Hydropower Cybersecurity Value-at-Risk Framework

Anuj Sanghvi,[1] Ryan Cryar,[1] Jordan Smart,[1] Nate Evans,[2] Amanda Joyce,[2] and Stephanie Jenkins[2]

1 National Renewable Energy Laboratory
2 Argonne 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-5R00-84841
February 2023

Hydropower Cybersecurity Value-at-Risk Framework

Anuj Sanghvi,[1] Ryan Cryar,[1] Jordan Smart,[1] Nate Evans,[2] Amanda Joyce,[2] and Stephanie Jenkins[2]

1 National Renewable Energy Laboratory
2 Argonne National Laboratory

Suggested Citation
Sanghvi, Anuj, Ryan Cryar, Jordan Smart, Nate Evans, Amanda Joyce, and Stephanie Jenkins. 2023. *Hydropower Cybersecurity Value-at-Risk Framework*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-84841.
https://www.nrel.gov/docs/fy23osti/84841.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-5R00-84841
February 2023

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

NOTICE

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

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

Acknowledgments

This project benefits from the participation of several hydropower industry organizations, including the U.S. Bureau of Reclamation, the U.S. Army Corps of Engineers, the Centre for Energy Advancement through Technological Innovation Infrastructure Protection and Security Group, Delta-Montrose Electric Association, and Berkshire Hathaway Energy's PacifiCorp.

List of Acronyms

CCS	Critical Cyber System
CEATI	Centre for Energy Advancement through Technological Innovation
CERT	Computer Emergency Readiness Team
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
CSS	Cascading Style Sheets
CVF	Cybersecurity Value-at-Risk Framework
DC	Direct Current
DDD	Domain-driven Design
DER-CF	Distributed Energy Resource Cybersecurity Framework
DOE	U.S. Department of Energy
HTML	Hypertext Markup Language
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IT	Information Technology
IEEE	Institute of Electrical and Electronics Engineers
NERC-CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OT	Operational Technology
PLC	Programmable Logic Controller
UPS	Uninterruptible Power Supply

Table of Contents

List of Figures

List of Tables

1 Introduction

The Hydropower Cybersecurity Value-at-Risk Framework (CVF) was developed by the National Renewable Energy Laboratory (NREL) and Argonne National Laboratory with support from the U.S. Department of Energy (DOE) Water Power Technologies Office. The CVF is an industry-accessible tool for user-friendly, risk-based cybersecurity assessments. This report describes the tool and its role in improving the cybersecurity posture of hydropower plants and dams. The CVF provides facility owners and operators with valuable guidance and identifies next steps to mitigate risks, including scores that stakeholders can use to prioritize future cybersecurity investments. The CVF online tool[1] guides users through a detailed analysis of plant cybersecurity control practices. Users answer a series of questions, and their responses are compared against multidimensional criteria for the risk of environmental, operational, and economic impacts. The CVF considers factors such as system operational mode, configuration, and the availability of in-person staff for manual intervention to generate scores representing the likelihood of a cyberattack. The CVF assessment also generates scores that indicate the financial value of the possible consequences of specific risks for which cybersecurity improvements are required to withstand future threats. This report describes the CVF's approach to cybersecurity valuation through examination of several facility-specific factors, such as risk profile, security control implementations, cybersecurity resilience, the probability of an attack occurring, and the potential magnitude of negative consequences of improper implementation. Because all these factors are influenced by an organization's processes, requirements for support functions, and specific implementations of business processes and security controls, the tool evaluates these facility-specific differences to accurately assess and recommend mitigations for cybersecurity risks.

1.1 Background

Hydropower plants are an important part of not only the energy system, but also the local communities and environment. They provide flexible, renewable power and grid benefits, like spinning reserve, while often supporting many non-power purposes like flood control, irrigation, and recreation. As such, it is vital to maintain secure and reliable operation in an ever-evolving power system. As hydropower plants become increasingly integrated via advanced smart devices alongside legacy systems, it is critical to address the cybersecurity challenges that arise (Arturo D. Alarcón, 2018). Over 40 cyber-attacks in the past 20 years have targeted hydropower facilities, including both information technology (IT) and operational technology (OT) with a clear trend of increasing OT system focus (Whyatt, M et al., 2021). One barrier to deploying an effective program of cybersecurity measures is the lack of a formal methodology to assess the value of improving the hydropower cybersecurity posture. Without this guidance, it is difficult for hydropower plant managers to justify or prioritize investments in improving their plant's cybersecurity maturity and to harden their plants against cyberattacks.

1.1.1 Distributed Energy Resource Cybersecurity Framework

As part of an effort to assist under-resourced utilities, NREL's Energy Security and Resilience Center researchers conducted cyber-governance assessments using the DOE Cybersecurity Capability Maturity Model (CESER, 2022). From the assessments, NREL highlighted gaps in organizations' cybersecurity postures, including the need to strengthen the cybersecurity workforce development, to manage external dependencies, and to manage risk to the organization from distributed energy resources. To meet these challenges, and through support from the Federal Energy Management Program, NREL developed the

[1] https://cvf.nrel.gov/

Distributed Energy Resource Cybersecurity Framework (DER-CF) (Powell, Charisa 2019). The framework is a web-based application that enables energy managers and operational technology security staff to assess their cybersecurity posture and to generate a prioritized set of action items. The DER-CF also produces executive summaries, reports, and graphs as depicted in Figure 1 that highlight the need for management support in weaker areas. This self-assessment tool evaluates fundamental cybersecurity hygiene based on user input. The DER-CF tool is not focused on hydropower, so the capabilities of that tool were reconfigured and refined to develop the CVF tool for hydropower.

Figure 1. Distributed Energy Resource Cybersecurity Framework Dashboard.

2 CVF User Guide and Technical Manual

The Cybersecurity Value-at-Risk Framework (CVF) is implemented as an online web application that walks users through a series of questions to create a semiquantitative value-at-risk (VaR) score, as well as a prioritized set of recommended actions to improve cybersecurity posture. This section serves as both a technical manual describing how the tool was developed and configured to assess hydropower cybersecurity posture by NREL and a user guide describing how to interact with the tool. The technical manual is presented first in Section 2.1 to provide context before describing the user procedures in Section 2.2.

The report will refer to two roles, 1) the administrator (NREL) who created the CVF in its current form and 2) the user, who will complete the assessment within CVF by answering questions set up by the

administrator. The CVF tool was created with hydropower owners and operators as the target audience. To best utilize the tool, users should be aware of their plant systems, operations, and existing cybersecurity posture. However, the web application provides tooltips and additional information to aid users throughout the process. Additionally, all questions do not need to be answered to create a VaR score. For the context of the users, a control practice is a combination of assessments questions, answers (also called as control implementations), associated action items and metrics tagged to each question. For questions and assistance regarding the web application, please contact the authors at Anuj.Sanghvi@nrel.gov.

2.1 CVF Technical Manual

The CVF technical manual documents the background research that informed the assessment of cybersecurity controls and their organization into domains within the tool, as well as the backend mechanisms that enable CVF tool functionalities.

2.1.1 Assessment

NREL created the assessment by identifying domains and sub-domains of cybersecurity controls to organize the presentation of questions into a user-friendly interface. The CVF assessment structure is depicted below:

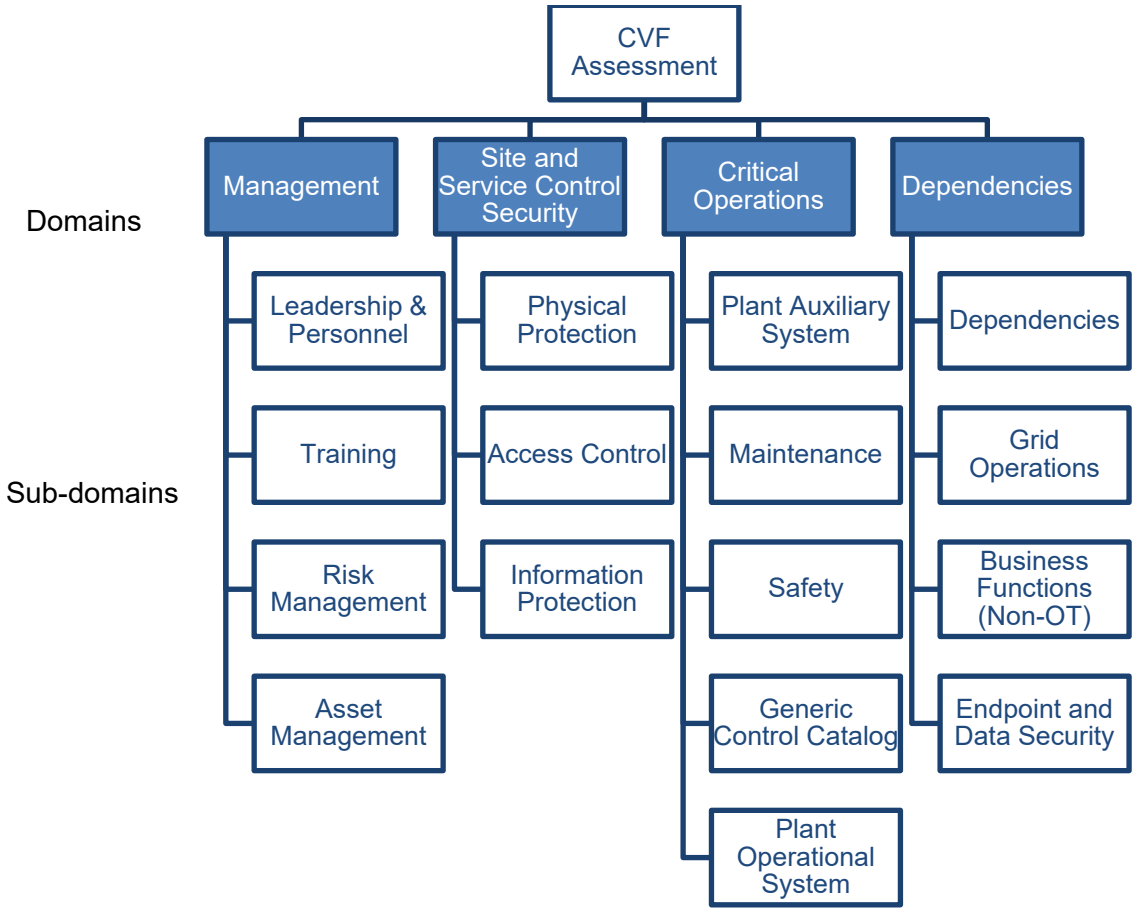

Figure 2. CVF assessment domains (at the top in solid boxes) and the subdomains (in the bottom branches with unfilled boxes).

Each of these sub-domains mentioned in Figure 2 above comprises a set of questions for the users to respond to. The hydropower valuation assessment includes cybersecurity controls that adhere and map to the NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) categories of Identify, Protect, Detect, Respond, and Recover which can be found in the appendix. Such categorization of controls along with mappings to NIST CSF enable appropriate identification of organization's personnel along with conforming to acceptable best-practices provided by NIST.
The following bullets describe the key components within CVF that are created by the administrator (NREL):

- **Control implementation details**: Each security control that was developed as part of the CVF's assessment stage, including authoring the practice, assigning an answer type, authoring the tailored recommendations/action items, and associating the implementation weights with the answers. Answers indicating the implementation level for each control result in a score between 0 and 1, with an associated set of action items where applicable. The implementation weights are a combination of scores to each answer about control implementation including follow-ups. These control implementation weight details allow the back end of the application to score the organization's cyber risk posture.
- **Impact categories**: The hydropower sector stands to gain the most value by addressing impact categories that are most likely to enhance cybersecurity and to reduce the potential for a high-consequence incident. The framework scopes these impact categories to associate each security control with its potential impact if it is poorly implemented.
- **Likelihood**: Factors that assist in calculating the probability of a threat event occurring are key inputs that are difficult to quantify accurately. Using the NIST Special Publication 800-30R1 (NIST, 2012) definitions for likelihood and risk determination, several factors for hydropower operations and system-level probability calculations were developed.

The underlying research and risk management principles leveraging the NIST SP 800-30 guidance follow impact and likelihood considerations based on the following examples in Table 1.

Table 1. Examples of Adverse Impacts.

Type of Impact	Impact
Harm to Operations	Inability to perform current missions/business function
Harm to Assets	Damage to or loss of physical facilities, systems, networks, technology, or equipment
Harm to Individuals	Injury or loss of life, identity threat
Harm to Other Organizations	Harm (eg. Financial) due to failure to deliver services
Harm to the Nation	Damage to critical infrastructure or loss of government continuity of operations

Some of the other hydropower-specific impact categories were also incorporated within the control metric development stage such as environmental and operational impacts to infer the outcomes of poorly implemented security control more accurately. Some of the likelihood factors were developed leveraging NIST's concept of the likelihood of attack initiation combined with the likelihood of attack occurrence. Although CVF's research did not include all the NIST likelihood factors involved, it arrives at a semi-quantitative likelihood score from control implementation scoring.

The assessment results are used to tailor a set of prioritized recommendations that enable immediate changes or modifications by facility operators. This informs a risk-based approach and improves decision-making. The CVF's outputs are:

- **VaR score**: The VaR score is based on the facility's risk posture and is a quantitative score proportional to the need for resource allocation (e.g., workforce, funding, or tools) in a given cybersecurity category.
- **Valuation guidance**: The CVF's assessment stage generates a list of prioritized action items and guidance that elaborates on the importance of avoiding the impacts of cybersecurity risks through valuing impacts. The valuation guidance can be used to articulate the loss in terms of equipment damage, operational downtime, and safety, which could be mitigated through cybersecurity investments.
- **Recommended action items**: A typical result of undertaking an assessment is to identify the steps to begin the next cycle of continuous improvement. The CVF provides recommended best practices specifically tailored to the hydropower valuation assessment. Items are populated within the applications Action Items tab as the questions are answered, and control implementation levels are scored.

2.1.2 Scoring Method

The CVF's dynamic approach to scoring the control implementations takes the user's response to each practice and analyzes the metrics tagged to each control practice to generate a score. The VaR score is calculated based on the formula below:

$$VaR = L*(1-CI)*I$$

L = Likelihood or the probability of an attack/event occurring and resulting in an impact

CI = Control implementations along with weights assigned to user's implementation of a control which represents unmitigated risks

I = Overall impact score using maximum recorded value for each impact category tagged per control

VaR scores range from 0.001 to 1 with VaR < 0.5 representing lower to moderate necessity to invest resources (workforce/funding/tools) to mitigate associated risks and VaR > 0.5 representing higher to extreme necessity to invest resources (workforce/funding/tools) to mitigate associated risks. Parameters tagged per control include metrics such as the NIST CSF categories, Impact categories, Confidentiality Integrity Availability (CIA) triad, Consequence categories, and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) relevance and allow the CVF to generate impact scores. The scoring method relies on a semi-qualitative impact scale ranging from low, moderate, and high, as described in Table 2, with each assigned to a numeric value.

Table 2. Scale - Impact of Threat Events.

Impact Qualitative Values	Description
High	Severe or catastrophic adverse effects on plant operations, assets, individuals, or the nation
Moderate	Serious adverse effects on plant operations, assets, individuals, or the nation
Low	Limited to negligible adverse effects on plant operations, assets, individuals, or the nation

2.1.3 Application Development Overview

The core application leverages the codebase and capabilities of DER-CF to achieve the design and objectives for CVF development. The repository of code is "forked" to exist independently of the original DER-CF repository codebase. This new stand-alone repository contains the modified components of the application to fit the needs of the CVF.

The architecture of the CVF is like that of the DER-CF; it uses domain-driven design (DDD) in its foundation. DDD is a set of practices in software development that aids in the overall development of the application. Breaking down the concepts into domain models, which are abstractions of business logic, can provide an understanding of the code from a business point of view (Laribee 2009). This design methodology was key to translating the practices and controls into a cohesive assessment because the design models were simultaneously built as the assessment matured over time. The domain models allowed a seamless transition from the business logic of the assessment, broken down into pillars, domains, and subdomains; to the code of the application itself. The models were developed by non-coders to enable a clearer division of labor and effectively manage time. This consistent approach allowed CVF to become part of a cohesive platform of tools supporting different applications.

The administrative side of the application enabled the team to build the assessment according to the design models that were laid out before the application was deployed and while the assessment controls were being developed. In this case, the team mapped the developed business logic into the domain models at the front end of the application, resulting in a user-friendly interface. Although much of the application could be developed from the repurposed components of the DER-CF, the overlay that made the CVF unique still needed to be developed. One DER-CF component that was modified for the CVF is question editing. When creating a question, the DER-CF allows the administrative user to change the criticality level of the control via a dropdown menu with options of low, medium, and high. Within the CVF, this functionality was changed from criticality to impact level. The impact level is how much impact a cyberattack might have if the control is not implemented. A weight is now assigned depending on how the question is answered, while maintaining the same process as the original application.

The administrator can tag questions with different metrics, which allows the application user to see information that is tailored to their own assessment experience. For example, using impact categories, defined as the area of operation that a potential attack might affect, the administrator can tag economic, environmental, operational, and/or safety as impacts, according to the question. The user can then select their answer to that question, and if the question is not answered with a high enough maturity level, the impact will be added to their final metrics. With the introduction of new question data, new charts were introduced to display the assessment results as the user progresses. These security controls and practices that were developed as a part of hydropower valuation catalog are associated with parameters used in the

scoring algorithm. These parameters are introduced within the administrator access of the application as metrics that are later represented as graphics to educate the user and to provide assessment outcomes in visual form. The control implementation along with tagged metrics represent the risk state of the CVF domains and is the source for calculating the VaR score. Figure 3 represents the CVF dashboard that includes graphs of the factors involved in valuation scoring. Some elements of the dashboard are explained above with more explanation within the application.

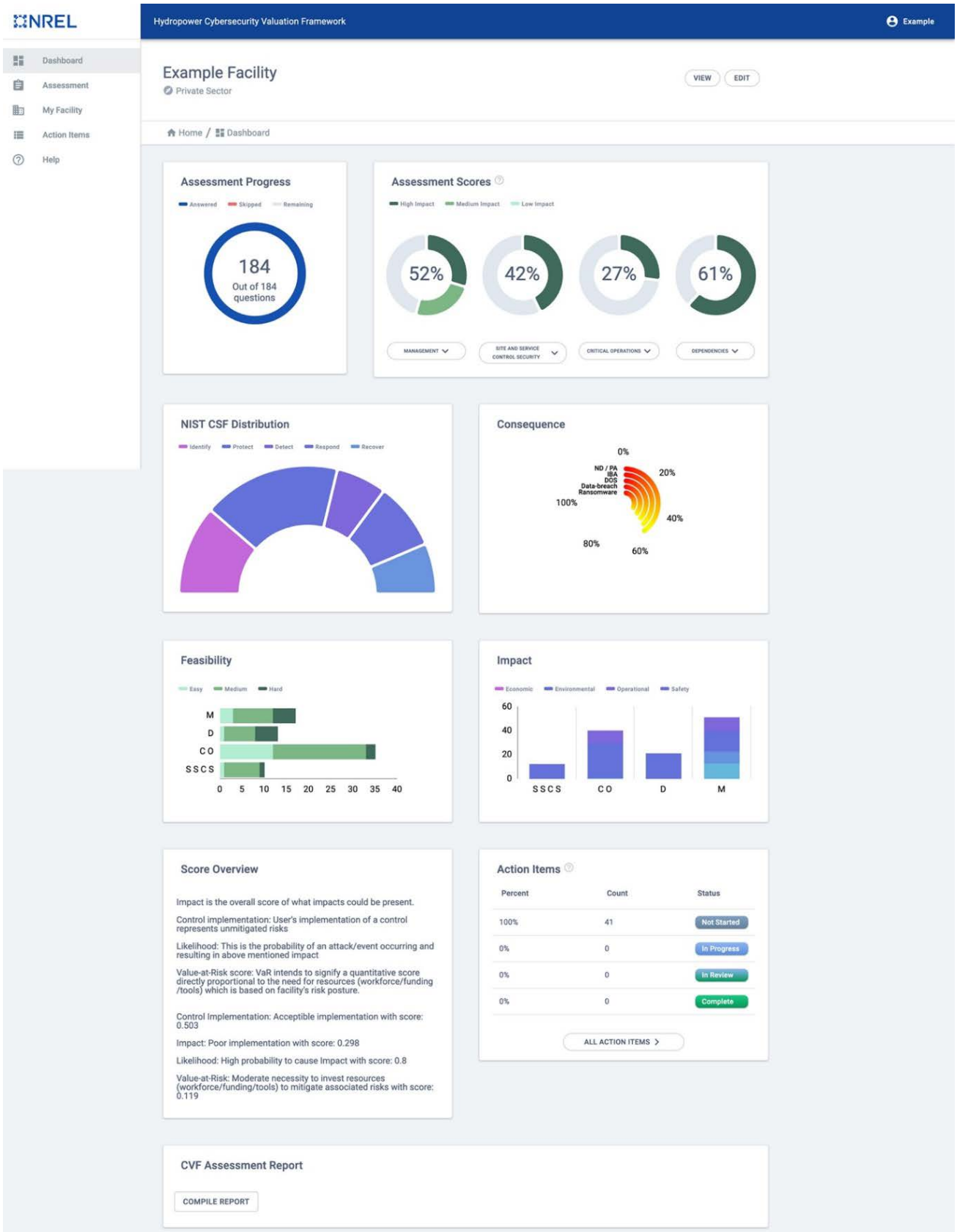

Figure 3. Snapshot of the CVF Dashboard.

2.1.4 Research

The phases of the CVF development consisted of a literature review of the existing standards to which hydropower facilities adhere. These standards have been developed for enabling conformity and reliability of hydropower operations and were used to develop hydropower specific requirements and industry challenges within CVF control practices development. Some include:

- Institute of Electrical and Electronics Engineers (IEEE) 1020: Guide for Control of Small Hydroelectric Power Plants [(IEEE, 2011)
- IEEE 1010: Guide for Control of Hydroelectric Power Plants (IEEE, 2006)
- International Electrotechnical Commission (IEC) 31010: Risk Assessment Techniques (IEC, 2019)
- IEC 62270: Guide for Computer-Based Control for Hydroelectric Power Plan Automation (IEC, 2013)
- Dams Sector Cybersecurity Capability Maturity Model (CISA, 2016)
- North American Electric Reliability Corporation Critical Infrastructure Protection (all) (NERC-CIP)

These standards influenced the final controls that made it to the assessment. To tie the application to the questions that were developed, it was necessary to enable the users to select responses that reflected the maturity of current practices. Many cybersecurity challenges are not binary, but a spectrum of maturity needing a more dynamic array of answers. To accurately reflect the posture, the maturity of a particular control was applied to each answer selection, where relevant. Maturity options included how much of a control had been implemented, on a scale from not implemented to fully implemented. If a control was only partially implemented, the user could assess whether their current implementation was appropriate for the current risk status. The questions also serve to identify the potential impact if a control was not implemented. This helps users understand how implementing a control influences their cybersecurity posture when viewing the report.

Table 3 shows the portion of the asset mappings that identified a set of critical hydropower operations, assets, and cyber-physical components that might be prone to manipulative attack scenarios. Addressing these mappings and authoring security controls and recommendations around them enhances the cybersecurity posture of the plant and, in turn, increases the security and resilience of the hydropower fleet.

Table 3. Hydropower System and Asset Mapping.

Hydropower System	Discipline and Assets	Critical Cyber Assets
Water conveyance operation	Gates, penstock, inlet valve, hydraulic actuators, water flow meter	Inlet valve/gate operation system, spill gate control system, powerhouse drainage system, water injection and wicket gate system, remote gate and dam operation system
Generator	Generator rotor and stator, exciter, protective relay, cooling water, air injection, carbon dioxide fire suppression, alarm system, governor	Condition monitoring system, vibration monitoring system, generation load control, generator circuit breaker, protective relay system, alarm system, governor control system
Turbine	Mechanical: turbine Electrical: turbine sensors	Speed sensor, hydro turbine control system, turbine shaft vibration monitoring system
Automation, control, and protection	Supervisory control and data acquisition system, networking equipment, human-machine interface, emergency shutdown system	Speed control and brake monitoring system, routers, switches, gateway devices (firewall, intrusion detection system/intrusion protection system), controller communication modules, fire and overspeed protection
Substation operation	Circuit switches, surge arrestors, transformers, line switches	Remote terminal unit, programmable logic controller, protective device, human-machine interface, gateway device
Plant auxiliary system	Station lighting, DC system—uninterruptible power supply and battery, diesel, and battery generator	Lighting plant control system, plant security system, plant DC monitoring system, diesel generator monitoring system

2.2 CVF User Guide

This section describes how users interact with the CVF tool to answer questions about control implementation and receive scoring and recommended actions to improve the security posture of their facility. The CVF consists of a user-friendly web interface that allows users to identify and assess cybersecurity risks and receive guidance and recommended next-steps. The application's landing page invites users to create a profile for their facility with an option to continue without account creation. Note: continuing with the assessment without creating a profile requires the users to finish answering all control implementation questions without letting the session expire and does not save any user-progress. Knowledgeable staff are asked to identify implementation details in response to several categories of questions about cybersecurity control practices. The CVF interface provides explanatory text where applicable detailing interpretation guidance. The following subsections focus on each of the dashboard pages accessible in the columnar menu on the left side of the dashboard.

2.2.1 My Facility

The user is prompted to optionally submit facility information to provide context for CVF assessment focus. Depending on organization's size and number of hydropower facilities, the My Facility tab will hold information about the facility undergoing the assessment. Future iterations will include the ability to add multiple facilities with respective assessments for an organization.

2.2.2 Assessment

The assessment page allows the user to step through the assessment in a series of domains and subdomains (Figure 2). As the user steps through each section answering questions about control implementation, the tool builds scores and recommendations reflecting the security posture. The interface keeps track of progress and highlights any missed items so that the user can easily return and complete them. In the following sections, the results from the assessment process will be displayed on a dashboard and used to compile a list of recommended actions.

2.2.3 Dashboard

As the CVF user progresses with answering control practices, the data being processed by the application is represented in the dashboard tab for the user to track progress and gauge performance. Some of the key graphical representations are explained below. Figure 4 shows the distribution of questions among the categories of the NIST Cybersecurity Framework (CSF) (NIST, 2018). NIST CSF core includes the functions and categories of Identify, Protect, Detect, Respond, and Recover, representing a robust classification of the security controls as they relate to these CSF categories. These categories form the basis to adhere to a more standardized approach, which is usually mandated within federally owned and operated power plants but can prove beneficial for the entire fleet. The example figure (Figure 4) divides the tagged control per NIST CSF categories and, upon click, one (in this case, Respond) expands to show the proportion of controls implemented for that category.

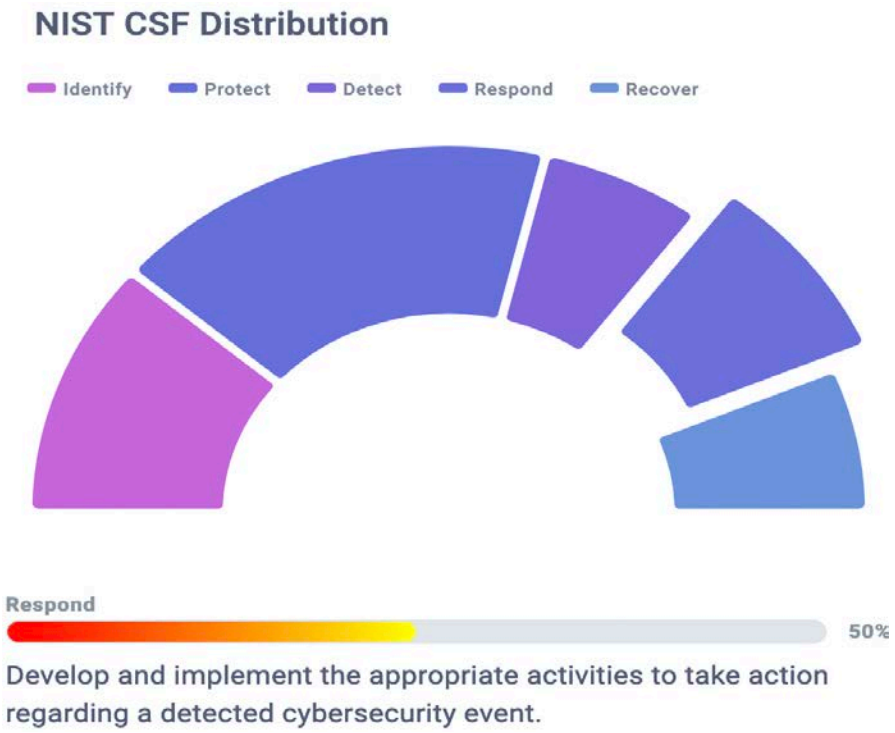

Figure 4. NIST CSF distribution of all questions.

The consequence category distribution (Figure 5) is a view of the consequences to which a facility is most susceptible. The categories of consequences are natural disaster/physical attack, integrity-based attack, denial of service, data breach, and ransomware. The annuli plot the total number of questions associated with a consequence category where responses indicate at least a medium posture. Within a consequence category, a higher proportion of controls implemented satisfactorily will result in annuli extending further

toward 100%. The gradient from red to green color indicates the reduction in risks or potential consequences resulting from control implementation.

Figure 5. Consequence categories by domain distribution based on assessments.

2.2.4 Action Items

When answers indicate a reduced cybersecurity posture, the tool identifies action items organized by impact (Figure 6). These action items are generated based upon what controls are not implemented and predefined linkages to the risks and potential consequences. For example, if a question is answered "no", indicating that a control has not been implemented, an action item is generated to indicate how that control might be implemented and the level of impact addressed. These action items are meant for the user to have an itemized list of recommended actions tailored to their assessment. These action items were developed with emphasis on hydropower sector leveraging the standards and frameworks mentioned in the Research section and the best practices were tailored to address the hydropower cybersecurity challenges. The CVF tool also allows progress to be tracked as the user updates status of action items from "not started" to "in progress" to "in review" to "complete". In addition, comments can be made to assign action items for users or to assess the status of the action item. The CVF's immediate feedback on action items, valuation guidance, and the VaR score enable users to identify and prioritize an approach to mitigating risks by implementing the suggested controls.

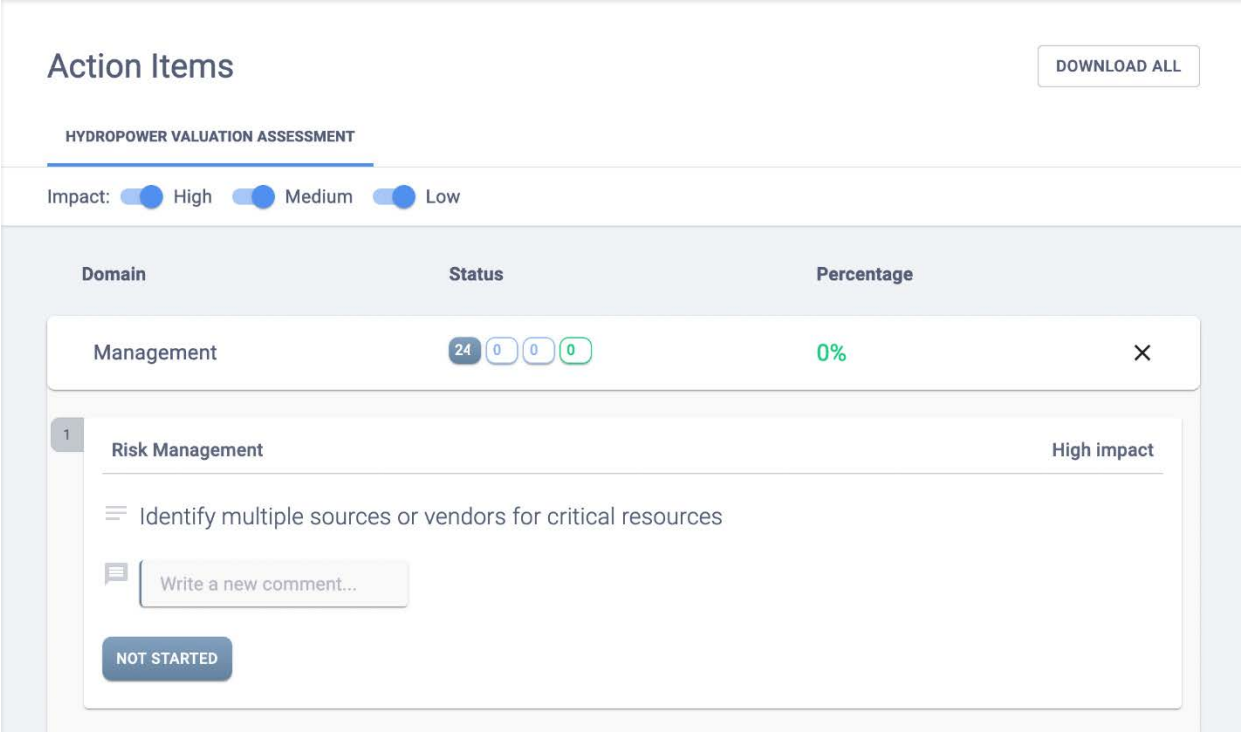

Figure 6. Example of the Action Items interface.

2.2.5 Report

The CVF application produces a downloadable report by dynamically inserting all the assessment information from the user into a Microsoft Word document to show the breakdown of the user's VaR score with associated graphics. The report includes an executive summary and detailed outcomes for next step. This report document acts as an editable template that can be downloaded and modified to further fit the needs of the user and their intended audience.

The report also acts as a record of security posture at the time of assessment, with the opportunity to return and retake the assessment, producing another report for comparison to reassess security posture over time.

3 End-User Engagement

To ensure the assessment was aligned with industry needs, , we engaged with several industry partners throughout the development of the application. This engagement culminated in a visit to a hydroelectric plant for a run-through of the assessment with one of our partners. Lessons learned through industry engagement helped to develop an application that both meets the needs of the industry members and challenges the industry to improve to a new level of cybersecurity posture.

3.1 Partners and Performance

With support from the DOE Water Power Technologies Office, the research findings and application development went through multiple reviews from industry partners, including the U.S. Bureau of Reclamation and privately owned utilities with a vast hydropower footprint. To further develop the application and receive key feedback, a discovery assessment needed to be conducted. An alpha version of the application was locally deployed for quick debugging or changes to reflect any feedback during the initial discovery assessment. The CVF alpha application underwent a discovery assessment process at an

operational hydropower plant with representatives from the plant present to answer and give feedback. Each item was answered, noting any clarifications needed or details that should be added to the question to improve the overall assessment process. The discovery assessment was performed over a period of 6 hours with site's OT security as well as IT security personnel answering over 200 questions about security control practices and implementation. Senior management was also involved within the assessment process for awareness and ensuring support for securing hydropower operations.

The constructive feedback received included various clarifications within the security controls as they relate to facility personnel and the development of parent practices for a hierarchical tree format of questions. With 4 domains and 15 subdomains that target different roles within an organization, the CVF recommendations are relevant to a variety of roles and responsibilities for cybersecurity practices. The CVF application is live for public use as of December 31, 2022 and can be found at https://www.cvf.nrel.gov.

4 Conclusion

The CVF takes a novel approach of conducting risk-based valuation assessments to guide the enhancement of hydropower plant cybersecurity. The next steps in growing the capabilities of the CVF are to improve threat identification by integrating the MITRE ATT&CK and the Common Vulnerabilities and Exposures (CVEs) systems. We intend to develop a pipeline for the automated tagging of threats to controls and for the automated analysis of CVEs that might be relevant to our systems. Other advancements of the CVF application will include an organizational view of cybersecurity risks, including multiple assessment results from different facilities within the organization. Reporting will be updated to include additional guidance and metrics as the application introduces more features to align with the assessment's maturity. The CVF provides a bird's-eye view of the value of investments in cybersecurity to enable enhanced decision making for stakeholders. As the valuations and guidance provided by the CVF are continually refined, the benefits to the cybersecurity posture of hydropower will continue to grow.

References

Arturo D. Alarcón, 2019. "Digitization: a revolution for the hydroelectric sector." https://blogs.iadb.org/energia/en/3286/.

Whyatt, Marie V., Thorsen, Darlene E., Watson, Mark D., Ham, Kenneth D., Pederson, Perry A., McKinnon, Archibald D., and DeSomber, Kyle R.. 2021. "Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021." https://www.osti.gov/servlets/purl/1899145.

NIST, 2018. "Framework for Improving Critical Infrastructure Cybersecurity." https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

CISA, 2016. "Dams Sector Cybersecurity Capability Maturity Model." https://www.cisa.gov/sites/default/files/publications/dams-c2m2-2016-508.pdf.

IEC, 2013. "Guide for computer-based control for hydroelectric power plant automation." https://webstore.iec.ch/publication/6682

IEC, 2019. "Risk management – Risk assessment techniques." https://www.iso.org/standard/72140.html

IEEE, 2006. "IEEE Guide for Control of Hydroelectric Power Plant." https://standards.ieee.org/ieee/1010/1465/

IEEE, 2011. "IEEE Guide for Control of Small (100kVA to 5 MVA) Hydroelectric Power Plants." https://standards.ieee.org/ieee/1020/5213/

NIST, 2012. "Guide for Conducting Risk Assessments." https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

CESER, 2022. "Cybersecurity Capability Maturity Model." https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Laribee, David. 2009. "Best Practice—An Introduction To Domain-Driven Design." *MSDN Magazine* 24 (2). Accessed December 8, 2022. https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/february/best-practice-an-introduction-to-domain-driven-design.

Appendices: Assessment Controls

This section contains a list of controls that can be found in the online assessment.

Table 4. List of assessment controls with the associated domain and NIST CSF categories.

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Management	Leadership and Personnel	Is there a manager/department in charge of day-to-day cybersecurity management of the entire facility	Identify
Management	Leadership and Personnel	Are there any other cybersecurity leaders with asset specific cyber responsibilities	Identify
Management	Leadership and Personnel	Is there a third-party contract arrangement for primary cybersecurity management for this facility	Identify
Management	Leadership and Personnel	Is there a third-party contract arrangement for primary cybersecurity management for a specific asset	Identify
Management	Leadership and Personnel	Are cybersecurity contractors or vendors used for day-to-day work	Identify, Detect
Management	Leadership and Personnel	Are background checks conducted for organizational, third-party, and supporting personnel	Identify, Detect
Management	Leadership and Personnel	Are recurring and periodic background checks conducted	Identify, Protect
Management	Leadership and Personnel	Are the cybersecurity positions formalized within the organization: Information Security Officer, Cybersecurity Policy and Planning Coordinator, Cybersecurity Incident Response Team Lead/ Commander, CERT Staff/ Triage Staff	Identify, Protect
Management	Leadership and Personnel	Does the organization have a policy that ensures authority and accountability for personnel having cybersecurity assignments	Protect, Detect
Management	Training	Do personnel (including third-party) complete annual security training	Protect
Management	Training	The basis of the training programs: Industry Recognized (ISO 27001), In-house/formal, Informal, Government-recognized	Identify
Management	Training	What is the frequency of continuation/refresher training	Protect
Management	Training	Are personnel trained in the following areas: Contingency, Server Administration, Network Administration, Incident Response, Threat Analysis, Risk Management	
Management	Training	Are cybersecurity personnel trained on the cybersecurity plan	Protect
Management	Training	Does the organization have a System Security Plan for OT	Identify, Protect
Management	Training	Has the organization established and documented a minimum level of training, education, and/or experience required for cybersecurity personnel	Identify, Protect
Management	Training	Does the organization maintain skills management as part of the performance monitoring process	Protect, Detect
Management	Risk Management	Does the organization have predefined plans for responding to cybersecurity incidents	Respond
Management	Risk Management	The organization has a defined incident response plan for handling cyber incidents, which (at a minimum) contains: Planned procedures for network	Identify, Protect, Respond, Recover

Domain	Sub-domain	Valuation Objective	NIST CSF Category
		containment(s), planned procedures for malware containment(s), plan procedures to rate limit in response to Distributed Denial of Service Attack, planned procedures to respond to an unauthorized access to OT sensitive information	
Management	Risk Management	Can cyber resources be isolated should there be a suspicion of compromise	Identify, Respond
Management	Risk Management	Does the organization perform an impact analysis to identify critical assets	Identify, Protect
Management	Risk Management	Once the main CCS is lost (without considering any redundant or alternative mode), what percentage of normal business function are lost or degraded	Identify, Protect
Management	Risk Management	Once the CCS is lost (without considering any redundant or alternative model), within what time period will the business be severely impacted	Respond, Recover
Management	Risk Management	Should the site become inoperable, does the organization have access to an alternative location	Recover, Respond
Management	Risk Management	How long does it take to fail over to the alternative site	Respond, Recover
Management	Risk Management	Does the organization have a documented continuity of operations plan	Recover
Management	Risk Management	Is annual contingency planning conducted on information systems including OT	Protect, Respond
Management	Risk Management	Can mission-critical processes be restored to pre-disruption state	Recover
Management	Risk Management	Are critical resources (i.e water, gasoline, etc) available through more than one source or vendor	Identify
Management	Risk Management	Are non-mission-critical resources recovered	Recover
Management	Risk Management	Is additional monitoring implemented during recovery process	Detect, Respond
Management	Risk Management	Does the organization have a defined and maintained document outlining courses of action based on cybersecurity threat	Identify, Protect
Management	Risk Management	If a course of action is listed, are corresponding threats or threat actors mapped	Identify, Protect
Management	Risk Management	Is this document frequently updated	Identify, Protect
Management	Risk Management	Can the organization's access control be changed if a threat or warning comes up	Respond, Protect
Management	Risk Management	Has the organization established points of contact when responding to a physical incident	Respond
Management	Risk Management	Can the organization deploy alternative resources rapidly	Protect, Respond, Recover
Management	Risk Management	Does the organization use shared threat information	Identify, Protect
Management	Risk Management	Which one or set of CCS assets if lost would cause the organization to go to an alternative site	Protect
Management	Risk Management	How many communities does the organization monitor	Protect, Respond
Management	Risk Management	Does the organization conduct cyber focused tabletop exercise	Identify, Protect
Management	Risk Management	Has the organization conducted a scheduled simulation/exercise to test course of action	Protect, Respond
Management	Asset Management	Is there an inventory of all critical assets for this facility	Identify, Protect

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Management	Asset Management	On what basis does the organization review, for the purpose of updating its inventory	Identify, Protect
Management	Asset Management	Is there a master version of mission-essential software and when was it updated	Identify, Protect
	Asset Management	Approximately, what percentage of the facility is not or cannot be updated with respect to critical vulnerabilities? (e.g., legacy system or business reason-i.e. break software application)	Respond, Recover
Management	Asset Management	If the organization has CCS systems that are not or cannot be updated with respect to critical vulnerabilities, approximately what percentage of these systems has compensating security control in pace that are not part of the original design?	Recover, Respond
Site and Service Control Security	Physical Protection	Can the resources be relocated physically (i.e backup facility)	Respond
Site and Service Control Security	Physical Protection	Can critical assets be physically relocated to limit future or further damage	Respond
Site and Service Control Security	Physical Protection	Can non-critical assets be related to reduce the exposure of critical assets to compromised non-critical assets	Identify
Site and Service Control Security	Access Control	Are multiple security control applied to critical assets	Protect
Site and Service Control Security	Access Control	Does the organization have a protocol for removing, suspending, or modifying user accounts upon change of employment	Identify
Site and Service Control Security	Access Control	Does the organization have a protocol for monitoring user activity after changes in employment related to termination	Identify
Site and Service Control Security	Access Control	Are administrative and operational activities enforced by dual authorization	Protect
Site and Service Control Security	Access Control	Is there a process implemented to ensure critical data is not left behind following the termination or deletion of this data	Protect
Site and Service Control Security	Access Control	Is access control maintained throughout a recovery process should the organization need to restore functionality following an event	Protect, Recover
Site and Service Control Security	Access Control	Does auding and monitoring continue throughout the recovery process	Recover
Site and Service Control Security	Access Control	Are stricter access control placed during the restoration process	Recover
Site and Service Control Security	Access Control	Are users granted privileged access based upon roles and responsibilities	Protect

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Site and Service Control Security	Access Control	Are privileged users reviewed on a consistent basis	Identify, Protect
Site and Service Control Security	Access Control	Do administrators administer both network and security components	Detect
Site and Service Control Security	Access Control	Does the organization have OT based Intrusion Detection System (IDS)	Protect
Site and Service Control Security	Access Control	Are cyber resources monitored by more than one sensor	Identify
Site and Service Control Security	Access Control	Are degrees of trust determined for users and cyber entities	Protect
Site and Service Control Security	Access Control	Can organization reassign administrative and management responsibilities based on risk to mission	Protect
Site and Service Control Security	Access Control	Has the organization established a business requirement for every access path to/from the facility	Protect
Site and Service Control Security	Access Control	Access to systems is based on criticality and sensitivity of information	Identify, Protect
Site and Service Control Security	Access Control	Has the organization established a business requirement for every access path to/from the maintenance system	Identify, Protect
Site and Service Control Security	Information Protection	Is the data validated to determine trustworthiness of restored resources	Detect
Site and Service Control Security	Information Protection	Is sensitive stored data encrypted	Protect
Site and Service Control Security	Information Protection	Are DNS servers under the organization's control hardened	Protect
Site and Service Control Security	Information Protection	Are there procedures in place to capture and then restore information resources to a known good state	Recover
Site and Service Control Security	Information Protection	Are there mission-critical hardware components for which protected alternates are maintained	Protect
Site and Service Control Security	Information Protection	Are there architectural alternatives for each type of key system element	Protect
Site and Service Control Security	Information Protection	Does the organization validate data integrity or restored resources	Detect, Recover
Site and Service Control Security	Information Protection	Does the organization implement deceptive environment to observe adversarial activities	Detect, Protect

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Site and Service Control Security	Information Protection	Is operationally sensitive information (i.e network diagrams, inventories) identified and categorized	Protect
Site and Service Control Security	Information Protection	How is operationally sensitive information managed	Protect
Site and Service Control Security	Information Protection	Is there a security review before operationally sensitive information is released outside the organization (partner sharing, public release, etc.)	Protect
Critical Operations	Plant Auxiliary System	Are there any emergency diesel generators available to site that support backup power to generating unit and also provide emergency power to the spillway gate	Identify
Critical Operations	Plant Auxiliary System	Does the facility include a secondary relay for emergency diesel generator that validates the action of the primary control relay in case of an unauthorized brake closure	Recover
Critical Operations	Plant Auxiliary System	Does the hydro facility install UPS in their electrical network to reduce the risk of power supply distortion? Note UPS is required for critical panel where short harmonic disruption effect the panel equipment	Recover
Critical Operations	Plant Auxiliary System	Does the DC system have redundant battery banks, each with its own battery charger to ensure the continuous operation	Recover
Critical Operations	Plant Auxiliary System	Has the organization established a process for authentication and authorization (i.e. identity proofing, registration, role-management) to limit access to the plant auxiliary system to only authorized persons	Protect
Critical Operations	Plant Auxiliary System	What is the basis for establishing authentication and authorization	Protect
Critical Operations	Plant Auxiliary System	Which of the following measures does the organization employ to control authorization	Protect, Detect
Critical Operations	Plant Auxiliary System	Which of the following measures does the organization employ to control administrator privileges (to include contractors performing administrative functions)?	Detect
Critical Operations	Plant Auxiliary System	Does the organization practice the concept of least privileges (i.e. users are only granted access to the information, files, and applications required to fulfill their roles and responsibilities) within the plant auxiliary systems for all accounts	Detect
Critical Operations	Plant Auxiliary System	Is username/password the primary means of any user authentication to the plant auxiliary system	Protect
Critical Operations	Plant Auxiliary System	Which of the following password management policies are implemented for the plant auxiliary system	Protect
Critical Operations	Plant Auxiliary System	What additional properties of authentication are employed for the plant auxiliary system	Detect
Critical Operations	Plant Auxiliary System	If the primary means of authentication failed, has the organization determined that compensating controls would provide sufficient authentication	Protect
Critical Operations	Plant Auxiliary System	Has the organization established a business requirement for every access path to/from the plant auxiliary system	Protect

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Critical Operations	Plant Auxiliary System	Does the organization implement security controls to limit access across the documented boundaries (e.g. firewalls, IDS port security, or rules of behavior)	Respond
Critical Operations	Plant Auxiliary System	Does the plant auxiliary system benefit from access control device(s) that restrict incoming and/or outgoing connections between the plant auxiliary system and the internet? (check all that apply)	Detect
Critical Operations	Plant Auxiliary System	Can a non-critical system act as a conduct (connection) between the Internet and plant auxiliary system	Identify
Critical Operations	Plant Auxiliary System	Does the plant auxiliary system benefit from access control device(s) that restrict incoming and/or outgoing connections between the plant auxiliary system and a non-critical system that is connected to the internet? (check all that apply)	Protect
Critical Operations	Plant Auxiliary System	Which of the following measures does the organization employ to control remote access to the organizations cyber services	Detect
Critical Operations	Plant Auxiliary System	Does the organization allow remote access to plant auxiliary system assets	Detect, Protect
Critical Operations	Plant Auxiliary System	Which of the following security measures does the organization employ for preventing exploitation of access paths	
Critical Operations	Maintenance	Is the remote maintenance of hydropower assets approved, logged, and performed in a manner that prevents unauthorized access	Protect
Critical Operations	Maintenance	Is the maintenance and repair of hydropower assets performed, logged, with approved and controlled tools	Protect
Critical Operations	Maintenance	Is access limited for external maintenance personnel	Respond
Critical Operations	Maintenance	Has the organization established a process for authentication and authorization (i.e. identity proofing, registration, role-management) to limit access to the maintenance system to only authorized persons	Protect, Respond
Critical Operations	Maintenance	What is the basis for establishing authentication and authorization	Respond
Critical Operations	Maintenance	Which of the following measures does the organization employ to control authorization	Protect
Critical Operations	Maintenance	Which of the following measures does the organization employ to control administrator privileges (to include contractors performing administrative functions)?	Protect
Critical Operations	Maintenance	Does the organization practice the concept of least privileges (i.e. users are only granted access to the information, files, and application required to fulfill their roles and responsibleness) within the maintenance system for all accounts	Protect
Critical Operations	Safety	Does the hydro facility install fire detection, suppression, and alarm systems for plant safety	Respond
Critical Operations	Generic Control Catalog	Is there a process to disable unwanted PPS (ports, protocols, and services	Protect

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Critical Operations	Generic Control Catalog	Is the operational technology (OT) specific data such as schematics, diagrams, control system layouts, etc. stored either on workstations or databases encrypted or password protected	Protect
Critical Operations	Generic Control Catalog	Are the default credentials of control system devices procured changed to having site-defined length and character requirements to add complexity	Protect
Critical Operations	Generic Control Catalog	Are patch management activities clearly defined for the Operational Technology (OT) devices	Protect, Recover
Critical Operations	Generic Control Catalog	Are there any programming activities within the operational technology (OT) environment including PLC programming	Identify, Detect
Critical Operations	Generic Control Catalog	Is there a list of authorized personnel for control system operations	Protect
Critical Operations	Generic Control Catalog	Is the communication channel for the alarm system along the alarm reporting system segmented and/or independent to prevent alarm suppression/disabling attacks	Identify
Critical Operations	Generic Control Catalog	Are critical serial communication (COM) given restricted access to authorized personnel to avoid command/control or reporting messages being blocked	Identify, Protect
Critical Operations	Generic Control Catalog	Are force and remote restart or shutdown control system devices disabled or highly restricted	Protect, Recover
Critical Operations	Generic Control Catalog	Are there wireless gateways, modems, and other access points installed for hydropower operations control and/or monitoring	Identify, Detect
Critical Operations	Generic Control Catalog	Is communication authentication considered within the operations technology (OT) environment	Protect
Critical Operations	Generic Control Catalog	Do managed systems undergo vulnerability scanning in accordance with the organization policy	Detect
Critical Operations	Generic Control Catalog	Once vulnerabilities are identified, the organization has a mitigation plan in place to monitor identified vulnerabilities	Respond
Critical Operations	Generic Control Catalog	Systems are patched on a regular basis	Protect
Critical Operations	Generic Control Catalog	Does the organization have managed systems for which automated patch management process is used	Protect
Critical Operations	Generic Control Catalog	The organization has a process for releasing patch installation upon the release of the patch	Protect
Critical Operations	Generic Control Catalog	Is there a defined security configuration required for network systems	Protect
Critical Operations	Generic Control Catalog	Are audits conducted to record analysis for inappropriate activity	Detect
		Hardware components have tamper-evident technologies applied to identify damaged components	Respond
Critical Operations	Plant Operational System	Does the computer-based hydro automation system have the capability to remotely control the operation of valves, blowers, compressors, etc.?	Identify
Critical Operations	Plant Operational System	Does the hydro turbine automation system have anomaly detection capability	Identify

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Critical Operations	Plant Operational System	Does the facility limit access to hydro generating unit to authorized users, processes, and associated devices only	Protect
Critical Operations	Plant Operational System	Does the hydro generator circuit breaker maintain a separate communication channel to communicate with control center	Protect
Critical Operations	Plant Operational System	Does the hydro automation system have a secondary relay for main protection and control	Recover
Critical Operations	Plant Operational System	Does the hydro automation system have the capability to perform synchronism logic functionality or transfer the model of operation remotely	Recover
Critical Operations	Plant Operational System	Is the remote access functionality enabled for water conveyance system	Protect
Critical Operations Critical Operations	Plant Operational System	Does the water conveyance system maintain a separate communication channel than the plant communication network	Detect
Critical Operations	Plant Operational System	Does the facility install unidirectional gateway technology to secure hydro automation network	Protect
Critical Operations	Plant Operational System	Does the hydro facility have their own secure data historian	Identify
Dependencies	Dependencies	Are diverse supply chains used for mission-critical technical components	Respond
Dependencies	Dependencies	Is there a process to verify supply chain integrity	Protect
Dependencies	Dependencies	Has the size of the supply chain attack surface been analyzed	Identify, Detect
Dependencies	Grid Operations	Are there processes implemented should the plant need to switch to manual operations	Respond
Dependencies	Grid Operations	Can the plant operate should the generator be isolated from the grid	Respond
Dependencies	Grid Operations	Generator protection relays help maintain system performance	Protect
Dependencies	Grid Operations	Specific loads are identified in a system restoration plan.	Respond
Dependencies	Grid Operations	There is a documented Black Start Capability Plan	Recover
Dependencies	Grid Operations	Are there alternative resources available in response to an adversarial event	Recover
Dependencies	Grid Operations	Is there an accommodating plan should there be a latency in resources due to the switching of resources	Recover
Dependencies	Grid Operations	Is there an alternate version of services that can be instantiated	Recover
Dependencies	Grid Operations	Can services and resources be virtually relocated	Recover
Dependencies	Grid Operations	Is data frequently backed-up	Protect
Dependencies	Grid Operations	Faulty or suspect service interactions are terminated when identified	Detect
Dependencies	Grid Operations	Does the organization identify and maintain mission dependencies on cyber resources	Identify
Dependencies	Grid Operations	Does the organization identify and maintain functional dependencies among cyber resources	Identify
Dependencies	Grid Operations	Does the organization document dependencies on external resources	Identify

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Dependencies	Grid Operations	Has the organization identified and eliminated single points of failure	Identify
Dependencies	Grid Operations	Has the organization identified and resourced alternative mission courses of action	Identify
Dependencies	Grid Operations	Are non-mission critical resources segmented from mission-critical resources	Identify
Dependencies	Business Functions (Non-OT)	Critical information is identified	Identify
Dependencies	Business Functions (Non-OT)	Least-privileged access is assigned to employees based upon their role	Identify
Dependencies	Business Functions (Non-OT)	Device accessing the internal network must be authenticated	Identify
Dependencies	Business Functions (Non-OT)	An incident response plan outlining procedures following an adverse event has been developed	Protect
Dependencies	Business Functions (Non-OT)	A recovery plan has been developed to limit potential damages to internal information	Protect
Dependencies	Business Functions (Non-OT)	Are business systems segmented from operational systems within the plant	Protect
Dependencies	Business Functions (Non-OT)	Is there a process to identify unavailable resources and business functions that have been destroyed	Identify
Dependencies	Business Functions (Non-OT)	The organization identifies trustworthy resources for business functions	Identify
Dependencies	Endpoint and Data Security	Do third-party vendors have monitored access to systems and upgrades	Protect
Dependencies	Endpoint and Data Security	Is cloud data protection implemented, for both data at rest and in motion	Protect
Dependencies	Endpoint and Data Security	Cloud data is managed externally by a third party	Protect
Dependencies	Endpoint and Data Security	Are security controls in place to protect endpoint devices, such as Programmable Logic Controllers (PLC)	Protect
Dependencies	Endpoint and Data Security	Data storing policies are in place	Protect
Dependencies	Endpoint and Data Security	Encryption is implemented on relevant devices for data processing	Protect
Dependencies	Endpoint and Data Security	Encryption is implemented on relevant devices for data at rest	Protect
Dependencies	Endpoint and Data Security	Are change parameters scheduled to control unpredictability	Protect
Dependencies	Endpoint and Data Security	Are automated change mechanisms restricted to allowable ranges	Protect
Dependencies	Endpoint and Data Security	Are cyber resources separated based on criticality	Protect
Dependencies	Endpoint and Data Security	IS there a maintained master version of mission-critical software	Identify
Dependencies	Endpoint and Data Security	Does the organization conduct damage assessments	Protect
Dependencies	Endpoint and Data Security	Does the organization validate the integrity of data	Identify
Dependencies	Endpoint and Data Security	What is the maximum time required to validate the integrity of services	Identify
Dependencies	Endpoint and Data Security	What is the frequency of service integrity checks	

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Dependencies	Endpoint and Data Security	Does the organization maintain acceptable levels of performance for mission-critical services should there be a degree of degradation	Respond
Dependencies	Endpoint and Data Security	Can cyber resources be reconfigured on demand	Respond
Dependencies	Endpoint and Data Security	Can cyber resources be reallocated on demand	Respond
Dependencies	Endpoint and Data Security	Can resources be relocated to minimize service degradation	Respond
Dependencies	Endpoint and Data Security	Can mission-critical functions failover	Recover
Dependencies	Endpoint and Data Security	Can mission-critical hardware components be replaced with protected alternates	Recover
Dependencies	Endpoint and Data Security	Can mission-critical functions switch to alternative processing paths	Respond
Dependencies	Endpoint and Data Security	Can mission-critical connections switch to alternative paths	Respond
Dependencies	Endpoint and Data Security	Does the organization validate the attribution of systems control data	Identify
Dependencies	Endpoint and Data Security	Can data assets be validated to ensure the integrity has not been corrupted	Identify
Dependencies	Endpoint and Data Security	Are software service integrity checks performed on operational systems	Identify
Dependencies	Endpoint and Data Security	Are hardware system integrity checks performed on operational systems	Identify
Dependencies	Endpoint and Data Security	Does the organization conduct data validation checks to identify potentially corrupt or falsified information	Identify
Dependencies	Endpoint and Data Security	Does the organization identify potentially compromised processes or services	Identify
Dependencies	Endpoint and Data Security	Does the organization identify potentially faulty or corrupted components in the operational environment	Detect
Dependencies	Endpoint and Data Security	Are resources in an active state for a limited lifespan	Identify
Dependencies	Endpoint and Data Security	Can compromised critical information be reconstructed from existing resources	Respond
Dependencies	Endpoint and Data Security	Does the organization track the security posture of cyber resources	Identify
Dependencies	Endpoint and Data Security	Are damage assessments conducted to understand the status of resources	Identify
Dependencies	Endpoint and Data Security	Does the organization conduct external searches for evidence of exfiltrated data	Identify, Protect
Dependencies	Endpoint and Data Security	Does the organization track effectiveness of defenses based on the number of cyber incidents	Identify
Dependencies	Endpoint and Data Security	Has the organization identified and replaced any data feed and connections for which risks outweigh benefits	Identify
Dependencies	Endpoint and Data Security	Are end point systems (desktops, laptops, tablets, etc.) required for the operation of the CCS	Protect
Dependencies	Endpoint and Data Security	Once the endpoint systems (e.g desktops, laptops, tablets, etc.) are no longer available (without considering any redundant or alternative mode), what percentage of normal cyber functions are lost or degraded	Respond

Domain	Sub-domain	Valuation Objective	NIST CSF Category
Dependencies	Endpoint and Data Security	Is there a contingency/business continuity plan with the provider for restoration	Respond
Dependencies	Endpoint and Data Security	Does the organization participate in the provider's priority plan for restoration	Respond, Recover