to enhance the overall cyber resilience of the system design.

4.4 An Application Guide for Implementing the Design Framework for Hybrid Systems

To facilitate the practical implementation of the cyber-resilient design framework, the consortium developed a comprehensive application guide (DOE Office of Scientific and Technical Information 2024). This guide takes the form of a structured series of probing questions that system designers must consider throughout the design process. These questions are designed to elicit critical thinking about potential vulnerabilities, threat scenarios, and mitigation strategies, ensuring that cybersecurity considerations are deeply integrated into every aspect of the system design.

To further enhance the usability and effectiveness of the application guide, the consortium created an interactive tool. This tool allows users to input their responses to the guide's questions and, based on their inputs, receive a calculated cyber-resilience score for their design. This score provides a quantitative measure of the system's resilience against potential cyber threats, enabling designers to identify areas for improvement and make informed decisions about resource allocation and risk mitigation strategies. The tool also serves as a valuable educational resource, helping users better understand the complex interplay between design choices and cyber resilience.

The development of this framework involved an iterative and collaborative process, leveraging the expertise of consortium members and incorporating feedback from various stakeholders. Team members, such as INL, heavily supported the development of the cyber-resilient design framework and provided feedback throughout the refinement of the framework. They also led the development of the application guide and aspect scoring to provide the scores and weight to each aspect in the final cyber-resilience score.

INL's contributions were seamlessly integrated into the consortium's efforts, ensuring that the framework aligned with industry best practices and addressed the specific challenges of hybrid renewable energy systems.

The cyber-resilient design framework has received positive feedback from consortium members and industry stakeholders. The consortium's input was critical in identifying the appropriate challenges for hybrid systems, the applicable standards that needed to be considered, and the best practices for hybrid system design. The consortium's input was sought on the game-theoretic mechanism for quantification of cyber resilience, and the tool will be offered to members for testing and further refinement.

In addition to the framework, the simulation models developed in the blended reference architectures were also used to demonstrate three different attack scenarios and how the implementation of the framework can be used to eliminate/mitigate these threats. These scenarios include:

1. Secure by default: This experiment shows the attacker trying to access a device in the network using a default password, but unable to get access.
2. Cloud connection: This experiment shows the disruption of the cloud service connected to the hybrid plant controller via a distributed denial-of-service attack, which is mitigated by using a combination of monitoring and segmentation.
3. Interdependent equipment failure: This experiment shows the impact of interdependent systems by flipping a breaker via fire-suppression-system affecting power generation. This is mitigated by utilizing a preconfigured response scheme.

Additional details on the overall framework and the other components are provided in the dedicated task report. The application guide (https://www.osti.gov/biblio/2403007) and its companion tool (https://sort.inl.gov/Artifact/Index/114194) are also available.

5 Conclusion

The RESCue consortium's collaborative efforts are a pivotal advancement in securing the future of hybrid renewable energy systems. By uniting industry leaders, researchers, and government agencies, the consortium fosters knowledge sharing and collaboration, accelerating innovation and problem-solving in cybersecurity. Through comprehensive research, the consortium has made significant strides in understanding cyber threats specific to hybrid systems, developing innovative tools for assessing and enhancing cyber resilience, and establishing best practices for designing and operating secure infrastructure.

The consortium's commitment to knowledge dissemination has raised awareness of cybersecurity's critical importance in the renewable energy sector. By actively sharing findings through publications, workshops, and outreach programs, the consortium empowers stakeholders with the knowledge and tools to proactively address risks. This work demonstrates the power of collective action in tackling complex challenges, paving the way for a more secure and sustainable energy future.

Building on this foundation, the consortium embarks on its next phase, involving ambitious research projects aimed at transforming the cybersecurity posture of hybrid renewable energy systems. These projects will delve deeper into emerging threats, explore cutting-edge technologies for threat detection and mitigation, and develop advanced frameworks for cyber-resilient system design. This ongoing commitment to research and innovation promises to further strengthen the resilience of hybrid energy systems, ensuring their reliable and secure operation in the face of evolving cyber threats.

Glossary

Term	Definition
Blended reference architectures	Comprehensive architectural blueprints that define the interdependencies and similarities among various hybrid renewable energy system configurations, guiding stakeholders in the secure design, deployment, and operation of these systems.
Cyber-resilient design framework	A structured approach to integrating cybersecurity considerations throughout the entire life cycle of hybrid renewable energy systems, ensuring security is baked in from the initial design phase.
Hybrid renewable energy systems	Integrated systems that combine multiple renewable energy sources, such as wind, solar, and energy storage, to provide reliable and efficient power generation.
IBRs	Electrical devices, such as solar inverters and wind turbine inverters, that convert DC to AC for integration into the electrical grid.
Public-private partnerships	Collaborative efforts between government agencies and the private sector to align cybersecurity initiatives, share threat intelligence, and develop comprehensive policies and programs to safeguard critical energy infrastructures.
Risk assessment methodology	A systematic process for identifying, analyzing, and evaluating cyber risks, considering the unique characteristics and operational requirements of hybrid renewable energy systems.
Situational awareness	The ability to detect, analyze, and respond to potential security incidents or anomalous behavior in real time, enabling proactive threat mitigation.

References

Cherry, Lindsay, and Bryan White. 2019. "SolarEdge and Enphase Now Control 80% of the US Residential Solar Inverter Market." GTM. Accessed December 18, 2019 https://www.greentechmedia.com/articles/read/solaredge-technologies-and-enphase-control-80-of-us-residential-solar-marke.

Hybrid Resources Task Force. 2022. *Unlocking the Flexibility of Hybrid Resources*. Reston, VA: Energy Systems Integration Group. https://www.esig.energy/reports-briefs.

Institute of Electrical and Electronics Engineers (IEEE) Standards Association. 2018. IEEE 1547-2018: IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. https://standards.ieee.org/ieee/1547/5915/.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). 2022. "ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection—Information security controls." https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en.

Johnson, Jay, Michael McCarty, Bryan Richardson, Craig Rieger, Rafer Cooley, Jake Gentle, Bradley Rothwell, Tyler Phillips, Beverly Novak, Megan Culler, Keith Schwalm, and Brian Wright. 2023. *Hardening Wind Energy Systems from Cyber Threats-Final Project Report*. https://www.researchgate.net/publication/368599508_Hardening_Wind_Energy_Systems_from_Cyber_Threats-Final_Project_Report.

National Institute of Standards and Technology (NIST). 2020. "NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations." https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

National Institute of Standards and Technology (NIST). 2022. "NIST SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." https://csrc.nist.gov/pubs/sp/800/161/r1/final.

National Institute of Standards and Technology (NIST). 2024. "The NIST Cybersecurity Framework (CSF) 2.0" https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

North American Electric Reliability Corporation. n.d. Critical Infrastructure Protection (multiple standards). https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx.

Office of Energy Efficiency & Renewable Energy. 2021. "DOE and Industry Partner to Ensure Cybersecurity for Wind Energy Systems." https://www.energy.gov/eere/wind/articles/doe-and-industry-partner-ensure-cybersecurity-wind-energy-systems.

Petersen, Lennart, Bo Hesselbaek, Antonio Martinez, Roberto Borsotti-Andruszkiewicz, Nathan Steggel, Dave Osmond, and Germán Tarnowski. 2018. "Vestas Power Plant Solutions Integrating Wind, Solar PV and Energy Storage." https://hybridpowersystems.org/wp-content/uploads/sites/9/2018/05/3B_3_TENE18_078_presentation_Petersen_Lennart.pdf.

The International Society of Automation (ISA) and International Electrotechnical Commission (IEC). n.d. ISA/IEC 62443 Series of Standards. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

The White House. 2023. National Cybersecurity Strategy. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

U.S Energy Information Administration. n.d. The Electricity Mix in the United States Shifts from Fossil Fuels to Renewables. https://www.eia.gov/outlooks/aeo/narrative/index.php#TheElectricityMixinth.

U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response. 2022. Cybersecurity Capability and Maturity Model (C2M2). https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

U.S. Department of Energy (DOE) Office of Scientific and Technical Information. 2024. “Application Guide for the Cyber-Resilient Design Framework for Hybrid Systems.” https://www.osti.gov/biblio/2403007/.

U.S. Department of Energy (DOE). 2021. Hybrid Energy Systems: Opportunities for Coordinated Research. Golden, CO: National Renewable Energy Laboratory. DOE/GO-102021-5447. https://www.nrel.gov/docs/fy21osti/77503.pdf.

Wilson, Adam. 2023. “GE, Vestas top US leaderboard in installed wind capacity, performance GE, Vestas Top U.S. Leaderboard in Installed Wind Capacity Performance.” S&P Global Market Intelligence. Accessed August 31, 2023. https://www.spglobal.com/marketintelligence/en/news-insights/research/ge-vestas-top-us-leaderboard-in-installed-wind-capacity-performance.

Wood McKenzie. 2022. “Power and Renewables Report. ”*US Solar Market Insight.* https://www.woodmac.com/industry/power-and-renewables/us-solar-market-insight/.