Cyber Resilient Design Framework for Hybrid Energy Systems

Venkatesh Venkataramanan[1] and Megan Culler[2]

1 National Renewable Energy Laboratory
2 Idaho National 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-5T00-90058
September 2024

Cyber Resilient Design Framework for Hybrid Energy Systems

Venkatesh Venkataramanan[1] and Megan Culler[2]

1 National Renewable Energy Laboratory
2 Idaho National Laboratory

Suggested Citation
Venkataramanan, Venkatesh and Megan Culler. 2024. Cyber Resilient Design Framework for Hybrid Energy Systems. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5T00-90058. https://www.nrel.gov/docs/fy24osti/90058.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-5T00-90058
September 2024

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

NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

List of Acronyms

CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CIE	cyber-informed engineering
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
DOE	U.S. Department of Energy
EIA	U.S. Energy Information Administration
HRES	hybrid renewable energy system
IBR	inverter-based resource
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
NERC	North American Electric Reliability Corporation
OT	operational technology
RESCue	Renewable Energy and Storage Cybersecurity Research
SAM	System Advisor Model

Table of Contents

List of Figures

List of Tables

1 Introduction

To facilitate the clean energy transition, the combination of renewable resources (primarily wind and solar energy) with energy storage to make the resources dispatchable, is of increasing interest. These systems are often referred to as a "hybrid renewable energy system" (HRES). These constitute an increasing share of the electricity mix in the United States (EIA 2023). These HRES have a wide range of configurations—e.g., colocated versus independent, virtual power plants, full versus partial hybrids—with specific cybersecurity challenges, such as rapid communications between subcomponents, rapid communications between the HRES and the grid, an increased attack surface, the interoperability of legacy and new equipment, and the potential use of third-party components with an unsecure supply chain (DOE 2021). This work describes a cyber resilient design framework for hybrid energy systems, performed as one of the research thrusts under the CESER-funded Renewable Energy and Storage Cybersecurity Research (RESCue) project. The RESCue project also hosts a hybrid renewable energy cybersecurity consortium, whose inputs have also been solicited and have been incorporated in this report.

Many hybrid plants are currently being developed and deployed, and some existing solar/wind plants are currently being upgraded to hybrid plants with energy storage, so there is an opportunity to consider cyber resilience during the design phase of these plants. Considering that adding energy storage makes these systems dispatchable, hybrid plants present a distinct advantage over independent solar/wind energy plants. This work proposes a concrete framework for designing HRES that leverages existing design best practices for cyber resilience, such as the concepts of cyber-informed engineering (CIE) (CESER 2024), Secure by Design (CISA 2023, 2024), and the cyber resiliency engineering framework (CREF) from the National Institute of Standards and Technology (NIST) *Special Publication 800-160, Volume 2* (SP 800-160) (NIST 2021). The framework identifies key system design and engineering considerations for HRES for various stakeholders to enhance their cybersecurity posture of the system.

The scope of this work is driven by the fact that many hybrid plants currently waiting for approval in the U.S. transmission system interconnection queue consist of a combination of wind, solar, and energy storage technologies (DOE 2024). This work focuses only on colocated plants—resources connected to the same point of connection at the transmission voltages; it does not consider virtual power plants (VPPs), or distributed energy resources (DERs) connected directly to the distribution system. Hybrid plants connected at the transmission level have a higher potential impact on the bulk electric system, while the impact of individual DER sites is lower. The focus is on colocated plants rather than VPPs since, from a design perspective, VPPs are considered as two or more separate sites designed and built separately, but managed together. The design decisions discussed in this framework apply best to a single site. Though designed to address the challenges of a limited scope of HRES, the framework is extensible to other deployments such as DERs in distribution systems with minimal adjustments. Considerations for other deployments of renewable energy systems will be included as part of the future work for this task.

2 Cybersecurity Challenges for Hybrid Renewable Energy Systems

There are several key technology development challenges facing HRES (DOE 2021):

1. Rapid communications between subcomponents: HRES typically consist of multiple components that require reliable, high-speed, and low-latency communications to support advanced grid functions and operate efficiently. This drives an increased importance of cybersecurity of disparate digital components and communications, introducing new challenges in ensuring the security of the combined system.
2. Rapid communications between HRES and the electric grid: HRES must communicate with the broader electric grid to ensure optimal operation participation in energy markets etc., However, these communication channels can be vulnerable to cyberattacks and require new methods for federated trust.
3. Increased attack surface: The integration of multiple subcomponents with varied security capabilities (usually from different vendors) in HRES can increase the system's attack surface, making it more susceptible to cyber threats.
4. Interoperability of legacy and new equipment: HRES often integrate legacy equipment with newer technologies, requiring careful consideration to ensure seamless interoperability without compromising security.
5. Potential use of third-party components with an unsecure supply chain: HRES components sourced from third parties could introduce security risks if their supply chains are not adequately understood or secure.
6. Control of HRES using distributed energy resource management systems (DERMS): Managing HRES using DERMS introduces complexities because it requires coordination among different technologies and subsystems.
7. Potential reliance on remote connections: HRES can potentially rely on multiple remote connections for monitoring and control from various vendors, original equipment manufacturers (OEMs), utilities, and other stakeholders. This can increase the complexity of cybersecurity considerations, especially when diverse stakeholders have access and ownership boundaries need to be defined.
8. Ownership boundaries are often unclear: HRES system components can be owned by a combination of entities, say the energy storage component and wind/solar component can have different owners.

These challenges have also been discussed with the RESCue consortium for incorporating industry feedback. In addition to these challenges, we note that there is a lack of guidance on cybersecurity or cyber-resilience in operational standards for HRES. IEEE Std 2800-2022 is the Institute of Electrical and Electronics Engineers (IEEE) Standard for Interconnection and Interoperability of Inverter-Based Resources (IBRs) Interconnecting with Associated Transmission Electric Power Systems (IEEE 2022). It includes considerations for performance requirements for the reliable integration of IBRs into the bulk power system, including, but not limited to, voltage and frequency ride-through, active power control, reactive power control, dynamic active power support under abnormal frequency conditions, dynamic voltage support under abnormal voltage conditions, power quality, negative-sequence current injection, and system protection. Cybersecurity, however, is absent. Also, it is not featured in the interconnection requirements set by the various independent system operators (ISOs). Both IEEE

Std 2800-2022 and the transmission interconnection requirement procedures refer to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards when providing guidance on cybersecurity. However, the NERC CIP standards are applicable only to plants that are already approved for grid connection, and although they provide requirements for their operation, they do not provide guidance on their design. Standards such as IEEE Guide 1547.3 are also referenced in IEEE Std 2800-2022; however, IEEE Guide 1547.3 primarily focuses on distributed energy resources, not utility-scale IBRs. Finally, neither IEEE Guide 1547.3 nor NERC CIP include guidance on cyber-resilience, which is an important factor considering that there is no silver bullet to security, and systems need to be designed with graceful failure and acceptable levels of performance requirements in case of cyber consequences.

Given that resilience is highly system dependent, and because determining the acceptable level of performance during a contingency is primarily a system owner-operator's decision, there is ambiguity in the definition of resilience for HRES. In this work, resilience is considered the HRES ability to meet its capacity and grid support commitments in the case of contingencies. Once resilience is defined, the next step is to quantitatively measure resilience. A report from the National Academy of Sciences, Engineering, and Medicine, titled *Enhancing the Resilience of the Nation's Electricity System*, states, "without some numerical basis for assessing resilience, it would be impossible to monitor changes or show that community resilience has improved" (National Academies of Sciences, Engineering, and Medicine 2017). In this work, we present a method of quantifying the impact on HRES cyber-resilience due to various design choices made by the system designer.

3 Existing Design Methodologies, Frameworks, and Philosophies

As part of this effort, a wide variety of design methodologies were considered to survey the current best practices for HRES. HRES deployments are gaining prominence, but there are currently no design frameworks or tools that consider the cyber-resilient design of these systems. Note that several tools and frameworks exist for the power system design and control system design of HRES, such as the National Renewable Energy Laboratory's System Advisor Model (SAM)[1] and REopt®[2], but these tools do not consider the design of the interdependent cyber and physical infrastructure nor offer recommendations for the design of the communication and cyber systems.

Several methodologies and recommendations provide guidance for the design of resilient cyber-physical systems. Of these, three methodologies are analyzed here in more detail because they provide the most pertinent guidance for HRES. These include the concepts of CIE (CESER 2024), Secure by Design (CISA 2023, 2024), and the CREF (NIST 2021). It is important to survey existing best practices and adapt the recommendations for specific applications to avoid redundancies and reduce the barriers to implementation by avoiding the costs of practitioners having to learn completely new design methodologies for their systems.

3.1 NIST Cyber Resiliency Engineering Framework

The cyber resiliency engineering framework focuses on creating cyber-resilient systems by applying concepts from systems security engineering and resilience engineering to develop survivable, trustworthy, secure systems. The framework intends to provide engineered systems with the capability to "anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources" (NIST 2021). This will enable users to minimize disruptions to critical functions, organizational and business impacts, and other damage from consequences originating from digital devices in cyber-physical systems. The framework is comprehensive and presents several cyber-resilience constructs, which include goals, objectives, techniques, approaches, and design principles. The authors recommend that organizations select, adapt, and use some or all the cyber-resilience constructs as required for their specific system. This work uses the constructs of design principles, techniques, and approaches, with a few modifications, which will be described in the later sections.

3.2 Secure by Design

Secure-by- Design (and secure-by-default) concepts are proposed by the Cybersecurity and Infrastructure Security Agency (CISA), an organization under the U.S Department of Homeland Security (CISA 2023, 2024). The term ``Secure by Design" includes both concepts of secure by design, and secure by default[3]. Secure-by-Design principles emphasizes the importance of "software manufacturers to make secure by design and secure by default the focal points of product design and development processes" (CISA 2024). Secure by Design is an effort to shift

[1] See https://sam.nrel.gov/.
[2] See https://reopt.nrel.gov/tool.
[3] https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf

the cybersecurity risk from the end consumers or users to the technology manufacturers, and hence it encourages every technology manufacturer to build their products based on reducing the burden of cybersecurity on customers, including preventing them from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions. Secure-by-Design principles also emphasize adding security features, such as the automation of configuration, monitoring, and routine updates. In addition, CISA encourages manufacturers to take ownership of improving the cybersecurity posture for their customers by incorporating Secure-by-Design practices to break the vicious cycle of constantly creating and applying fixes.

3.3 Cyber-Informed Engineering

The concept of CIE was originally proposed by Idaho National Laboratory, and it has been championed by CESER (CESER 2024). CIE extends secure-by-design concepts beyond the digital realm to include the engineering of cyber-physical systems. CIE introduces cybersecurity considerations at the earliest stages of system design, before the incorporation of software and security controls. It calls on engineers to identify engineering controls and design choices that could eliminate or mitigate the impacts of cyber-induced consequences on key system functions. This approach recognizes the role of engineering teams, not only cybersecurity teams, to enhance the cyber resilience of their systems by using the physics of engineering controls.

4 Cyber-Resilient Design Framework for Hybrid Renewable Energy Systems

This section describes the proposed cyber-resilient design framework. The intent of the proposed framework is not as a replacement for the existing state-of-the-art methodologies that were described in the previous section but rather to combine the best practices to provide comprehensive guidance for HRES. The design framework is intended to provide directly applicable guidance for developers, owner-operators, and engineering, procurement, and construction (EPC) contractors of HRES. This design framework adapts current best practices from the NIST CREF, CIE, Secure by Design.

All three methodologies provide guidance from different perspectives:

1. NIST CREF– cyber resiliency from a system security engineering approach
2. CISA Secure by Design – Focuses on secure software
3. DOE CIE – focused on engineering mitigations (what an engineer would do, and not what a security professional would do)

We attempt to combine the guidance from all three approaches and contextualize it for HRES.

Adaptation from NIST CREF: As discussed, NIST recommends that organizations choose from and adapt the proposed cyber-resilience constructs. In this work, we used the strategic design principles, the structural design principles, and the corresponding Techniques and Approaches. The strategic design principles and the structural design principles from the CREF (such as Focus on Common Critical Assets and Reduce Attack Surfaces) are adapted to HRES by replacing them with the CIE principles and secure-by-design principles to provide both operational technology (OT) and information technology (IT) principles and mitigations. NIST includes a library of 14 standard Techniques (such as non-persistence, privilege restriction, realignment, and redundancy) that can be used (in addition to other engineering-based techniques) to implement the principles. The Approaches provide the actual methodologies for implementing the techniques to align with the strategic design and structural design principles. In our proposed framework, we retain the same library of Techniques and Approaches as the methods of implementation for increasing cyber resilience. Considering that methods for improving cyber-resilience is not in the scope of this work, readers are encouraged to directly refer to CREF to implement the right Approaches and Techniques.

We also introduce two new cyber-resilience constructs: design aspects, which are specific parameters about which system designers need to make a decision; and design metrics, which build quantification into the framework. These changes are introduced to provide increased context for HRES, and they allows us to enumerate more details than are included in the CREF and that are applicable to all cyber-physical systems in general.

Our proposed framework is presented in Figure 2; it is modeled based on the NIST CREF.

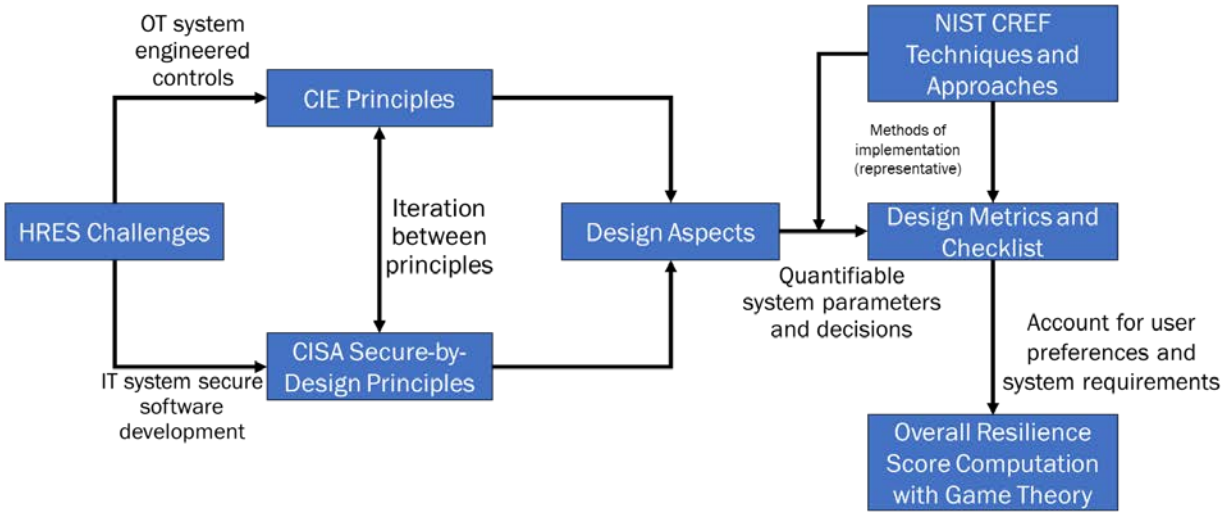

Figure 1. Overview of our proposed cyber-resilient design framework

Design principles: For cyber-physical systems, design principles are the guidelines and design considerations that the architects apply to support better decision making. In other words, design principles are the value statements describing the critical goals of the concerned system serving and benefiting the end users. For the proposed cyber-resilient design framework for HRES, the principles are directly derived from CIE and secure by design by mapping them to address specific challenges in these systems.

Design aspects: Design aspects are the second element in the hierarchy of a cyber-resilient system. For a cyber-physical system, the design aspects are the core characteristics that define the design elements' contribution to the system's cyber resilience. In this work, we propose creating two-tiered aspects: The first tier includes the main aspects that the designers need to make decisions about, and the second tier includes the subaspects that can be chosen per the constraints of the HRES. This allows for flexibility in choosing different design metrics to track performance over time, as will be explained in the next subsection. The following list shows the aspects in these two tiers:

1. Vendor selection and management (IT, OT)
    A. Vendor technical and process acumen
    B. Vendor security practices
    C. Vendor risk profile
    D. Vendor collaboration
2. Device selection and management (IT, OT):
    A. Power system device selection (OT)
    B. Communication system device selection (IT).
3. High consequence scenarios
    A. Identification of high consequence scenarios
4. Asset and configuration management:
    A. Storage of design information (IT, OT)

   B. Asset inventory (IT, OT)
   C. Backups for critical functionality (IT)
   D. End point hardening (IT).
5. Access management:
   A. Access control (IT, OT)
   B. Authentication (IT).
6. Network architecture:
   A. Network segmentation (IT)
   B. Firewall placement (IT)
   C. Protocol requirements (IT)
7. Monitoring:
   A. Monitoring tools (IT)
   B. Sensor placement (IT, OT).
8. Response:
   A. Incident response plan (IT, OT).
9. Controls Design:
   A. Choice of control scheme (central versus distributed) (OT)
   B. Increase observability (OT)
   C. Increase controllability (OT).

For the purpose of this report and its application, a system designer is not a singular entity; it usually comprises (1) designers at the owner-operator level who will determine the broad goals and objectives; (2) designers at the engineering, procurement, and construction firms; and (3) a collection of finance, OT, and IT personnel whose input and approval is needed before final deployment. For more in-depth implementation strategies, the reader can directly refer to the CIE (CESER 2024), secure-by-design (CISA 2024), and CREF (NIST 2021) documentation.

Adaptation from CIE and Secure by Design: In this framework, we attempt to map the specific challenges to HRES to design principles from the different methodologies (CIE, secure by design, and the CREF) to create contextualization specific to HRES. Note that this mapping of specific principles to address specific challenges to HRES is representative and is not the *only* appropriate way of addressing these challenges. The intent of this mapping is to provide an intuitive way of using these principles to directly address HRES challenges and to reduce the barriers for system designers to engage with the framework. In actuality, the CIE and secure-by-design principles are quite broad, and a number of combinations are possible for their application for HRES. Figure 1 shows a Sankey diagram illustrating the potential combinations of CIE and secure-by-design principles mapped to the specific design principles used for HRES in this work. The diagram illustrates that multiple principles can be used to address various challenges, but it is important to consider a combination to specifically address challenges across both IT and OT systems.

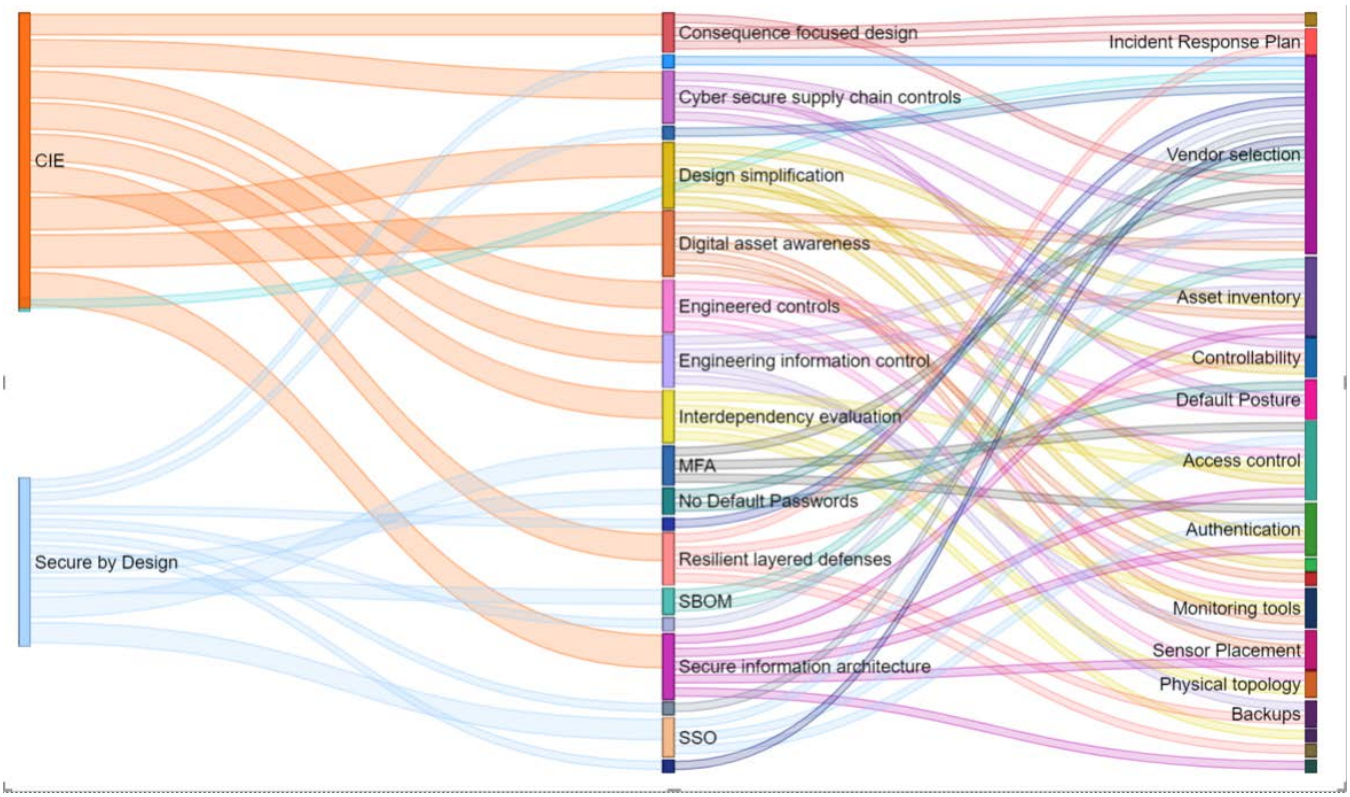

Figure 2. Sankey mapping of CIE and secure-by-design principles to design aspects

Considering that CIE proposes to mitigate cyber-induced consequences using engineering methods, and considering that secure-by-design principles provide approaches to design secure software and products, it becomes important to consider both approaches when developing a comprehensive framework for HRES. There is overlap between both CIE and secure-by-design methodologies, but ultimately, both these methodologies need to be used together to make decisions on design aspects. All the principles from CIE and secure by design are equally important and applicable to address challenges, and providing a mapping enables both the system design engineer and the IT security professional to jointly approach the implementation of the best practices from a tangible starting point. Not all CIE and secure-by-design principles have been used in this framework, and engineering judgement is used to create a mapping from HRES challenges to specific CIE and secure-by-design principles. A few of the assumptions and engineering intuition behind the mapping is detailed below.

Some principles are straightforward to map to the challenges, whereas other challenges can be addressed using different principles or a combination of principles. For example, Challenge 5 from Section 2 (supply chain considerations), has a direct mapping to the CIE principle of cyber-secure supply chain controls and to the secure-by-design principle of mandating a software bill of materials. But this direct mapping becomes more challenging for a different problem, e.g., the interoperability of legacy and new equipment. The CIE principle chosen to address this concern is engineered controls, which is designed to implement controls to reduce avenues for attack or the damage that could result from a successful attack. An example of an engineered control to address interoperability would be to use automated isolation devices, which could range from simple fuses or a reconfiguration algorithm, to isolate equipment that might have been

compromised. On the secure-by-design principle, it is important to identify the risk profile from the vulnerabilities present in older, legacy equipment, and to catalog that information.

Interoperability challenges could also be addressed using the CIE principle of digital asset awareness, which aims to understand what and where digital assets are used, which functions they are capable of, and any assumptions about how they work. For example, when adding an energy storage and photovoltaic arrays to an existing wind plant to create a hybrid plant, it is important to consider which features the hybrid controller might have (such as Volt/VARcontrol) that might not be available on the wind plant and wind turbine controllers. It is important to enumerate other such features that exist and to evaluate the effect of sending these control signals to the wind plant. If this is not performed, it could result in an attacker using these "unused" functions to create unintended consequences. Considering these challenges from an engineering point of view would also enable the system designer to better mitigate the risks from interoperability challenges between legacy and new equipment. Similarly, the secure-by-design principle of defense-in-depth can be used to suitably harden legacy equipment and address interoperability. To reduce the burden of implementation for system engineers, a representative mapping among the challenges, CIE and secure-by-design principles, and design aspects is presented later in Table 1. Using the presented mapping will provide OT and IT engineers a head start before pursuing a deeper dive into both CIE and secure-by-design methodologies.

Table 1. Mapping Between HRES Challenges, Design Principles, and Design Aspects

#	Challenge	Challenge to CIE Principle	Challenge to Secure by Design Principle	Challenge to Design Aspects
1.	Rapid communication between subcomponents	Design simplification	Secure by design—secure hardware and software components	Network architecture
2.	Rapid communication between HRES and grid	Interdependency evaluation	Secure by design—memory safe programming, parametrized queries (more relevant for communications to control center)	Device selection and management
3.	Increased attack surface	Digital asset awareness	Secure by default—secure logging	Monitoring
4.	Interoperability of legacy and new equipment	Engineered controls	Secure by design—common vulnerability and exposure (CVE) completeness, vulnerability disclosure programs	Engineered controls
5.	Potential use of third-party components with unsecure supply chain	Cyber secure supply chain controls	Secure by design—software bill of materials (SBOM)	Access management
6.	Control of HRES using plant controller → How is it different from individual technologies?	Resilient layered defenses	Secure by design—defense-in-depth	Vendor selection and management
7.	Heavier reliance on remote connections	Planned resilience	Secure by default—multifactor authentication (MFA), default passwords	Asset configuration and management
8.	Ownership boundaries need to be defined	Secure information architecture and engineering information control	Secure by default— – MFA, single sign-on (SSO)	Response

Design metrics: The last element of the proposed framework of a cyber-resilient system design is the design metrics. The metrics are the evaluation of the system design to measure whether they reflect organization- or system-specific assumptions, priorities, and constraints. The design metrics of a cyber-resilient system should reflect the evaluation or measurement of how much the system design elements contribute to the system's cyber resilience. The metrics can be used either to directly measure a specific design aspect—e.g., the number of network segmentations—or as observability and controllability metrics. To increase the ease of implementation, however, the metrics are designed as responses to an evaluation tool, where a series of yes/no questions are formulated that the system designer will answer when performing an assessment. The responses are then assigned a binary value, and they are eventually combined into a weighted resilience score. The scoring matrix is explained in detail in Section 5. It is important to note that the metrics are not meant to be absolute, and are chosen with subjectivity involved. Resilience is inherently unique to specific systems/deployments, and hence trying to quantify it with a tuple of metrics or an aggregated metric (as will be discussed in the next section) will always result in losing some nuance. The user may choose to use a different set of metrics that may be more suitable for their objectives in measuring performance of design aspects. The metrics are intended to be used to compare designs and evaluate cyber-resilience effects of design tradeoffs, and are not meant to compare different sites/deployments.

5 Cyber-Resilience Score Formulation

The cyber-resilience of a particular HRES depends on the individual deployment's functions and requirements. For example, a HRES inside a critical military installation might have different requirements than a smaller HRES owned by an independent power producer. To account for these differences, we propose a game-theoretic scoring mechanism that can directly quantify the user's preferences. It includes two levels of weighting: a simple weighting for the subaspects and a game-theoretic weighting for the aggregated aspects. The same weighting mechanism can be used for both levels, to either simplify or be more comprehensive in the weighting choices. This choice is left to the end user, but an example methodology incorporating both options is presented below.

We propose the following method to determine the score for each aspect – each sub-aspect is weighted equally. Each sub-aspect is broken down into a series of questions in the application guide (which is provided as a standalone document as a companion to this work), and hence all the questions contribute equally to the ultimate score of an aspect (Ackenhusen 2024). This set of questions was developed using industry best practices and subject-matter expert review, but the questions may not be entirely comprehensive and may miss certain considerations for certain designs. Although this is a weakness in this scoring mechanism, there are a large number of questions (340 in total), which means that for each aspect, the user's answers to the questions should provide a good measure of maturity in that aspect. In probability, the law of large numbers states that as for a collection of independent, random samples, as the number of samples increases, the average result of those samples converges to the true value. This concept helps support the rigor of this scoring method. Additionally, this method is objective, the yes-no questions should have a known answer based on the design of the system, and repeatable, different people should be able to evaluate the same system and get the same results despite any biased perceptions they may have. After answering all of the questions, the user will have a score between 0 and 1 for each aspect that represents the percentage of questions answered affirmatively for that aspect.

For the nine main design aspects, the user is prompted to go through a game-theoretic mechanism that offers an opportunity to critically weigh one design aspect against another using a pairwise comparison, and it uses the inputs from this comparison to create a weighting for the design aspects. This offers two advantages: (1) It accounts for user preferences in the definition of resilience, considering the importance of a particular challenge/aspect; and (2) it forces the user to consider the trade-offs that are implicit in weighting one aspect over another, offering a critical view of the impact of design decisions on resilience.

There are various multiple-criteria decision-making (MCDM) frameworks that can be used for this application; the analytic hierarchical process (AHP) has been chosen in this application. Other decision-making frameworks include analytical network process, Choquet integral, etc. The user can even choose to directly assign weights based on their preferences without going through the pairwise comparison process, but apart from losing the advantages specified here, there is no way of ensuring consistency among user weights and their alignment with the design goals and principles. The AHP can use the concept of fuzzy measures (Grabisch 2015), where the relative importance of one aspect over another is not measured in absolute terms but in fuzzy terms, which offers the advantages of the mathematical stability of the final measure (i.e.,

consistency among the choices made during the comparison) and a wider tolerance in the design choices. Initially, the user is asked to consider how importance one design aspect is over another—e.g., vendor selection compared to incident response. A HRES operator that is particularly concerned about supply chain issues might choose to weight vendor selection, with higher importance, against response to ensure cyber resilience by design rather than responding to incidents. The user is asked to quantify this using the choices listed in Table 2, which is often referred to as the Saaty table because the method is based on Thomas L. Saaty's work (Saaty 2008).

Table 2. Saaty Table with the Options for Pairwise Comparison

Value	Definition	Comments
1	Equal importance	The two aspects contribute equally to overall resilience.
3	Moderate importance	Slightly favors one aspect over another
5	Strong importance	Strongly favors one aspect over another
7	Very strong importance	Very strongly favors one aspect over another—its dominance can be demonstrated
9	Extreme importance	The dominance of one aspect over another is demonstrated and absolute.
2, 4, 6, 8	Used to express intermediate values	
Reciprocity	Reciprocity of weights in pairwise comparison matrix	If aspect i has one of the above nonzero numbers assigned to it when compared with aspect j, then j has the reciprocal value when compared with i.

The fuzzy measures used here allow the user to specify a range of values in this comparison—e.g., if the user were to choose a value of 4, the fuzzy measure would be (3,4,5) to account for the differences when applied to a particular scenario. For ease of understanding, however, the process is described further with a single value instead of the complete fuzzy measure. Once the nine aspects are compared against each other using the pairwise comparison, a complete pairwise comparison table is formulated with all the user's inputs. This process can be completed by more than one designer to account for different priorities, and by using the AHP can combine these preferences into the final set of weights. An illustrative comparison is shown in Table 3.

Table 3. Illustrative Pairwise Comparison

	Vendor Selection and Management	Device Selection and Management	High consequence scenarios	Asset Config and Management	Access Management	Network Architecture	Monitoring	Response	Engineered Controls
Vendor Selection and Management	1	0.2	0.5	3	3	7	5	5	7
Device Selection and Management	5	1	0.75	0.75	3	3	3	5	7
High consequence scenarios	2	1.333333	1	3	3	7	5	5	7
Asset Config and Management	0.333333	1.333333	0.333333	1	1	0.5	0.67	1	7
Access Management	0.333333	0.333333	0.333333	1	1	1	1	0.67	7
Network Architecture	0.142857	0.333333	0.142857	2	1	1	3	3	7
Monitoring	0.2	0.333333	0.2	1.492537	1	0.333333	1	1	7
Response	0.2	0.2	0.2	1	1.492537	0.333333	1	1	7
Engineered Controls	0.142857	0.142857	0.142857	0.142857	0.142857	0.142857	0.14285714	0.142857	1

From the pairwise comparison, a relative weight for each aspect needs to be calculated, which can then be used to calculate the final weighted resilience score. Various calculation methods can be chosen to derive these relative weights, such as the approximate eigenvector method, the largest eigenvector method, and the geometric mean method. The geometric mean method can also support fuzzy measures if they are implemented during the pairwise comparison. This is given by:

$$Geometric\ mean = \left(\prod_{i=1}^{n} x_i\right)^{1/n} = \sqrt[8]{x_1 * x_2 \dots x_9}$$

Here, because the total number of aspects, n, is 9, the geometric mean is calculated using the ninth root of the product of each row (of individual aspects). The normalized geometric mean, which is calculated by taking the sum of the geometric mean for each aspect and normalizing the individual scores against the sum, is used as the final "relative" weights for each individual aspect contributing to the overall resilience of the HRES. The consistency of these choices can be verified by computing a consistency score as follows:

$$Consistency\ score = \frac{\lambda_p - n}{(n-1)}$$

where λ_p is the principal eigenvalue for the matrix, and n is the total number of aspects. The consistency score needs to be less than 0.1 for the overall weighting to be consistent. The user

needs to adjust their inputs to the pairwise comparison matrix if this score turns out to be inconsistent. The overall resilience score is given by:

$$Resilience(t) = \sum_{n=1}^{N} W_n S_n$$

where, $n = 1,2,3, \ldots, N$ which represent N aspects; $W = 1,2,3 \ \ldots, \ N$; represents weights from AHP; and S represents the evaluation metric score related to the n^{th} aspect. This overall procedure is provided as a companion Excel spreadsheet and is represented in Figure 3.

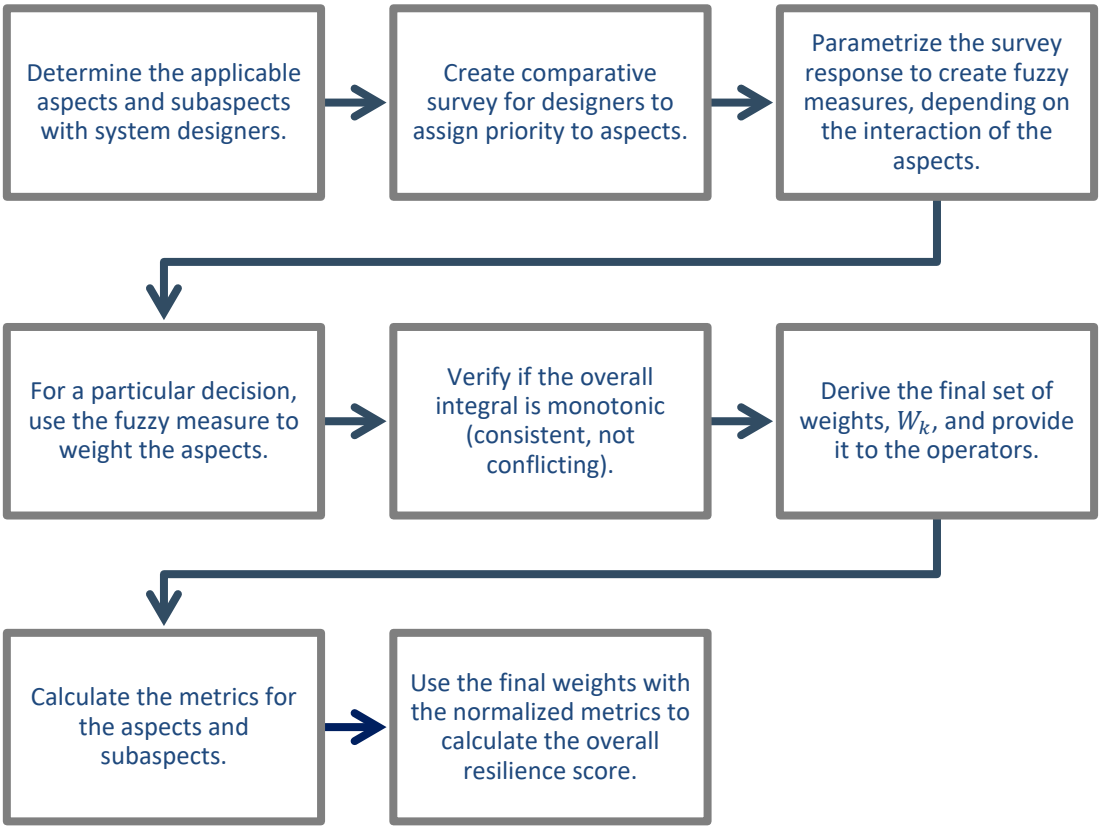

Figure 3. Overall resilience score computation process

The 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, 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. 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. 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, weakness, and recommendations to improve cyber resilience.

6 Conclusion

The cyber-resilient design framework provides a comprehensive methodology to address hybrid renewable energy systems challenges by combining current design best practices, such as NIST Cyber Resilient Engineering Framework (CREF) (NIST 2021), DOE's Cyber-Informed Engineering (CIE) (CESER 2024), and CISA's Secure by Design (CISA 2024). The overall framework is adapted from CREF and uses CIE and secure-by-design principles to address OT and IT challenges, and it proposes to use CREF *Techniques* and *Approaches* for implementation. The document is intended to be used by system designers (a collection of OT and IT security engineers across design firms, developers, owner-operators and installers) during system planning. This document also has a companion piece (Ackenhusen 2024) that enumerates a list of questions that the system designer can use to assess the cyber resilience of their existing systems or to assess the impact of design decisions on the system under development. A game-theoretic resilience scoring mechanism using the analytical hierarchical process (AHP) is also described; it can be used to quickly compare design decisions and their impact on the final resilience score. The game-theoretic mechanism allows the user to define "cyber-resilience" for their particular system and the corresponding impact of various decision aspects. Future iterations of this framework will refine the scoring mechanism based on user feedback, and we will consider reducing/expanding the aspects and their questions based on real-world use cases.

References

Cybersecurity and Infrastructure Security Agency (CISA). 2023. *Secure by Design: Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*. Washington, D.C.: U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.

———. 2024. "Secure by Design." U.S. Department of Homeland Security. https://www.cisa.gov/securebydesign.

Institute of Electrical and Electronics Engineers (IEEE). 2022. *IEEE Std 2800-2022 – Standard for Interconnection and Interoperability of Inverter-Based Resources (IBRs) Interconnecting With Associated Transmission Electric Power Systems*. Piscataway, NJ.

National Academies of Sciences, Engineering, and Medicine. 2017. *Enhancing the Resilience of the Nation's Electricity System*. Washington, D.C.: The National Academies Press. https://doi.org/10.17226/24836.

National Institute of Standards and Technology (NIST). 2021. *NIST SP 800-160 Vol. 2 Rev. 1 – Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. Gaithersburg, MD. https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final.

Office of Cybersecurity, Energy Security, and Emergency Response (CESER). 2024. "Cyber-Informed Engineering." U.S. Department of Energy. https://www.energy.gov/ceser/cyber-informed-engineering.

Saaty, Thomas L. 2008. "Decision Making With the Analytic Hierarchy Process." *International Journal of Services Sciences* 1 (1): 83–98.

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.

———. 2024. *Transmission Interconnection Roadmap: Transforming Bulk Transmission Interconnection by 2035*. Washington, D.C. https://www.energy.gov/sites/default/files/2024-04/i2X%20Transmission%20Interconnection%20Roadmap_1.pdf.

U.S. Energy Information Administration (EIA). 2023. "The Electricity Mix in the United States Shifts from Fossil Fuels to Renewables." *Annual Energy Outlook: Narrative—In This Issue*. March 16, 2023. https://www.eia.gov/outlooks/aeo/narrative/index.php#TheElectricityMixinth.

Grabisch, Michel. 2015. "Fuzzy Measures and Integrals: Recent Developments". *Fifty years of fuzzy logic and its applications*, pp.125 - 151, 2015, 10.1007/978-3-319-19683-1_8. hal-01477514

Ackenhusen, Heather, Culler, Megan J, Venkataramanan, Venkatesh. 2024. "Application Guide for the Cyber-Resilient Design Framework for Hybrid Systems". Idaho National Laboratory Technical Report, INL/RPT-24-78909. https://www.osti.gov/biblio/2403007