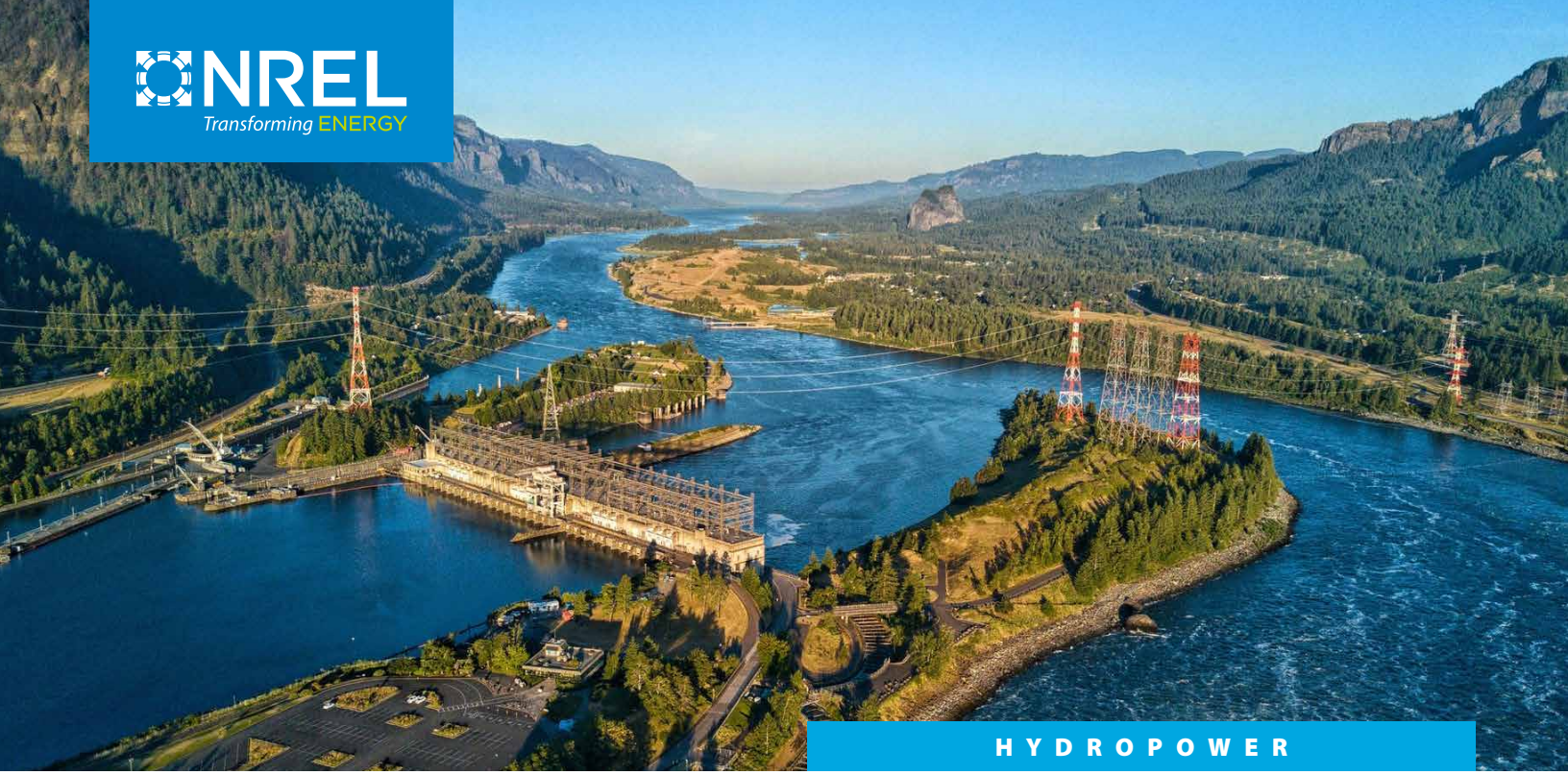

The Cybersecurity Value-at-Risk Framework will provide an industry-accessible, self-guided, automated tool that will allow hydropower plant managers to identify best practices and make sound cybersecurity investment decisions for their systems. Pictured here is the Bonneville Dam in Portland, Oregon. *Photo courtesy of Rafael Kaup*

Informing Cybersecurity Decisions With the Value-at-Risk Framework

A new tool informs cybersecurity investment decisions, maintaining the security and cost-competitiveness of the hydropower fleet and improving its potential to contribute to a secure, reliable, and resilient grid.

Hydropower accounts for 37% of utility-scale, renewable electricity generation in the United States. With the increasing deployment of distributed energy sources such as wind and solar, hydropower is a reliable baseline resource that plays a significant role in achieving a clean energy future.

Hydropower's Challenges: A Diverse Fleet, Aging Infrastructure, and Cyber Threats

Appropriately scaled security at every hydropower site is critical for any source on the grid, but the diversity and expanding capabilities of the U.S. hydropower fleet complicates across-the-board security investment decisions. The threat of cyberattacks naturally increases as the interconnection between information technology and operational technology networks broadens. Although this interconnection is essential for the dynamic nature of the grid, investments in system security must also be appropriately scaled.

Hydropower plants require custom analyses that are specific to the unique challenges and characteristics of any given facility. Facilities, however, often do not have the resources necessary for managers to make informed decisions on investments based on assessed capabilities and risks.

Data for Sound Investment Decisions

To address these challenges, the U.S. Department of Energy's National Renewable Energy Laboratory (NREL), with funding from the U.S. Department of Energy's Water Power Technologies Office and in partnership with Argonne National Laboratory (Argonne), is developing the Cybersecurity Value-at-Risk Framework (CVF).

The framework will provide an industry-accessible, self-guided, automated tool that will allow hydropower plant managers to identify best practices and make sound cybersecurity investment decisions for their systems.

Hydropower facility managers can better secure their plants by using the framework to:

- **Identify cybersecurity dependencies.** Investigate new and existing cybersecurity risks, as well as institutional constraints when addressing them.
- **Optimize and manage risks.** Improve operational risk management to better enable hydropower systems to provide resilient grid services.
- **Invest and improve capabilities.** Make data-driven decisions on cybersecurity investments in advanced technologies that improve hydropower's ability to provide secure grid services.

The CVF tool will guide users through an assessment and detailed analysis of a hydropower plant's operations. The tool will then provide results and data to inform effective cybersecurity investment decision-making and planning. The results will help managers understand the risk probability of cyberattacks on their facilities and how best to use resources to mitigate those risks.

Simplified Decisions, Enhanced Security

The CVF has the potential to ease the process of making cybersecurity investment decisions. By answering a series of questions, facility managers will have access to the information they need to determine what to focus on and what to do next to improve their cybersecurity posture.

This standardized method of assessing risks and approaches can broadly benefit the hydropower industry. In years to come, the CVF is expected to contribute to enhanced cybersecurity for dam infrastructure, reduce operation and maintenance costs, and increase the resilience of natural ecosystems.

Improving the cybersecurity maturity of the hydropower sector will enhance the United States' energy security and ensure hydropower continues to contribute to an ever-more resilient, flexible, and reliable grid.

Work With Us

NREL offers opportunities for hydropower industry, university, and government agency members to leverage our research expertise and state of-the-art capabilities in both cybersecurity and water power technologies. Join us in accelerating the movement to turn secure, renewable energy and energy efficient solutions into practical applications. Learn more at www.nrel.gov/workingwithus.

Expanding Distributed Energy Resource Assessment Capabilities

The CVF builds upon existing capabilities developed for the Distributed Energy Resource Cybersecurity Framework (DERCF, dercf.nrel.gov), which helps federal agencies assess the cybersecurity posture—or health—of distributed energy resource systems. The CVF leverages this existing online platform and other functionalities developed for DERCF and expands them for use, specifically, with hydropower.

The CVF tool follows National Institute of Standards and Technology (NIST) frameworks for data handling (NIST SP 800-53) and risk scores (NIST SP 800-30). National Electric Sector Cybersecurity Organizational Resource is also used for impact criteria scoring and threat scenarios to calculate and improve impact ratings for hydropower plants' environmental footprint, operations, and economics.

Together, these core components help facility managers make cybersecurity investment decisions more quickly and confidently.

Laboratory and Real-World Partnerships

Partnerships and advisory resources ensure that the findings and direction of the CVF apply to varied hydropower plant facilities.

National Renewable Energy Laboratory

NREL brings cybersecurity research expertise to distributed energy resources, including legacy industrial control systems like those at aging hydropower facilities. NREL researchers specialize in emulating system components that perform cybersecurity analysis and vulnerability assessments.

Argonne National Laboratory

Argonne uses resilience scoring experience to refine the resilience score calculated by the DERCF tool for use in the Cybersecurity Value-at-Risk Framework. Argonne also lends expertise in assessing the cybersecurity of hydropower plants.

Advisory Board and Implementation Resources

The U.S. Bureau of Reclamation, the U.S. Army Corps of Engineers, Holy Cross Energy, and Delta Montrose Electric Association serve as external advisory partners that verify the applicability of the framework in real-world settings. Delta Montrose Electric Association's hydropower facilities serve as an initial case study for the framework.

NREL Transforming ENERGY

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

NREL prints on paper that contains recycled content.

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

NREL/FS-5R00-80179 • August 2021