Cybersecurity Value-at-Risk Framework

Preprint

Anuj Dilip Sanghvi and Ryan Cryar

National Renewable Energy Laboratory

Presented at the 2023 IEEE Power and Energy Society General Meeting
Orlando, Florida
July 16–20, 2023

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

Conference Paper
NREL/CP-5R00-84412
September 2023

Cybersecurity Value-at-Risk Framework

Preprint

Anuj Dilip Sanghvi and Ryan Cryar

National Renewable Energy Laboratory

Suggested Citation

Sanghvi, Anuj Dilip, and Ryan Cryar. 2023. *Cybersecurity Value-at-Risk Framework: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-84412. https://www.nrel.gov/docs/fy23osti/84412.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

Conference Paper
NREL/CP-5R00-84412
September 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. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

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

NREL prints on paper that contains recycled content.

Cybersecurity Value-at-Risk Framework

Anuj Dilip Sanghvi
Energy Security and Resilience
National Renewable Energy Laboratory
Golden, Colorado USA
anuj.sanghvi@nrel.gov

Ryan Cryar
Energy Security and Resilience
National Renewable Energy Laboratory
Golden, Colorado USA
ryan.cryar@nrel.gov

***Abstract*—As more variable renewable energy sources are added to the grid, the role of hydropower as a reliable baseline and firming resource is growing more critical. However, the U.S hydropower fleet is not fully prepared to face modern issues such as cybersecurity threats. Hydropower accounts for 37% of U.S. utility-scale renewable electricity but is challenged by diverse infrastructure and legacy devices that predate modern security practices. While new cybersecurity solutions cannot simply be added to current hydropower generation and operation technologies, custom cybersecurity assessments can reveal system-specific threats and risk probabilities and identify mitigating enhancements.**

***Keywords*—distributed energy, cybersecurity valuation methodology, risk management, value-at-risk, web-based application**

I. Introduction

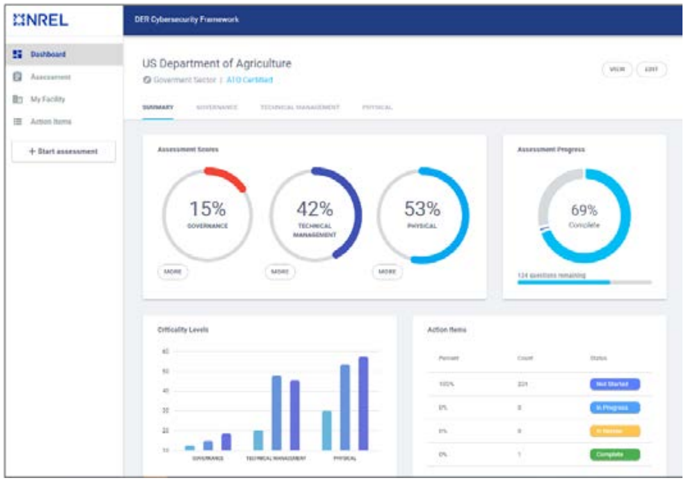
The Cybersecurity Value-at-Risk Framework (CVF), a tool developed by the National Renewable Energy Laboratory (NREL) and Argonne National Laboratory with support from the U.S. Department of Energy's Water Power Technologies Office, aims to develop an industry-accessible platform with user-friendly navigation of risk-based assessments. This paper describes the CVF platform and its role in improving the cybersecurity posture of hydropower plants and dams. The platform provides facility owners and operators with valuable guidance and next steps to mitigate risk and gives indicative scores for stakeholders to make future cybersecurity investment decisions. As an online tool, CVF guides users through a detailed analysis of plant operations. Users answer a series of questions, and their responses are compared against multidimensional criteria for environmental, operational, and economic impacts. CVF considers factors such as system operational modes, configuration, and staff attendance for manual intervention to generate a score that represents the likelihood of a cyberattack. The CVF assessment also generates scores that indicate the financial value of specific risks for which cybersecurity improvements are required to withstand future threats.

II. Background

As hydropower plants become increasingly connected via relatively advanced and "smart" devices along with legacy systems, it is critical to address cybersecurity challenges that arise along with this interconnection [1]. One of the primary concerns in deploying security measures is the lack of a formalized methodology to assess and generate the value of hydropower cybersecurity posture. In the absence of this guidance, it is difficult for hydropower plant management to effectively make investment decisions in improving cybersecurity maturity and the overall resiliency of their plants to defend against cyberattacks.

A. Distributed Energy Resources Cybersecurity Framework

As part of an effort to provide assistance to under-resourced utilities, NREL's Energy Security and Resilience researchers conducted cyber-governance assessments using the U.S. Department of Energy's (DOE's)_Cybersecurity Capability Maturity Model. From the assessments, NREL highlighted gaps in organizations' cybersecurity postures, including the need to strengthen cybersecurity workforce development, manage external dependencies, and 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 Distributed Energy Resources Cybersecurity Framework (DER-CF) [2]. The framework is a web-based application that enables energy managers and operational technology security staff to assess their cybersecurity posture and generate a prioritized set of action items. DER-CF also produces executive summaries, reports, and graphs that show the need for management support in weaker areas. This self-assessment tool promotes fundamental cybersecurity hygiene based on user input.



Percent	Count	Status
100%	221	Not Started
0%	0	In Progress
0%	0	In Review
0%	1	Complete

Fig. 1. Example of NREL's Distributed Energy Resources Cybersecurity Framework interface [3].

B. Valuation Methodology

In response to addressing the DOE's goals of strengthening the security and resilience of aging hydropower fleet, NREL staff have conducted research in identifying hydropower operations and critical assets that potentially be targeted to disrupt operations. Hydropower plants have complex grid interactions and are expected to produce power reliably. Hydropower plant owner/operators and other decision makers are required to address impacts such as environmental, economic, safety, and operational and structure their funding allocation and budgets based on maintenance needs. It is critical to introduce factors that identify cybersecurity risks and potential attacks that influence the above impacts [4]. Table I represents the portion of the research mappings that identified a set of critical hydropower operations, assets, and the cyber-physical components that may be prone to manipulative attack scenarios. Addressing these mappings and authoring security controls and recommendations around them enables a stronger outcome and, in turn, an increase in the state of security and resilience for the hydropower fleet.

TABLE I. CRITICAL ASSET MAPPINGS

Hydropower Operations	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, CO2 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 sensor	Speed sensor, hydro turbine control system, turbine shaft vibration monitoring system
Automation, Control, and Protection	Supervisory system, networking equipment, HMI, emergency shutdown system	Speed contol and brake monitoring system, routers, switches, gateway devices (firewall, IDS/IPS), controller communication modules, fire and overspeed protection
Substation Operation	Circuit switches, surge arrestor, transformers, line switches	Remote terminal unit, programmable logic controller, protective device, HMI, gateway device
Plan Auxiliary System	Station lighting, DC system-UPS and battery, diesel and battery generator	Lighting plant control system, plant security system, plant DC monitoring system, diesel generator monistoring system

III. Cybersecurity Valuation

Addressing cybersecurity valuation involves several facility-specific factors such as risk profile, security control implementations, cybersecurity resilience, and probability of an attack occurring. Since all these factors are influenced by an organization’s processes, requirements for support functions, and specific implementations of business process and security controls, it becomes necessary to articulate these facility-specific differences to accurately assess and mitigate cybersecurity risks. CVF (“the framework”) addresses these challenges with a methodology and an agile platform that uses a modular approach for considering facility-specific factors. The methodology performs a semi-quantitative scoring analysis on user-driven data to produce a Value-at-Risk (VaR) score. The VaR score is numeric value that assists system owners and other stakeholders in making cybersecurity investment decisions on certain domains. The domains within the assessment are critical areas that form the foundation of an organization’s cybersecurity portfolio. The framework’s current inputs are as follows:

- Control implementation details: Each security control that was developed as part of the framework’s assessment stage includes authoring the practice, assigning an answer type, authoring the tailored recommendations/action items, and associating implementation weightages to the answers. These control implementation details construct the backend of the application to accurately score the organization’s cyber risk posture.

- Impact categories: The hydropower sector’s unique challenges include the impact categories that are most likely to be stakeholders’ priorities to reduce the potential for a high-consequence incident. The framework scopes these impact categories as a way to associate each security control to its potential impact if implemented poorly.

- Likelihood: The biggest input and the most challenging task are developing factors that assist in calculating the probability of a threat event occurring. Using the National Institute of Standards and Technology (NIST) Special Publication 800-30R1 definitions for likelihood and risk determination, some factors for hydropower operations and system-level probability calculations were developed.

The valuation is backed by a tailored set of prioritized recommendations that enable immediate changes or modifications by facility operators. This informs a risk-based approach and improves decision-making. The framework’s outcomes are:

- VaR score: The VaR score intends to signify a quantitative score directly proportional to the need for resource allocation (workforce/funding/tools) and is based on facility’s risk posture.

- Valuation guidance: The outcome of the framework’s assessment stage generates a list of prioritized action items and guidance that elaborates on the importance of mitigating the identified cybersecurity risks through valuing the risk impacts. The framework aims at articulating the loss in terms of equipment damage, operational downtime, and safety, and indicates the need for cybersecurity investments through the VaR score and the valuation guidance.

- Recommended action items: A typical result of undertaking an assessment is also to identify the immediate next steps to feed the continuous cycle of a feedback loop. The framework's outcomes provide recommended best practices specifically tailored for the hydropower valuation assessment type.

A. *Research*

The first phase of CVF consisted of a literature review of the existing standards hydropower facilities adhere to. Some of the researched standards include:

- IEEE 1020: Guide for Control of Small Hydroelectric Power Plants
- IEEE 1010: Guide for Control of Hydroelectric Power Plants
- IEC 31010: Risk Assessment Techniques
- IEC 62270: Guide for Computer-Based Control for Hydroelectric Power Plan Automation
- DOE: Dams Sector Cybersecurity Capability Maturity Model.

B. *Development/Application Overview*

The core application leverages the DER-CF to form the design and concepts of development [3]. The repository of code is "forked" to exist independently of the original repository codebase. This stand-alone repository contains the modified components of the application to fit the needs of the CVF.

One component that has been modified is the question editing. The DER-CF, when creating a question, allows a user to change the criticality level of the control via dropdown with options of low, medium, and high [3]. Within CVF, this functionality was changed from criticality to impact level. Impact level is how much impact a cyberattack might have if the question is not implemented. This impact definition yields the capability to assign weights to the question depending on how it gets answered, in addition to keeping the same process of the original application.

The administrator can author questions with different metrics to tag within the question editor, which allows the user of the application to see different information that is tailored to their own assessment experience. For example, using impact categories defined as the area of operation that a potential attack may impact, the administrator tags economic, environmental, operational, and/or safety according to the question. The user then selects their answer to that question, and if the question is not answered with a high enough maturity, the impact will be added to their final metrics. With the introduction of new question data, new charts to display the results of the assessment as the user progresses were also introduced. These new security controls and practices associate to various parameters that enable the scoring mechanism. These parameters are introduced within the administrator access of the application as metrics that are later represented as graphics to educate the user and provide assessment outcomes in visual form.

Figure 2 shows the distribution of the different categories of the NIST Cybersecurity Framework (CSF) that each question applies to. This graph is used to show how the overall assessment maps to the CSF and how they may be able to categorize their own posture. NIST CSF core includes functions and categories that include *Identify, Protect, Detect, Respond, and Recover*, representing a robust classification of the security controls as they relate to these CSF stages. These stages form the basis to adhere to a more standardize approach, which is usually mandated within the federally owned and operated plants but can prove beneficial for the entire fleet.

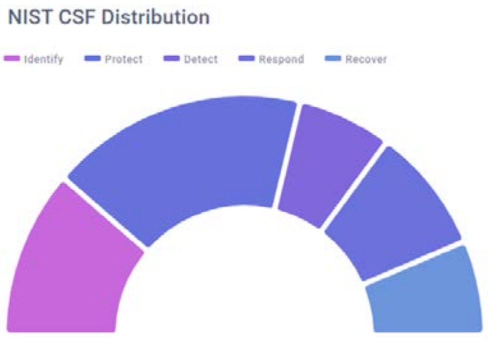


Fig. 2. National Institute of Standards and Technology (NIST) CSF distribution of all questions.

The consequence category distribution (Fig. 3) is an overall view of what consequences a user is most susceptible to based off the answers in their assessment. This graph represents the total number of questions that contain an identified consequence category, and only moves the lanes if a user answers a question with less than a medium posture. The graph will change depending on the user's answers to give them a visual representation of their scores. The categories of consequences are natural disaster/physical attack (ND/PA), integrity-based attack (IBA), denial of service (DOS), data breach, and ransomware.

As the user progresses, they can see action items that are organized by impact when they answer questions that may lower their overall cyber posture.

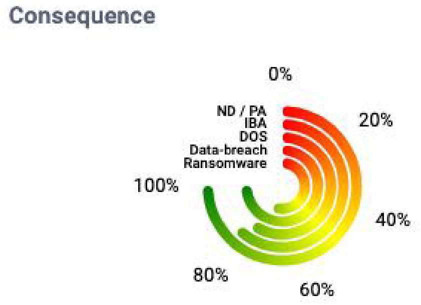
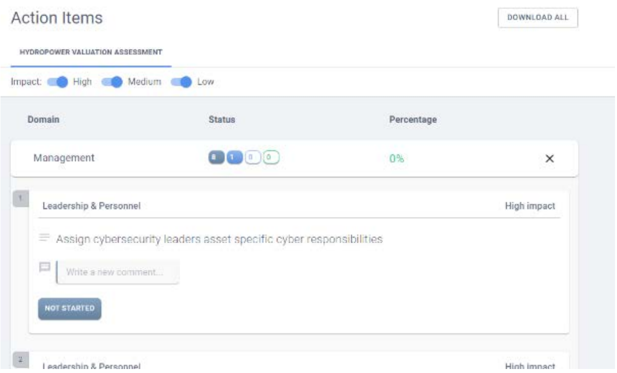


Fig. 3. Consequence categories by domain distribution.

Action items (Fig. 4) can be modified by assessing progress under the description of the action items. In addition, comments can be made to assign action items to users or to assess the status of the action item. Action items are automatically generated from each question that is answered without the ideal answers.



Action Items

Domain	Status	Percentage
Management	8 1 0 0	0%

1 Leadership & Personnel — High impact

Assign cybersecurity leaders asset specific cyber responsibilities

2 Leadership & Personnel — High impact

Fig. 4. Example of the Action Items interface.

For example, if a question has a yes or no answer, the action item is generated upon a user answering no. These action items are meant for a user to have an itemized list of actions they should take that was tailored to their assessment.

The application culminates in a report that can be downloaded by the user. The report dynamically inserts all the assessment info from the user into a Microsoft Word document to show the breakdown of their value-at-risk score with associated graphics. This report was designed to be templated, so a user can download it and modify it to further fit their needs.

IV. End-User Engagement

Throughout the development of the application, we engaged with several industry members, culminating with a visit to a hydroelectric plant to do a run-through of the assessment with one of our partners.

A. Partners and Performance

With support from the U.S. Department of Energy's Water Power Technologies Office, the research findings and development went through multiple reviews from industry partners, including the Bureau of Reclamation and privately owned utilities with a vast hydropower footprint. The CVF-*alpha* application went through a discovery assessment process at an operational hydropower plant. The constructive feedback received includes various clarifications within the security controls as they relate to facility personnel and development of parent practices for a hierarchical tree format of questions. With almost 200 control practices that target different roles within an organization, the framework may include delineation of roles and responsibilities for cybersecurity practices. The *alpha* version of the application was run locally and will be moved to NREL cloud for web-based accessibility and ease of use. The application is publicly accessible at www.cvf.nrel.gov. Given the success of DER-CF and the growing userbase, the performance metrics have been determined to continually maintain and enhance the user experience.

V. Conclusions and Future Work

The Cyber Value-At-Risk Framework is a novel approach to hydropower plant cybersecurity. The next steps are to take our current way of threat identification and improve upon it with the use of MITRE ATT&CK, and Common Vulnerabilities and Exposures (CVEs). We want to develop a pipeline for the automated tagging of threats to controls, and automated analysis of CVEs that may be relevant to our systems. This future work could be adapted to improve the future cybersecurity posture of hydroelectric plants. Other advancements of the CVF application will include an organizational view of cybersecurity risks, including multiple assessment results from different facilities within the organization. The bird's-eye view enables enhanced decision making for stakeholders. Resource allocations can be challenging, and iterations of the framework will be made to accurately produce the valuation score and guidance.

Acknowledgment

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 in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

References

[1] A. Alarcon, E. Malagon, and V. Snyder, "Digitization: a revolution for the hydroelectric sector," IDB, 9 October 2018. [Online] Available: https://blogs.iadb.org/energia/en/3286/.

[2] C. Powell, K. Hauck, A. Sanghvi, A. Hasandka, J. Van Natta, and T. Reynolds, "Guide to the distributed energy resources cybersecurity frameowrk," Golden, CO: National Renewable Energy Laboratory, 2019.

[3] National Renewable Energy Laboratory, "Distributed energy resource cybersecurity framework." [Online] Available: dercf.nrel.gov.

[4] Water Science School, "Hydroelectric Power Water Use," USGS, 8 June 2018. [Online]. Available: https://www.usgs.gov/special-topics/water-science-school/science/hydroelectric-power-water-use#:~:text=Hydropower%20does%20not%20pollute%20the,habitats%20in%20the%20dam%20area.