INL/RPT-24-78909

Application Guide for the Cyber-Resilient Design Framework for Hybrid Systems

May 2024

Heather Ackenhusen and Megan J. Culler
Idaho National Laboratory

Venkatesh Venkataramanan
National Renewable Energy Laboratory

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance, LLC*

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/RPT-24-78909

Application Guide for the Cyber-Resilient Design Framework for Hybrid Systems

Heather Ackenhusen and Megan J. Culler
Idaho National Laboratory
Venkatesh Venkataramanan
National Renewable Energy Laboratory

July 2024

Idaho National Laboratory
Infrastructure Security
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Cybersecurity, Energy Security, & Emergency Response
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

Table of Contents

Figures

Tables

Page intentionally left blank

Acronyms

CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cybersecurity Performance Goals
DOE	U.S. Department of Energy
EPC	engineering, procurement, and construction
HIDS	Host-based intrusion detection systems
HRES	Hybrid renewable energy systems
IDS	Intrusion Detection System
IPS	Intrusion Protection System
IT	Information Technology
NCSC	National Cyber Security Centre
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OT	Operational Technology
PCB	Printed Circuit Board
PE	Power Electronics
PLC	Programmable Logic Controllers
PoC	Point of Connection
PPC	Power Plant Controllers
PV	Photovoltaics
RC	Resistor/Capacitor
RF	Radio Frequency
RTO	Recovery Time Objective
RTU	Remote terminal units
SBOM	Software Bill of Material
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VLAN	virtual local area network
VPN	virtual private network

Application Guide for the Cyber-Resilient Design Framework for Hybrid Systems

1. HYBRID POWER PLANTS: ASSESSING PLANT DESIGN FOR CYBER RESILIENCE

1.1. Overview

As the energy landscape evolves, hybrid power plants—integrating multiple renewable energy sources (e.g., solar, wind, and battery storage) with the bulk power electric system—play a crucial role in meeting growing energy demands. However, with a hybrid power plant's increased number of components, complex network connectivity and digitization of controls, these systems face growing cybersecurity risks. To help mitigate these risks, Idaho National Laboratory (INL) presents this application guide specifically designed for operators and systems engineers to evaluate the cybersecurity resilience of their hybrid power plant's design.

1.1.1. Purpose of the Guide

The purpose of this guide is to provide operators and power systems engineers with a mechanism to quantitatively evaluate critical aspects of the hybrid power plant design based on the unique challenges facing these types of plants. The goal is to identify potential vulnerabilities and gaps, along with opportunities for improvement which, if addressed, will enhance the plant's overall resilience to cybersecurity threats and attacks.

1.1.2. Mechanism for Evaluation

This guide includes a structured scoring mechanism—an excel spreadsheet, "Hybrid Power Plant Resilience Scoring Matrix"—which asks a series of yes/no questions. These questions cover key topics related to cyber resilience of the hybrid power plant's design, evaluating key topics such as these:

- Security practices of equipment vendors and software suppliers
- Vulnerability of selected power systems and communication devices
- Ability to configure, control, and monitor power plant components
- Authorization mechanisms, access controls, and management of privileges for users
- Segmentation and protection of communication networks
- Ability to support incident detection, response procedures, and recovery plans
- Engineered controls in the plant's design.

1.1.3. Framework and Sources

The evaluation is based on the design aspects highlighted in the National Renewable Energy Laboratory's (NREL) Cyber-Resilience Framework for Hybrid Energy Systems. [3] Additionally, the series of questions draw from vetted best practice guides and studies, including the following:

- NIST Cybersecurity Framework and Cyber-Resilient Engineering Framework
- U.S. Department of Energy's (DOE) CESER Cyber-Informed Engineering Implementation Guide
- Cybersecurity Capability Maturity Model (C2M2)
- NERC Guidelines
- IEEE Power and Energy Society Recommendations
- ACM Insights

- CISA and CIS Resources
- MITRE CREF Navigator and EMB3D for Embedded Devices/OT
- Linux Foundation's Open-Source Security Foundation (OSSF)
- Power Systems Cybersecurity (ISBN: 978-3-031-20359-6)
- Research from NREL and INL
- ITIL V4 Information Security Management (ISM) based on ISO/IEC 27001:2022.

By leveraging these industry-endorsed sources, this application guide focuses on distilling key areas of risk faced by hybrid power plant operators when designing a plant, while providing a practical approach to a cyber-resilience assessment.

1.2. Challenges Facing Hybrid Power Plants

DOE research calls out specific challenges for hybrid power plants' cybersecurity, including (1) rapid communication between subcomponents, (2) rapid communication between the plant and the grid, (3) increased attack surface due to the greater number of targets, (4) interoperability of legacy and new equipment, (5) potential use of third-party components with an unsecure supply chain, (6) control of the plant using a distributed energy resources management system (DERMS), (7) heavier reliance on remote connections, and (8) diverse stakeholders with access/ownership boundaries that are not well defined.

These challenges do not require novel cyber-resilience solutions; however, they can inform the prioritization of design criteria and solutions that meet the identified challenges.

1.3. Cyber Resilience Aspects

To address these challenges, DOE formed the Renewable Energy and Storage Cybersecurity Research (RESCue) project. In addition to creating the Cyber-Resilience Framework for Hybrid Energy Systems, another of the project's goals is to provide a mechanism to assess the cyber resilience of new and existing hybrid power plants. In support of that goal, INL created this application guide.

The application guide is intended to provide tangible criteria to help a hybrid power plant systems engineer apply NREL's Cyber-Resilience Framework for Hybrid Energy Systems. This application guide focuses on evaluating the unique design risks of hybrid power systems using quantitative metrics.

Note: *Due to its exclusive focus on design, this application guide should not be viewed as a comprehensive assessment of a hybrid power plant's overall cyber resilience. This guide is also not intended to replace the application of cybersecurity standards or practices used within a company or across an industry.*

NREL's Cyber-Resilience Framework for Hybrid Energy Systems highlights specific design aspects that are identified as critical to the cyber resilience of hybrid power plants. The application guide is structured around evaluating decisions that affect those design aspects. The design aspects are as follows:

- Vendor Selection and Management
- Device Selection and Management
    - Power System Devices
    - Communication System Devices
    - Identification of High Consequence Scenarios
- Asset and Configuration Management
    - Storage of Design Information
    - Asset Inventory

    - Backups for Critical Functionality
    - Endpoint Hardening
- Access
    - Access Control
    - Authentication
- Network Architecture
    - Network Segmentation
    - Firewall Placement
    - Protocol Requirements
- Monitoring
    - Monitoring Tools
    - Sensor Placement
- Response
    - Incident Response Plan
- Engineered Controls
    - Choice of Control Scheme (Central vs. Distributed)
    - Increase in Observability
    - Increase in Controllability.

The nine design aspects, which include multiple sub-aspects, are intended to identify areas of the design that affect cyber resilience. The sub-aspect classification helps combine related aspects down into larger classes, which are easier to digest.

Starting in Section 3, the design aspects are broken down in detail. For each design aspect, the purpose, importance, and/or objective(s) is described. These aspects are broken into sub-aspects, where appropriate, to aid in the evaluation and scoring of that aspect's cyber resilience. For each sub-aspect, several questions are asked, which are intended to guide the user's design of a system and evaluate cyber-resilience choices. The questions are not intended to be entirely exhaustive of all design considerations but rather to provide a solid base for evaluating cyber resilience in each sub-aspect. The questions, which are mirrored in the scoring matrix, are also provided in this guide. Note that some questions may appear similar but could have different answers based on the context of the aspect. Questions that are repeated have relevance to multiple aspects and may be answered in all categories without over-emphasizing their importance. Recognizing that operators may have different priorities and goals related to cyber resilience, the scoring matrix is structured so that the assessor can assign a level of importance and weight to each sub-aspect as well as to the primary design aspects.

1.4. Cyber-Resilience Evaluation Criteria

To arrive at the cyber-resilience metric described in the Cyber-Resilience Framework for Hybrid Energy Systems, a score must be assigned to each of the design aspects. This final cyber-resilience score is intended to be a comparative score that allows users to assess tradeoffs between different design decisions. It is not an absolute score, nor a guarantee of a certain level of resilience against cybersecurity hazards. There is an unavoidable degree of subjectivity in this score; in fact, there is an intentional degree of subjectivity in the assignment of weights to each aspect that is included in the overall score, which is based on the user's priorities across the aspects.

There are many ways that the score for each aspect could be assigned. Users could self-assign a score for each aspect using the information in the application guide to inform a self-assessment. The user could pick key metrics that they feel represent each aspect and measure their system design against these metrics. For the purposes of repeatability and transparency, this simple scoring mechanism is suggested:

For each aspect, a series of yes and no questions are presented that address best practices related to that aspect and sub-aspect.

For each aspect, the score is calculated as the percentage of questions that are answered "yes" out of the total number of questions for that aspect. A "not applicable" option is available to reduce the number of total questions used for the score calculation. This is intended to provide an option for users who identify questions that do not apply to their system or are not feasible to implement so those questions do not penalize the score. Again, we note that the score is not intended to be an absolute measure of resilience, but rather a comparative method to evaluate design choices.

The benefit of this approach is that the scoring for each aspect is transparent and repeatable. Although answering all the questions in the guide may be time consuming, the large number of questions lends credibility to the final score in the sense that evaluating many contributing factors to each aspect gives a better overall impression of the strength than evaluating one or two contributing factors. This method is quantitative and can be backed by data.

The drawback of this approach is that the questions in this application guide are not guaranteed to be a full set of all the potentially relevant questions for a cyber-resilient hybrid system design. The questions have been selected from industry-accepted resources and vetted by subject matter experts, but they may not be fully comprehensive. Still, they provide a good basis of understanding for the level of cyber-resilience maturity in each aspect and inform the user on areas of strength and weakness and recommendations to improve cyber resilience. Alternate scoring methodologies may be considered if the user desires to assign scores for each aspect, which can then still be fed into the final cyber-resilience score calculation.

2. BACKGROUND

2.1. What are Hybrid Systems?

Hybrid systems can be defined simply as two or more generation sources, typically renewable, that share a single point of connection (PoC) with the grid. They can include many types of generation, as well as storage and conversion technologies, as seen in Figure 1. Hybrid systems may be used in front-of-the-meter, behind-the-meter, microgrid, and off-grid applications. They may provide both energy and non-energy products. For example, a hydrogen generation hybrid would use excess energy from its paired generation component (e.g., a wind plant) to produce hydrogen gas, which may be used for long-term energy storage or to power hydrogen fuel cells.

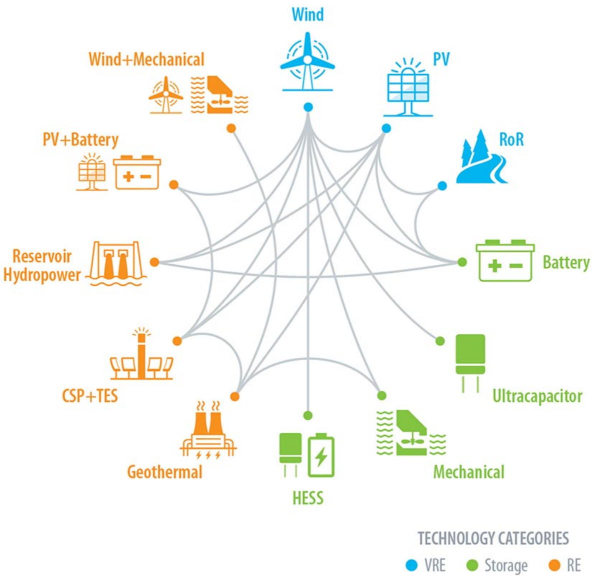

Figure 1. Hybrid system components and potential combinations. [1]

Hybrid plants may include co-located systems and full hybrid systems. Co-located plants have multiple resources behind the same PoC but may have distinct models and dispatch for individual resources behind the shared interconnection. In contrast, full hybrid systems operate with a single bidding and dispatch strategy for multiple resources behind the shared interconnection. This distinction is visualized in Figure 2.

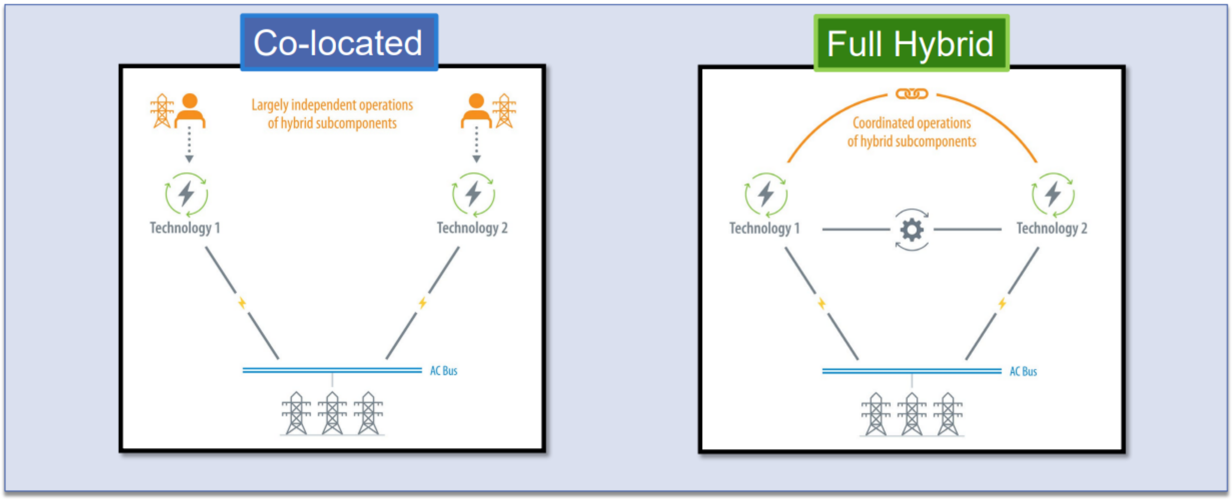
Co-located
Largely independent operations of hybrid subcomponents
Technology 1
Technology 2
AC Bus
Full Hybrid
Coordinated operations of hybrid subcomponents
Technology 1
Technology 2
AC Bus

Figure 2. Co-located vs. full hybrid plants. [2]

Full hybrid systems may either be AC-coupled or DC-coupled, while co-located hybrid systems are limited to being AC-coupled. AC-coupled plants have an AC/DC inverter for each generation resource that requires one (e.g., solar and battery each have their own inverter), while DC-coupled plants use the same AC/DC inverter for multiple generator types. In AC-coupled plants, resources of the same type may be centralized, for example, in a single battery yard accompanying a solar plant. In contrast, a DC-coupled plant would distribute the batteries throughout the solar plant so that they could be close to the inverters.

2.2. Scope for the Application Guide

In this study, we limit our study to systems that are connected to the bulk grid, which excludes microgrid and behind-the-meter applications. Additionally, we focus the scope on systems for which electricity is the only output. This excludes systems in which chemicals, fuels, heat, or freshwater could be other products of the hybrid system.

The breadth of potential applications, generation mixes, and configurations is large, even given the narrowed scope. Many choices will be made through the design process to optimize the plant layout, network configuration, data collection, and more in service of optimizing performance. Along with performance goals, it is important to consider the resilience and cyber-resilience requirements for the system. To that end, a framework for cyber-resilient design of hybrid energy systems as well as this accompanying application guide has been developed. The purpose of this guide is to present design considerations for hybrid energy systems, which will have an impact on the overall cyber resilience of the system. After walking through this guide, a user will be equipped to evaluate hybrid energy system designs using the framework's scoring methodology to evaluate tradeoffs between design choices.

2.3. Limitations of Framework

This framework is intended to be flexible, enabling the user to set their own priorities that are reflected in the scoring calculation.

In the framework application, there are some limitations of the framework identified. These are highlighted below to help users identify the ways in which the framework should be applied.

- Some of the metrics identified for certain aspects are only possible to measure in operation. For example, the effectiveness of an incident response plan can only be measured when there is an incident or at least when operators can practice the response plan. These are difficult to measure in the design phase.
- There can be things included in the design process that are only effective at reducing risk if they are leveraged in operation. For example, metrics on performance, security, or network activity can be collected from sensors designed into the system, but these metrics do not provide value unless an operator (human or machine) monitors and evaluates them regularly.
- There is subjectivity in the framework. The authors of the framework have used subject matter expertise in a variety of areas to select the principles and aspects that informed the list of metrics. There is intentional flexibility built into the framework to allow users to prioritize areas of cyber resilience that are most important to them and select metrics that best apply to their systems. However, this introduces a degree of subjectivity in the evaluation process. Users should be aware of this and should use the metrics as a comparative tool to evaluate different design choices. The framework is not intended to provide an absolute measure of cyber resilience or be used to compare the cyber resilience of arbitrary hybrid energy systems.

2.4. Stakeholder Considerations

Who Should Apply This Framework?

This framework is designed specifically for hybrid energy systems. It is focused on the design of hybrid systems, although it could be a tool to evaluate existing hybrid energy systems as well. Many stakeholders may be involved in the design and development process. Some of those possible roles are shown in Table 1, although not all stakeholders may exist for each new project.

Table 1. Roles of stakeholders in design and development of hybrid energy systems.

Stakeholder/Role	Fund Development	Identify Specifications	Build and Assemble Subsystems	Procure Subsystems	Build and Assemble	Operate
Engineering Procurement and Construction (EPC) firm	—	X	—	X	X	—
Original Equipment Manufacturer (OEM)	—	—	X	—	—	—
Developer	X	X	—	X	X	—
Investment Firm	X	—	—	—	—	—
Independent Operator	X	X	—	—	—	X
Utility	X	X	—	—	—	X

It is worth noting that there are multiple stakeholders that may be involved in the identification of specification for the system, which is the stage at which many decisions affecting the cyber-resiliency of the system will be made. End users, like the operators or utilities, may define many of the performance, interconnection, and communication requirements. If they want to enable certain cyber-resilient operational practices, like monitoring, these should be included in the specifications to ensure that those implementing the systems, such as the EPCs or developers, create systems that enable operational practices. Some things are easier to add than others after the system is built. It may be feasible to add additional physical or cyber sensors to advanced monitoring after the system is built, but this may add unnecessary complexity and cost to do this after rather than during the construction process. As an additional example, if there is a desire for regular backups of OT device configurations or data, there must be a way to collect that data from the system. If there is no historian and data pipeline to this historian included in the design, an operator may need to do it manually, which would likely limit the frequency of collecting backups at all.

3. VENDOR SELECTION AND MANAGEMENT

Vendor selection and management is a key part of cyber resilience as it gives the system engineer or designer some control over the source of components. While the engineering, procurement, and construction (EPC) firm, developer, or end user (e.g., a utility) will have more direct control over the components and the layout of the hybrid energy system, these designers will not have direct control over the manufacturing and design of subcomponents. Instead, the vendors and suppliers will be the ones implementing secure coding practices, developing policies that prevent the use of default passwords, and implementing other Secure-by-Design principles. Choices made about the suppliers of subcomponents can have a profound impact on overall cyber resilience.

An operator or systems engineer can prefer vendors that show evidence of cyber-resilient implementation of their products, but it is unreasonable to expect that this will be the only consideration. Technical specifications, performance requirements, and cost will be key to identifying a pool of acceptable vendors, and cost, existing relationships, and familiarity with a brand may narrow down this pool. Still, the vendor considerations described below may help select the most secure provider from the acceptable pool.

3.1. Vendor Technical and Process Acumen

Objective: Assess the vendors used in the design based on the following criteria.

- **Technical Expertise**:
  - Does the vendor have extensive experience in designing, installing, and maintaining hybrid power components, especially as it relates to the vendor's history in mitigating and managing cybersecurity attacks on those components?
  - Do cybersecurity experts recognize the vendor as a leader in designing their product/service for cyber resilience?
  - Does the vendor leverage security processes and controls throughout their product/service life cycle?
- **Commitment to Security and On-Going Reliability**:
  - Does the vendor publish metrics and test results demonstrating a commitment to secure and reliable products?
  - Do the vendor's warranty terms include remediation of vulnerabilities and activities, which improve cyber resilience?
  - Does the vendor maintain cybersecurity plan documents, including how the program is enacted internally, as well as its security relationship with external groups? More specifically, does the plan do the following:
    - Does the plan include security policies, procedures, and remediation plan?
    - Does the plan describe the vendor's cybersecurity program requirements and how they meet them?
    - Does the plan address challenges that are unique to hybrid power plant operators, reflecting the urgency and importance of mitigating threats to critical infrastructure?
    - Does the plan include specific technical and operational cybersecurity topics, such as these:
      - User data privacy and protection
      - Secure data transfer and protection for data at rest
      - Secure communications protocols
      - Cloud protections
      - Access management
      - Patching and upgrades
      - Incident response reporting and recovery with a communications plan, audits, and assessments
      - Continuity of operations
      - Risk acceptance and mitigation and disaster recovery.
- **Financial Stability and Contractual Support from Third Parties**:
  - Are the vendor's financial reports and investor ratings strong/healthy?
  - Does the vendor include cybersecurity requirements in their contracts and agreements involving third parties?
- **References and Case Studies**:
  - Did the vendor provide multiple positive references from other clients?
  - Did the vendor provide case studies demonstrating their successful mitigation of cybersecurity threats?

3.2. Vendor Security Practices

Objective: Verify that the vendor follows CISA, NIST, and IEEE/IEC standards.

- **Cybersecurity Practices**:
  - Are the vendor's cybersecurity policies and practices comprehensive?
  - Does the vendor's product(s) and components include cybersecurity certifications (e.g., ISO 27001, ISA 62443)?
  - Does the vendor use mechanisms (e.g., processes, technology automation) to verify their cybersecurity policies and practices are followed and enforced?
  - Does the vendor participate in and promote a responsible disclosure program for vulnerabilities discovered by researchers or external partners?
  - Does the vendor participate in E-ISAC and/or related orgs?
  - Does the vendor have a process for timely patching of software components, firmware upgrades, etc.?
  - Does the vendor use CISA services, including scanning and testing?
  - For internet-accessible assets, does the vendor leverage CISA Cyber Hygiene services for regular review, reporting, and mitigation of vulnerabilities?
  - Did the vendor perform a CPG assessment by CISA's regional cybersecurity advisors?
  - Does the vendor subscribe to NCSC's free Early Warning service (UK organizations)?
  - Can the vendor be compliant with NERC CIP (low/medium) regulations if required?
- **Access Management:**
  - Does the vendor eliminate default passwords and require strong passwords as a general practice?
  - Does the vendor mandate multifactor authentication for privileged users where changes to engineering logic or configurations are safety-impacting events in critical infrastructure?
  - Does the vendor include logging of all change and access control logs using open standard logging formats?
- **Secure Communication Protocols**:
  - As a general practice, do the vendor devices/components support secure, standardized communication protocols?
- **Resilience of Products/Services**:
  - Does the vendor include specific redundancy and/or resilience features in their product(s)/service(s), including such features for remote connections?
  - Does the vendor have after action reviews if/when their product(s)/service(s) is compromised? If so, do those reviews include remediation actions, which are tracked and implemented?
- **Supply Chain:**
  - Does the vendor publish or share a software bill of material (SBOM) for their products, including all open-source and third-party software components, versions, and patch levels?
  - Do patches and/or upgrades trigger updates to the vendor's SBOM?
  - Does the vendor publish or share a hardware bill of material (HBOM), particularly one leveraging CISA's published HBOM framework?

3.3. Vendor Risk Profile

Objective: Identify any major risks associated with this vendor.

- **Reputational Risk:**
    - Does the vendor have a history of frequent large-scale data breaches and/or cyberattacks?
    - Does the vendor have a poor net promoter score from its customers or low public perception?
    - Has the vendor been cited for regulatory compliance issues or misconduct?
- **Supply Chain Security Risks:**
    - Does the vendor assess and mitigate risks associated with third-party components?
    - Does the vendor maintain and update a Vulnerability Exploitability eXchange (VEX) to track the exploitability of any vulnerabilities associated with components in the SBOM?
    - Does the vendor trace the origin of all subcomponents used in their products?
    - Does the vendor perform audits of their suppliers? If so, are the audits done on a frequent basis and is the audit scope comprehensive?
    - Does the vendor handle vulnerabilities discovered in subcomponents in a timely manner? Do they have a related response plan in place?
    - Does the vendor employ methods to verify the integrity of hardware components (e.g., Non-Destructive Testing [NDT]).
- **Supply Chain Availability Risks:**
    - Do other vendors produce similar products and are the products interchangeable (e.g., if electrical relays are being purchased from a primary vendor, do other vendors offer similar products with the same functionality in case the primary vendor becomes a bottleneck)?
    - Is the vendor's production capacity sufficient to meet demand during large-scale disaster events, and/or can it be scaled up quickly in response to increased demand?
    - Are the standard lead times for the vendor's products reasonable, and how do they vary under different market conditions?
    - Does the vendor have alternate manufacturing sites in different regions to mitigate geopolitical risks?
    - Does the vendor have redundancy built into their own supply chain for critical components?
    - Does the vendor have a strategy for diversifying supply sources to avoid single points of failure?
    - Does the vendor effectively manage inventory levels for critical subcomponents? Does the vendor have systems in place to ensure the continuity of supply in case of sudden demand spikes or supply disruptions?
    - Does the vendor have logistics capabilities, which can handle transportation disruptions? Do they provide visibility into the transportation process, including carrier performance and potential bottlenecks?
    - Does the vendor communicate and report supply chain issues? Do they update clients on supply chain status and potential risks on a frequent basis?
- **Geopolitical Risks (Vendor Location, Political Stability):**
    - Are the vendor's subcomponents manufactured in areas of geopolitical instability?
    - Can the vendor provide traceability records for subcomponents, including their origin and journey through the supply chain?
    - Does the vendor take measures to verify the authenticity and ensure the integrity of subcomponents during manufacturing?
    - Does the vendor have robust quality assurance processes and what certifications do they hold?

3.4. Vendor Collaboration

Collaboration with vendors brings more attention to potential security issues and enables improved communication. Collaboration supports a more comprehensive review of the design for points of failure, introduction of risk, and threat assessment.

- Was the vendor involved early in the design process?
- Did the vendor collaborate on system integration, interoperability, and cybersecurity testing?

3.5. Quantitative Scoring

In the scoring matrix, assign weights to each subcategory above (e.g., vendor risk profile).

Score each vendor by answering yes/no to the questions above using the scoring matrix.

4. DEVICE SELECTION AND MANAGEMENT

Vendor selection is intended to assess the overall vendor organization. In this section, we consider specific devices provided by a vendor, focusing on hardware components. This aspect can assess the cyber resilience of product lines from the same manufacturer or compare similar devices across manufacturers. Like with vendor selection, it is important to note that cyber resilience will be just one factor in the overall design of the system and selection of devices. Technical specifications, performance requirements, and cost will be key drivers of this selection. To that end, there is focus not only on the selection of devices, but the integration and management of the devices too, something which a designer may have more control.

4.1. Power System Device Selection and Management

Objective: Assess whether cyber-resilient devices and management systems are incorporated into the overall hybrid power plant design.

The following device characteristics should be considered:

- Comprehensive security features and coverage, such as data encryption
- High reliability when exposed to threats or attacks
- Communication interface is compatible with secure communications protocols
- Equipped with manual, fail-safe mechanisms to prevent catastrophic failures
- Equipped with fail-operational mechanisms to protect availability of the device, where possible.

4.1.1. Energy Generation and Storage Resources

Assess whether the selected wind turbines, solar panels, and/or batteries in the design support the following:

- Dedicated and secure communication channels for control of the device
- Regular updates to device firmware
- Controlled access for monitoring and maintenance activities, along with authentication of authorized users
- Physical access barriers to prevent tampering
- Isolation of control functions from monitoring functions

- Detection and alarming for unauthorized modifications and/or abnormal behavior
- Regular assessment of vulnerabilities associated with each software component
  - Use of the SBOM to proactively address security risks when new vulnerabilities are discovered.

4.1.2. Power Electronic Converters, Transformers, and Circuit Breakers

Assess whether the design includes resilience mechanisms for these components, such as listed:

- Fault detection
- Shielding around the critical components to protect against electromagnetic signals
- Physical stops to prevent damage from malicious signals (e.g., transformer pressure relief, breaker low gas alarm, operation counters, tap changer limits set)
- Verification checks that validate Power Electronics (PE) hardware layer authenticity when initiating inverter operation (e.g., Printed Circuit Board (PCB) authentication using RC (resistor/capacitor) filters.
- Adherence to applicable standards such as IEEE 1547 and 2030.5
- Adhere to certification standards (such as UL 2941) provided by various agencies, such as ANSI, and certified by a Nationally Recognized Testing Laboratory, such as Underwriter's Laboratory.

4.1.3. System Protection and Critical Control (e.g., Relays, Fuses, Sensors and Actuators)

Assess whether the devices selected to control and monitor frequency, voltage, current, and circuit breaker condition have the following features and functionality:

- **Communication Security:**
  - Does the device use secure communication protocols (e.g., TLS/SSL (transport layer security/secure sockets layer)) to protect data transmission?
  - Does the device authenticate with the network to prevent unauthorized access?
  - Does the device support network segmentation if it is multi-functional (e.g., has monitor and control capabilities)?
- **Data Integrity and Authenticity – Providing Accurate and Tamper-Proof Data:**
  - Does the device support digital signatures to verify data authenticity?
  - Does the device timestamp data to track events accurately?
- **Resilience to Physical Attacks:**
  - Is the device protected by a tamper-proof enclosure?
  - Does the design include redundant sensors and actuators to maintain functionality even if one fails?
  - Does the design specify that these devices use wired communications or IEMI-resistant wireless?
  - Does the design include the deployment of broadband RF (radio frequency) detectors to alert operators to the presence of abnormal electromagnetic (EM) fields?
- **Adaptability and Self-Healing:**
  - Does the device have backup power (e.g., battery or universal power supply [UPS]) to maintain synchronization during power outages?
  - Does the device perform self-diagnostics and report anomalies?
  - Does the device auto-recover from disruptions (e.g., reset after a communication failure)?

- **Cybersecurity Updates:**
  - Does the configuration of the device support regular firmware updates to patch vulnerabilities?

4.1.4. Control and Management Devices

Assess whether the devices selected to access, control and manage the hybrid power plant have the following features and functionality:

4.1.4.1. Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs)

- Does the device support secure communication protocols (e.g., TLS, SSL) to protect data transmission?
- Does the device use memory-safe programming that prevents privilege escalation or unauthorized changes to firmware and configurations?
- Does the device maintain segregation of data between multiple devices that it may manage?
- Are the configuration parameters of the device locked to settings within a range that is enforced through cyber or physical means?
- Is the device designed to gracefully handle failures (e.g., power outages, communication disruptions)?
- Does the device support redundant communication paths?

4.1.4.2. GPS Clock

- Does the device have strong authentication mechanisms where only authorized personnel can configure or access the GPS clock?
- Does the device transmit data in an encrypted format between the GPS clock and other systems to prevent eavesdropping or tampering?
- Does the device use secure communication protocols (e.g., NTP over TLS) to prevent unauthorized access or data manipulation?
- Does the device support regular updates to its firmware to patch security vulnerabilities?
- Does the device include mechanisms to prevent physical tampering?
- Does the design segment the GPS clock from all other control networks to limit the impact of potential breaches?
- Does the design deploy redundant GPS clocks to ensure continuous time synchronization even if one fails?
- Does the design implement failover mechanisms to switch to an alternative time source (e.g., another GPS clock or an internal oscillator) in case of GPS signal loss?
- Does the GPS clock support monitoring to detect anomalies (e.g., sudden time drift) and trigger alarms?
- Does the design support continuous assessment of GPS timing relative to the quality of time synchronization?
- Does the GPS clock have backup power (e.g., battery or UPS) to maintain synchronization during power outages?
- Does the design enable the GPS clock’s functionality to be tested to simulate failure scenarios to verify resilience?

4.1.4.3. Power Plant Controllers for PV, Wind, BESS, Hybrid Plants and DERMS

- **Data Collection**:
  - Does the Power Plant Controllers (PPC) collect and store data in an encrypted format from various components of the power plant, including the power generation units (like wind turbines and solar panels) and the energy storage systems?
- **Command Distribution**:
  - Does the PPC have mechanisms to verify its collected data and vet the validity of curtailment commands?
  - Does the PPC distribute commands to the different components through an authorized and access-controlled dispatch function?
  - Does the PPC capture existing settings and configurations prior to issuing downstream changes?
  - Does the PPC have feedback mechanisms to assess the impact of changes made to components, such as ensuring active power output is properly managed and reactive power output to maintain the voltage at the high side of the substation transformer remains within a specified range?
- **Optimization**:
  - To ensure frequency stability and cybersecurity of the load frequency control (LFC) system, does the PPC have a data prediction algorithm to predict any delayed or lost data?
  - Can the PPC track and assess measurement variation dynamics (e.g., larger deviation of measurement from the historical data and indicate the presence of false data)?
  - Does the PPC have embedded algorithms to identify attacks and/or suspend LFC activity during an attack?
  - Can maximum ramp rate be set and enforced to prevent sudden system disturbances?
  - Is the PPC coordinated with any protective systems, such as fault and overload protection, to ensure an operator cannot produce voltage or current conditions, which will trigger system protective outages?
  - Does the PPC flag changes made to algorithms such as those that promote increased renewable energy utilization?
  - Can the PPC take commands from a grid operator for reliability and grid support?
- **Bulk Electric System Compliance**:
  - Can the PPC handle grid saturation situations by distributing the energy produced throughout the day?
  - Does the PPC satisfy compliance and contractual requirements, such as the interconnect agreement and NERC generator reliability standards?

4.1.4.4. Cybersecurity Devices: Intrusion Detection System (IDS), Intrusion Protection System (IPS), Security Information and Event Management (SIEM)

Assess whether the devices selected to detect and protect the hybrid power plant from cyberattacks and threats have the following features and functionality:

- Are host-based intrusion detection systems (HIDS) installed on devices that can support this kind of monitoring?
- Are HIDS alerts tuned for the system to reduce the number of false-positive alerts and alarms?
- Is the HIDS data managed by a person or system?
- Is an IPS installed on devices that can support this?

- Is the IPS tuned for normal and anomalous behaviors of the system?
- Is the IPS regularly updated with signatures of emerging threats?

Assess the following with consideration for SIEM (collecting, analyzing, and correlating security event data to provide insights and detect threats in real time):

- Are alerts centrally collected in a security information and event management (SIEM) platform?
- Is the SIEM turned to the performance of the system so that true anomalies can be detected?
- Is the SIEM actively monitored by a person or service?

4.2. Communication System Device Selection and Management

Objective: There is a need for suppliers and operations staff to be able to access the hybrid plant remotely for monitoring and to communicate with power system devices such as issuing commands that control and/or change the state of hybrid power plant assets. Communication system devices include routers, switches, and the communication medium. These devices perform information exchange between the various tiers of devices. Communication medium can be wired or wireless.

4.2.1. Selection of Communication System Devices

Assess whether the devices and wiring selected to enable secure communications across the hybrid power plant components have the following features and functionality:

4.2.1.1. Switches and Routers

- Are access lists maintained for switches?
- Is remote administration of routers and switches restricted to need-only personnel?
- Is traffic flowing through switches and routers collected and monitored?
- Are switches and routers located in physically protected areas?
- Are switches and routers included as part of patch management planning?
- Are configuration files of switches and routers maintained as backups?

4.2.1.2. Firewalls

- Do the selected firewalls support stateful inspection (i.e., monitors all sessions and verifies all packets)?
- Do the selected firewalls monitor active connections and inspect packet headers and payloads?
- Are firewalls included as part of patch management planning?
- Are firewall configurations regularly maintained as backups?

4.2.1.3. Physical Communication Mediums

- Which parts of the planned communication medium require physical connectors or jump points?
- Are security tradeoffs between different mediums considered (e.g., serial vs. ethernet)?
- Are backups of communication cables and jump points maintained in case parts fail?
- Are servers, modems, or jump points for wireless communications kept in physically secure areas?
- Are backups of servers, modems, or jump points for wireless communication maintained in case parts fail?

4.2.2. Management of the Communication System

Assess whether the design fosters secure access to communications functions across the hybrid power plant:

- Does the design prohibit a separate dedicated back door or local connections?
- Does the design include the use of bastion hosts (i.e., dedicated server that lets authorized users access the hybrid power plant components from an external network or the internet) or jump servers to restrict users to using applications authorized by the asset owner?
- Does the design require both external vendors/contractors and internal enterprise users to use the same method to access industrial assets within the hybrid systems?
- Does the design ensure users are given access to reach the bastion hosts only?
- Does the design include full logging and auditing capabilities for all remote access connections.

4.3. Quantitative Scoring

In the scoring matrix, assign weights to each subcategory above (e.g., power system device selection).

Score each category by answering yes/no to the questions above using the scoring matrix.

5. HIGH CONSEQUENCE SCENARIOS

5.1. Identification of High Consequence Scenarios

5.1.1. Purpose and Importance

The overall goal is to prioritize security measures based on situations that negatively impact safety, operations, and/or performance of critical hybrid power plant infrastructure. By identifying the worst possible scenarios that could occur based on a cybersecurity incident, the related components and processes can be prioritized for risk mitigation methods.

5.1.2. Design Effectiveness in Mitigating High Consequence Scenarios

Objective: Assess whether the design includes mechanisms that improve the system's overall resilience when attacked.

- Were high consequence scenarios defined as part of the design process?
- Does the design ensure that all high consequence scenarios have a component-based risk assessment?
- Does the design document mitigation activities for each high consequence scenario?
- Does the design specify software and hardware limits to the manipulation of physical processes, limiting the impact of a successful compromise?
- Are the limits of software and hardware enforced and tested?
- Does the design incorporate manual overrides for all high consequence scenarios?
- Does the design include manual controls to maintain the ability to operate a given system manually?
- Does the design ensure that all critical components within a given system have manual overrides and/or manual controls?
- Does the design support mechanisms to routinely check the integrity of PLC ladder logic or other PLC programming languages and diagrams, as well as check for any unauthorized modifications to ensure correct operation?

5.2. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

6. ASSET AND CONFIGURATION MANAGEMENT

In addition to selecting the assets that will be included in the system, the hybrid energy system designer must consider how the assets will be configured and managed. Selection of configuration parameters has the potential to make a system more or less cyber resilient. For example, a device may support both Modbus and REST secure communication protocols, but the designer must choose a protocol and configure the system to use it. This section discusses asset and configuration management choices that a designer should make.

6.1. Storage of Design Information

Objective: Safeguard design documentation and configurations.

- Design Storage best practices:
  - Is design information stored in an encrypted format?
  - Are access controls (authentication and authorization) enabled for design repositories?
  - Are regular backups of design files performed?
  - Are network diagrams updated regularly to reflect both the IT (Information Technology) and OT (Operational Technology) networks?
  - Does the operator apply the principles of least privilege and need-to-know for individuals' access to network diagrams?
  - Are access control and audit logs implemented to monitor and restrict who can view or modify network diagrams?

6.2. Asset Inventory

6.2.1. Purpose and Importance

An accurate asset inventory provides a comprehensive view of all components within the hybrid power plant. It includes renewable energy sources (solar panels, wind turbines), energy storage systems (batteries), control devices (PLCs, RTUs), and communication infrastructure (routers, switches, firewalls, servers, workstations). A comprehensive asset inventory is important for these functions:

- **Maintenance Planning**: Knowing all assets and their configuration enables effective maintenance scheduling and resource allocation.
- **Risk Assessment**: Identifying critical assets helps prioritize security measures.
- **Performance Optimization**: Tracking asset performance over time enables data-driven decisions and vulnerability tracking.
- **Threat Detection**: Automates detection and investigation of new assets on the network to find unauthorized devices; identifies assets at risk due to outdated software/firmware.

6.2.2. Asset Identification and Classification

Evaluate the design's use of asset tags and labels.

- Does the design account for assignment of unique identifiers (tags or barcodes) to each asset?
- Does the design include information such as asset type, location, and installation date?

Classification criteria considers the following:

- Does the design support categorizing assets based on their function (generation, storage, control)?
- Does the design consider grouping by technology (solar, wind, battery)?

6.2.3. Data Collection and Central Repository

Evaluate how data is collected and stored across the hybrid power plant.

- Does the design support gathering of data from various sources?
  - **Installation Records**: Details from initial setup
  - **Maintenance Logs**: Records of repairs, replacements, inspections, firmware upgrades, and software upgrades/patches
  - **Sensor Data**: Real-time performance metrics.
- Does the design include a digital repository (database, EAM system) for asset information?
- Does the design support discovery and collection of attributes such as these:
  - Asset ID
  - Location (geospatial coordinates)
  - Manufacturer
  - Model
  - Warranty details
  - Maintenance history

6.2.4. Regular Updates and Audits

- **Scheduled Audits**: Does the design enable periodic physical audits to verify asset existence and condition?
- **Dynamic Updates**:
  - Does the design support inventory updates as new assets are installed or decommissioned?
  - Does the design support inventory updates for upgrades and repairs?
  - Are field personnel trained in tracking changes to assets or configurations in the asset inventory?

6.2.5. Asset Inventory Effectiveness

Evaluate the effectiveness of the asset inventory design:

- **Completeness**: Does the design enable an inventory that covers all assets?
- **Accuracy**: Does the design support ensuring the inventory information is up-to-date and reliable (e.g., automated device discovery – moves, adds, changes)?
- **Integration**: Does the design ensure that the inventory is integrated with other systems (e.g., maintenance, procurement)?

6.3. Backups for Critical Functionality

6.3.1. Purpose and Importance

Backups serve as a safety net, allowing the system to recover quickly from failures, whether due to hardware issues, cyberattacks, or natural disasters. In hybrid power systems, critical functionality includes energy generation, control, and communication. Backups should be factored into the design to do the following:

- **Minimize Downtime**: Backups enable rapid restoration, minimizing downtime during failures.
- **Mitigate Risk**: In case of component failure, backups ensure uninterrupted operation.
- **Recover from Disasters**: Backups are crucial for disaster scenarios (e.g., extreme weather events).

6.3.2. Types of Backups

Objective: Assess the hybrid system design's backup strategy including these aspects:

- Data Backups
  - **Objective**: Preserve critical data (configuration files, historical data, control logic).
  - **Actions**:
    - Does the design enable regular back up of data to secure storage (onsite and offsite)?
    - Does the design require encrypting data in transit as well as at rest?
    - Does the design support automated backup processes?
    - Does the design facilitate the testing of data restoration procedures?
- Configuration Backups
  - **Objective**: Capture system configurations (PLC programs, Supervisory Control and Data Acquisition (SCADA) settings).
  - **Actions**:
    - Does the design enable documentation of configurations?
    - Does the design establish nominal/standard configurations?
    - Does the design enable logging of changes to configurations, as well as flag changes made that deviate from nominal values/ranges?
    - Does the design ensure that backups are stored securely?
    - Does the design enable version control for changes?
- Redundant Components
  - **Objective**: Deploy redundant components (e.g., redundant relays, inverters, controllers).
  - **Actions**:
    - Does the design include spare components for critical infrastructure items (i.e., one spare component for every N active components)?
    - Does the design support automatic failover to redundant components?
- Communication Path Redundancy
  - **Objective**: Ensure communication continuity.
  - **Actions**:
    - Does the design use multiple communication paths (e.g., cellular, satellite, wired)?
    - Does the design have failover mechanisms for communication failures?

6.3.3. Testing and Validation

- **Regular Testing**: Does the design support periodic testing of backups and failover mechanisms?
- **Scenario Testing**: Does the design enable failure simulation (e.g., component breakdown, cyberattack) to validate backup effectiveness?

6.3.4. Effectiveness of Backups

- **Recovery Time Objective (RTO)**:
  - Does the design set criteria for how quickly critical functionality is restored?
  - Does the design enable automated backups of all digital components?
  - Does the design enable frequent testing of restoration procedures (e.g., weekly)?
  - Does the design stipulate the retention period for backups?
- **Data Integrity**:
  - Does the design include mechanisms to verify that data is accurately backed up?
- **Redundancy Level**:
  - Does the design include redundant components for all critical functions?

6.4. Endpoint Hardening

6.4.1. Purpose and Importance

Endpoint hardening focuses on reducing vulnerabilities and minimizing attack surfaces at the device level. In the context of hybrid power systems, endpoints include servers, workstations, Internet of Things (IoT) devices, and control components (PLCs, RTUs). A design, which ensures endpoint hardening, provides these:

- **Threat Mitigation**: Hardened endpoints are more resilient to cyberattacks, reducing the attack surface exposure and likelihood of successful system compromise.
- **Resilience**: Strengthened endpoints enhance system resilience against both accidental failures and intentional attacks.
- **Compliance**: Many industry standards (e.g., NERC CIP, IEC 62443) mandate endpoint security practices.

6.4.2. Key Strategies for Endpoint Hardening

Objective: Assess whether the design enables effective strategies for securing endpoints in hybrid power systems:

- Patch Management
  - **Objective**: Design facilitates identification of vulnerabilities as well as updates to fix software and firmware vulnerabilities.
  - **Actions**:
    - Does the design support automated vulnerability scans and reporting?
    - Does the design facilitate tracking of vulnerability disclosures from hardware and software vendors?
    - Does the design support automated triggers to regularly apply security patches?
    - Does the design include mechanisms to prioritize critical vulnerabilities?
    - Does the design support testing of patches before deployment?
    - Does the design identify who is responsible for applying patches (job function for an operator's staff or automatically applied by vendor)?
    - Does the design support rollback of patches that are found to create operational issues?

    - Are there mitigations available if patches are not released for known vulnerabilities or if they cannot be applied for other reasons?
    - Is a timeframe included in vendor agreements by which patches must be released for critical and non-critical disclosed vulnerabilities?

- Software Upgrades
  - **Objective**: Design facilitates upgrades to software.
  - **Actions**:
    - Does the design support testing upgrades for equipment prior to deployment?
    - Does the design prescribe a time interval by which upgrades should be applied after their release?
- Secure Configurations
  - **Objective**: Configure endpoints securely from the outset.
  - **Actions**:
    - Does the design ensure that unnecessary services and ports are disabled?
    - Does the design ensure that strong authentication mechanisms are enabled (e.g., complex passwords, multifactor authentication)?
    - Does the design follow industry best practices (e.g., Center for Internet Security (CIS) benchmarks)?
    - Does the hardware have secure boot features?
    - Are applications running on the same machine properly segmented?
- Device Authentication
  - **Objective**: Ensure only authorized devices can access the network.
  - **Actions**:
    - Does the design require the use of digital certificates or secure keys?
    - Does the design implement network access controls (NAC)?

6.4.3. Endpoint Hardening Effectiveness

Objective: Assess endpoint hardening effectiveness.

- **Patch Expediency and Frequency**:
  - Does the design enable easy application of security patches?
  - Does the design support automated patching?
- **Configuration Compliance**:
  - Does the design enable endpoint configuration management according to security guidelines?
  - Does the design support automatic flagging of endpoints that are misconfigured?
- **Vulnerability Remediation Time**:
  - Does the design include mechanisms to quickly remediate identified vulnerabilities?

6.5. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

7. ACCESS MANAGEMENT

Access management is the aspect that helps determine who has access to what systems based on their organizational affiliation, role, and current tasking, as well as the mechanisms by which access is granted for systems or tasks. Strong access management practices can play a significant role in ensuring adversaries cannot execute attacks on objectives, even if they have compromised parts of the system, because they cannot access the final targets.

7.1. Purpose and Importance of Authentication and Access Control

Security and Authorization:

- Authentication: Verifies the identity of users or devices accessing the system. It ensures that a user is who they say they are.
- Authorization: Verifies if a user has permission to use a particular resource or access a system. It ensures that only authorized personnel can interact with critical components.
- Access Control: Methods for determining who or what classes of users can access specific resources (e.g., control interfaces, data logs). Proper access control prevents unauthorized modifications.

Protection Against Cyber Attacks:

- Weak authentication or inadequate access control can lead to unauthorized system manipulation, data breaches, and disruptions.
- Robust mechanisms safeguard against cybersecurity threats, including unauthorized commands or malicious code injection.

Data Integrity and Confidentiality:

- Authentication ensures that data exchanged between components remains untampered.
- Access control restricts access to sensitive information, preventing unauthorized leaks.

7.2. Design Assessment Questions for Authentication and Access Control

7.2.1. Authentication Mechanisms:

Multi-Factor Authentication (MFA):

- Does the design implement MFA for authorized personnel accessing control interfaces?
- Does the design require a combination of something the user knows (password) and something user has (smart card, token) or something the user is (biometrics)?

Digital Certificates:

- Does the design use X.509 certificates for secure communication between devices?
- Does the design require certificates to validate the authenticity of devices and prevent spoofing?

Remote Access:

- Does the design identify all points of remote access and ensure that strong passwords (no factory default passwords) and multifactor authentication control are in place?
- Are passwords for remote access stored encrypted or hashed, not in plaintext?
- Does the design specify password obfuscation on all remote settings panels?

- Does the design specify establishment of an allowlist the permits only authorized device Internet Protocol (IP) addresses during specific times of day?
- Does the design ensure logging of all remote logins as well as alerting and monitoring of access attempts?
- Does the system lock out a user after a specified number of unsuccessful login attempts?

7.2.2. Access Control Policies:

Role-Based Access Control (RBAC):

- Does the design require role definition (e.g., operator, administrator) and permission assignment based on roles?
- Does the design support restricted access based on job responsibilities?
- Are there policies in place to add, remove, or modify a user's role as their job function or employment status changes?

Access Zones:

- Does the design divide the plant into zones (e.g., turbine area, battery storage)?
- Does the design apply access control rules based on zone criticality?

7.2.3. Metrics Collection for Assessing Access Control and Authentication

- Does the design support collection of the following authentication metrics:
  - Authentication Success Rate: Measures the percentage of successful authentications. A high success rate indicates robust authentication mechanisms.
  - Authentication Latency: Evaluates the time taken for authentication. Low latency ensures efficient user access.
  - False Positives and False Negatives: Assess the rate of incorrectly accepted (false positives) or rejected (false negatives) authentication attempts.
  - Password Strength Metrics: Analyze password complexity (e.g., length, character diversity) to prevent weak passwords.
- Does the design support collection of the following access control metrics?
  - Access Requests per Unit Time: Tracks the frequency of access requests. Sudden spikes may indicate anomalies.
  - Access Approval Rate: Measures the percentage of access requests approved. High approval rates suggest effective access control policies.
  - Least Privilege Violations: Identifies instances where users have excessive permissions. Minimizing violations enhances security.
  - Access Revocation Time: Evaluates how quickly access is revoked when needed (e.g., employee termination).
- **RTO**:
  - Does the design include recovery mechanisms for access control breaches as well as set RTOs?
  - Note: Shorter RTO indicates better resilience.
- **Mean Time Between Failures (MTBF)**:
  - Does the design enable measurement of the average time between access control failures?
  - Note: Higher MTBF indicates greater resilience.

- **Incident Response Time**:
  - Does the design include mechanisms to assess how swiftly the system responds to unauthorized access attempts?
  - Note: Swift response minimizes damage.

7.3. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

8. NETWORK ARCHITECTURE

The network architecture specifies the digital devices for a system and how they are connected to enable communications supporting business functions. This can include segmentation of networks, placement of firewalls, selection of protocols, and requirements for routing equipment. Network segmentation is closely tied to the required functionality of the system, the users that have access to the system, and the communications to connect them.

8.1. Network Segmentation

8.1.1. Purpose and Importance

Network segmentation involves dividing the network into distinct segments or zones based on functionality, security requirements, and risk levels. In the context of hybrid power plants, effective segmentation provides several benefits:

- **Security Isolation**: Segmented networks prevent an attacker from easily moving laterally across the entire infrastructure. Compromising one segment does not automatically grant access to others.
- **Reduced Attack Surface**: By limiting communication paths, the attack surface is minimized. This is crucial for protecting critical components like control systems and SCADA networks.
- **Compliance**: Many industry standards (e.g., NERC CIP, IEC 62443) mandate network segmentation as a security best practice.

8.1.2. Segmentation Strategy Assessment

Objective: Assess the strategies used in segmenting the networks within the hybrid power plant.

- Does the design implement functional segmentation?
  - **Objective**: Group devices based on their functions (e.g., generation, distribution, monitoring) and isolate networks based on resource type (e.g., solar, wind).
  - **Implementation**:
    - **Control Network**: Includes PLCs, remote terminal units (RTUs), and other control devices.
    - **Monitoring Network**: Houses sensors, meters, and monitoring equipment.
    - **Corporate Network**: For administrative tasks (email, office applications) but isolated from critical systems.

Note*: For devices that perform both monitoring and control functions, recommend that the Purdue architecture be leveraged, separating low OT level controls (Tiers 0–2) from platform/plant level controls (Tiers 3–5).*

- Does the design implement physical segmentation?
  - **Objective**: Physically separate network segments to prevent unauthorized access.
  - **Implementation**:
    - **Separate virtual local area networks (VLANs)**: Does the design use VLANs to isolate traffic?
    - **Air Gaps**: Does the design have the capability to physically disconnect critical systems from external networks (e.g., the internet)?
- Does the design implement security zones?
  - **Objective**: Define security zones with varying levels of trust.
  - **Implementation**:
    - **DMZ (Demilitarized Zone)**: Between the corporate network and external networks (e.g., the internet). Hosts public-facing services (e.g., virtual private network (VPN) gateways, web servers).
    - **ICS Zone**: Contains critical control systems. Access restricted to authorized personnel.
    - **Engineering Zone**: For system maintenance and updates.

8.1.3. Effectiveness of Network Segmentation

When assessing network segmentation, consider the following metrics:

- **Number of Segments**: Does the design implement enough network segments to allow finer-grained control, balancing increased complexity in network management?
- **Segment Isolation**: Does the design include a high degree of isolation between segments?
- **Access Control**: Does the design include comprehensive access rules (firewall rules, ACLs) governing communication between segments?
- **Redundancy**: Does the design enable redundant paths for critical communication?
- **Monitoring**: Does the design ensure visibility into each segment for anomaly detection?

8.2. Firewall Placement

8.2.1. Purpose and Importance

Firewalls act as the first line of defense against unauthorized access, malicious traffic, and cybersecurity threats. In the context of hybrid power plants, their strategic placement ensures the protection of critical systems and data.

8.2.2. Zones and Segments

Objective: Assess how the following zones are incorporated within the hybrid power plant's design.

- Corporate Zone (IT Network):
  - Contains administrative systems.
  - Firewall Placement:
    - Between Corporate Zone and External Networks: Does the design include a firewall to protect administrative systems from external threats (e.g., internet-based attacks)?
  - Rules:
    - Allow necessary outbound traffic (e.g., web access).
    - Restrict inbound traffic to authorized services (e.g., VPN gateways).

- Industrial Control System (ICS) Zone:
  - Houses critical control systems (PLCs, RTUs, SCADA).
  - Firewall Placement:
    - Between Corporate Zone and ICS Zone: Does the design isolate ICS components from corporate networks?
    - Between ICS Zone and Vendor Connections: Does the design isolate ICS components from vendor networks?
    - Within the ICS Zone: Does the design separate disparate functions within the ICS Zone?
  - Rules:
    - Allow minimal communication (only essential services).
    - Block unnecessary traffic (e.g., file sharing, remote desktop).
- Engineering Zone:
  - Used for system maintenance, updates, and engineering tasks.
  - Firewall Placement:
    - Between ICS Zone and Engineering Zone: Does the design control access to engineering systems?
  - Rules:
    - Permit authorized engineers' access.
    - Limit exposure to critical systems.
- DMZ (Demilitarized Zone):
  - Interfaces with external networks (e.g., grid interconnection, internet, vendors).
  - Firewall Placement:
    - Between DMZ and External Networks: Does the design protect public-facing services?
    - At Grid Connection Point: Does the design include a firewall at the point of interconnection between HRES and the grid?
  - Rules:
    - Allow specific services (e.g., VPN, web servers).
    - Monitor traffic for anomalies.
- Additionally, the design should ensure that all human machine interfaces (HMI), such as the touchscreens used to monitor or make changes to the system or PLCs, are disconnected from the public-facing internet. If remote access is necessary, implement a firewall and/or VPN with a strong password and multifactor authentication to control device access.

8.2.3. Firewall Placement Effectiveness

Objective: The previous firewall-related section includes questions about firewall placement to enable network segmentation. This section focuses on general firewall placement. Evaluate firewall placement based on the following.

- **Number of Firewalls**:
  - More firewalls increase complexity but enhance security.
  - Does the design include enough firewalls to enhance security and protect vital network segments?

- **Placement Effectiveness**:
    - Evaluate the strategic positioning of firewalls to reduce risk.
    - Does the design position firewalls in ways which provide comprehensive coverage of power system devices and communication system devices?
- **Rule Complexity and Effectiveness**:
    - Assess firewall rules (ACLs, NAT rules).
    - Does the design ensure firewall rules are clear, specific, and enforced?

8.3. Protocol Requirements

Objective: Select and use secure communication protocols.

- Use of encrypted protocols (e.g., TLS, HTTPS, SSH).
    - Does the design support use of encrypted protocols for all communication paths?
    - Are unencrypted protocols blocked, where possible, by firewall rules?
- Compliance with industry standards.
    - Does the design support use of standardized communication protocols?
    - If proprietary vendor protocols are required, can the protocols be vetted for security practices?
- Adherence to IEEE 1547.
    - Does the design adhere to IEEE 1547, which requires one of the following?
        - SunSpec Modbus
        - DNP3
        - IEEE 2030.5.
    - Has the system been tested and certified under IEEE 1547.1?
- Does the design implement port-based NAC using 802.1X for authentication and authorization?
- Does the design require SNMPv3 with strong authentication and encryption for monitoring and management?

8.4. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

9. MONITORING

Monitoring contributes to cyber resilience by enabling the fast detection of issues or anomalies in performance data, communications data, or other tracked metrics. Quick detection means that the problem can start to be remediated faster, limiting potential impact of events or reducing downtime. From a security perspective, appropriate monitoring is necessary to detect when adversaries may gain access to a system and to assess what their objectives are.

9.1. Monitoring Tools

9.1.1. Purpose and Importance

Monitoring tools provide real-time visibility into various aspects of the hybrid power plant. Their role extends beyond performance monitoring; they also aid in fault detection, predictive maintenance, and security. Monitoring tools are used for the following functions:

- **Performance Optimization**:
  - Monitor energy production (solar, wind) and storage (battery charge/discharge)
  - Monitor voltage, frequency, and current at each asset and the PoC
  - Identify underperforming components and optimize system efficiency.
- **Early Detection of Issues**:
  - Anomalies in sensor data can indicate potential failures.
  - Early detection allows timely intervention and prevents downtime.
- **Cybersecurity Monitoring**:
  - Monitor network traffic for suspicious patterns.
  - Detect unauthorized access attempts or abnormal behavior.

9.1.2. Types of Monitoring Tools

Objective: Assess design in terms of its ability to monitor the overall system and subsystems.

- SCADA Systems
  - **Purpose**: Real-time monitoring and control of critical components.
  - **Functionality**:
    - Does the design enable data collection from all sensors and devices?
    - Does the design support visualization of system performance?
    - Does the design enable automated alarming for abnormal conditions?
    - Is the interval for data collection sufficient to respond to abnormal conditions?
- Data Historians
  - **Purpose**: Store historical data for analysis and trend identification.
  - **Functionality**:
    - Does the design support recording sensor readings over time?
    - Does the design enable performance comparisons (e.g., minute-to-minute, hour-to-hour, month-to-month, year-to-year)?
- Energy Management Systems (EMS)
  - **Purpose**: Optimize energy production and consumption.
  - **Functionality**:
    - Does the design enable metrics and controls to balance supply and demand?
    - Does the design enable metrics to forecast energy availability (solar irradiance, wind speed)?
    - Does the design support comparison of expected outputs to real outputs to help verify system performance?
- Cybersecurity Monitoring Tools
  - **Purpose**: Detect and respond to cybersecurity threats.
    - **Functionality**:
    - Does the design include multiple network intrusion detection systems (NIDS) based on segmentation?
    - Does the design include SIEM tools?
    - Can communication packets be collected to feed into the IDS and SEIM?

    - Are HIDS running on computing machines that enable this?
    - Does the end user have the tools and resources to monitor the data collected by cybersecurity tools and/or a monitoring service?

9.1.3. Integration and Interoperability

- **Holistic View**: Does the design integrate the monitoring tools to provide a holistic view of the hybrid system?
- **Interoperability**: Does the design ensure compatibility between different monitoring tools?

9.1.4. Effectiveness of Monitoring Tools

Objective: Assess how monitoring tools are implemented in the overall hybrid plant design.

- **Coverage**:
    - Does the design ensure monitoring of all critical components?
    - Note: Full coverage helps mitigate risk.
- **Granularity**:
    - Does the design specify collection of detailed data?
    - Note: Data granularity aids in troubleshooting and response to cyberattacks.
- **Real-Time Alerts**:
    - Does the design specify that alerts are timely and actionable?
    - Does the design specify that alerts are integrated with the incident response system?
    - Note: Real-time system alerts aid in the detection of security incidents.

9.2. Sensor Placement

9.2.1. Purpose and Importance of Sensor Placement

Sensor placement is crucial for accurate data collection, system monitoring, and overall performance of hybrid power plants. Properly positioned sensors enhance cyber resilience by providing timely information for decision making and early detection of anomalies.

9.2.2. Effectiveness of Sensor Placement in the Overall Design

- Data Completeness:
    - Does the design ensure that sensors and sensor data cover all plant components, including digital components (i.e. enable network monitoring)?
    - Key indicators: Percentage of operational sensors, spatial coverage, coverage across all subnets/ VLANs.
- Data Consistency:
    - Does the design support the ability to assess the consistency of sensor readings over time?
    - Key indicators: Standard deviation of sensor data, drift over calibration cycles.
- Sensor Redundancy:
    - Does the design include backup sensors?
    - Key indicators: Number of redundant sensors, failover time.
- Sensor Health Monitoring:
    - Does the design enable regular monitoring of sensor functionality and accuracy?
    - Key indicators: Sensor calibration frequency and response time to sensor failures.

- Early Anomaly Detection:
  - Does the design enable automated alarming and triggering of abnormal sensor conditions?
  - Does the design specify the speed at which sensors are designed to detect abnormal conditions (e.g., sudden wind speed changes, temperature spikes)?
  - Key indicators: Time to detect anomalies, false-positive rate.

9.3. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

10. RESPONSE

Incident response is a key part of cybersecurity. It is one of the core functions of the NIST Cyber Security Framework. Although incident response itself occurs while the system is in operation, there are choices that can be made in the design phase that will enable various incident response practices. If these choices are not considered at the design phase, it may be difficult to make changes while the system is in operation.

10.1. Incident Response Plan

Objective: Be prepared for security incidents.

Assess how effective the design is in enabling incident response activities.

- Does the design include a documented incident response plan, including the following?
  - Response team members, roles, communication channels, training requirements, and a central point of contact for coordination.
  - Complete inventory and documentation of critical assets and architecture.
  - Up-to-date list of contacts for vendors, utilities, and regulatory bodies.
- Does the design support regular incident response and recovery exercises?
- Does the design enable maintenance and active testing of processes and equipment needed during an incident?
- Does the design use security orchestration, automation, and response (SOAR) tools, including the orchestration and automation components as well as playbooks for common incidents (e.g., are containment actions automated, such as blocking malicious IPS, and are recovery tasks automated such as rolling back configurations)?
- Does the design enable isolation of the affected systems and/or components to prevent further spread?
- Does the design enable the storage and retrieval of data to investigate the root cause of the incident?
- Does the design support automated restoration of services?
- Does the design include functionality that aids in the validation of system integrity?

10.2. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

11. CONTROLS DESIGN

Controls design refers to mitigations that a system engineer can put in place to eliminate or mitigate consequences from digital devices even if they were to be compromised by malicious actors. We propose three (non-comprehensive) controls design categories for hybrid renewable energy systems (HRES).

11.1. Choice of Control Scheme

The engineer can choose to implement a central control scheme for the HRES, while also providing a redundant option to the individual components to enable them to function locally, without relying on a central controller. This is usually achieved by providing some local computation to the edge devices, which can then use local measurements to continue to operate. The operation might result in a degraded performance, which is not optimized by a central controller, but will enable the system to still be functional, mitigating the risk of a malicious actor taking the entire HRES plant offline.

Objective: Assess whether the design supports the following control capabilities.

- Does the central hybrid power plant controller offer the ability to operate in centralized and decentralized/distributed mode?
- Does the decentralized mode offer similar capabilities and performance as the centralized mode?
- Is the central controller capable of identifying communication failures or malicious activity in the system to move to a more robust configuration?
- Is the decentralized mode robust enough to support resilient performance with communication failures/malicious actors in the system?
- Are the individual solar/wind/BESS controllers capable of operating in local-only mode in case of communication failure to the central controller?

11.2. Increase in Observability

Observability refers to the ability of the system operator to observe (i.e., gain measurements from the HRES) to enable them to properly estimate the system state using applications such as state estimation. For critical portions of the HRES, the operator can choose to augment existing measurement mechanisms with additional sensors or use computational techniques to provide redundancy. This control will ensure that even if a sensor is being manipulated or taken offline by a malicious actor, the operator retains the ability to estimate the system state.

System observability is measured using an observability metric. This is defined for a given system: when the initial state, , of a system can be deduced given a set of inputs, , and outputs, the system is said to be observable in time steps. An alternate definition is for a system with system matrix A, input matrix B, and output matrix C, the system is said to be observable if the observability matrix, , is fully ranked.The engineer can choose to deploy additional sensors in the network or increase observability on the network using techniques, such as correlational measurements [where data from adjacent sensors is used to mathematically infer the measurements from the lost/compromised sensors], which increases the observability of the network in case a particular sensor is compromised.

Objective: Assess whether the design provides increased observability.

- Is the base system completely observable (measured by verifying if system observability matrix is fully ranked)?
- Are there engineering mitigations (such as correlational measurements) in place to enhance observability if some of the sensors fail/are compromised?

11.3. Increase in Controllability

Similar to observability, controllability refers to the ability of the operator to control a portion of the HRES using the tools and techniques available to them. For critical portions of the HRES, the operator can choose to augment existing control mechanisms with additional controls to mitigate against potential cyber consequences. This is measured using the controllability metric, which is defined below.For example, in a power distribution system, the operator may have tap changers and voltage regulators which allow the operator to control the voltage of the feeder. In a scenario where these traditional controls are compromised, the system operator can plan on having auxiliary control mechanisms, which allow them to still control the system to mitigate high consequence events.

When each state, , can be moved to the desired state in a finite amount of time by using a control input, , the system is said to be controllable. For a system with system matrix A, input matrix B, and output matrix C, the system is said to be controllable if the controllability matrix, C, is fully ranked. The system engineer can choose to deploy additional control mechanisms (such as a fuse to isolate the compromised sections of the system or a reconfiguration control algorithm, which will achieve a similar effect) to mitigate high consequence events.

Objective: Assess whether the design provides increased controllability.

- Is the base system completely controllable (measured by verifying if system controllability matrix is fully ranked)?
- Are there engineering mitigations (such as power network reconfiguration/isolation schemes) in place to enhance controllability if some of the control components fail/are compromised?

11.4. Quantitative Scoring Approach

In the scoring matrix, assign weights to each subcategory above.

Score each category by answering yes/no to the questions above using the scoring matrix.

12. CONCLUSION

This application guide provides concrete considerations for the design choices that a system engineer will make to affect the cyber resilience of a hybrid energy system. The considerations provided are not an exhaustive list of all options, tradeoffs, or elements that a designer may need to consider, but they are intended to help evaluate scores in each of the design aspects identified by the Cyber-Resilience Framework for Hybrid Energy Systems.

Users should leverage this guide during the design process to inform the selection of devices, physical and network topologies, configurations, and software deployment. The guide can also be used to develop policies for the implementation and operation of the system, including vendor agreements that require a standard of care for maintaining cyber resilience by original equipment manufacturers (OEMs), service providers, and other third parties.

Following the implementation of the guide, the user can evaluate the relative cyber resilience of the design using the associated spreadsheet to calculate a score for each aspect, which is weighted according to the priorities set by the user. The scores can help a user evaluate different design tradeoffs across all the aspects or evaluate the cyber resilience of a system over time as changes are made in the production environment.

13. REFERENCES

1. McCamey, D. 2021. “Are Hybrid Systems Truly the Future of the Grid? NREL’s Magic 8-Ball Says: ‘Concentrate and Ask Again.’” Accessed May 28, 2024. https://www.nrel.gov/news/features/2021/are-hybrid-systems-truly-the-future-of-the-grid.html.

2. Bolinger, M., W. Gorman, J. Rand, and S. Jeong. 2023. "Hybrid Power Plants: Status of Operating and Proposed Plants, 2023 addition." Lawrence Berkeley National Laboratory, Berkeley, CA. Accessed March 19, 2024. https://emp.lbl.gov/sites/default/files/empfiles/hybrid_plant_tracking_2023_08.08.2023.pdf.
3. Venkataramanan, V., Culler, M., and H. Ackenhusen. 2024. "Cyber-Resilient Design Framework for Hybrid Energy Systems." Accessed July 2, 2024. https://www.nrel.gov/docs/fy24osti/90058.pdf