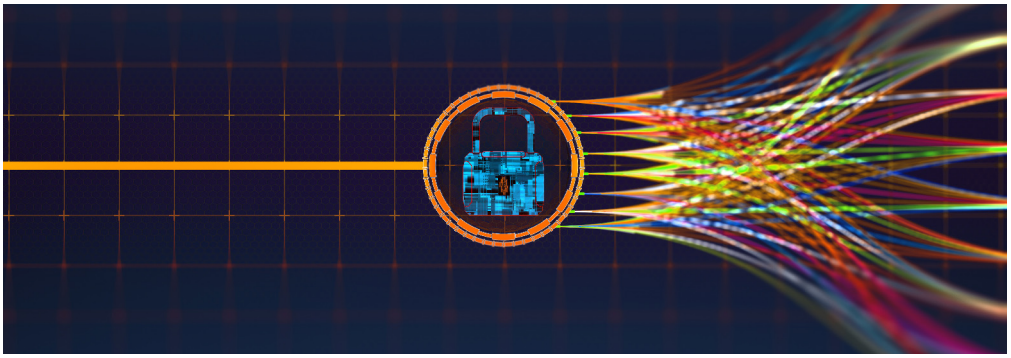
The Cybersecurity Value-at-Risk Framework

Manage cyber risk at energy facilities with an established and trustworthy tool

Ryan Cryar and Anuj Sanghvi



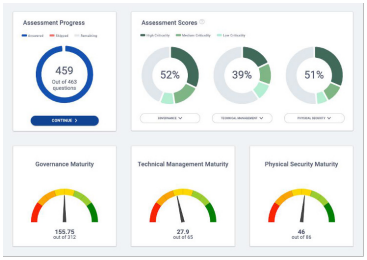
What is the Cybersecurity Value-at-Risk Framework?

The Cybersecurity Value-at-Risk Framework is a self-guided assessment tool to inform cybersecurity investment decisions. It provides site-specific evaluations of any facility, indicating where its energy assets, data networks, and physical access could be adjusted to improve security and resilience. The framework fills a gap that does not exist elsewhere by incorporating established standards and considering risks spanning environmental, economical, safety, and operations factors.

Step 1: *Register facility.* The user inputs detailed information about their facility and its energy assets and connections.

Step 2*: Define roles.* Facility managers and participants in the assessment define their roles and oversight of the facility.

Step 3*: Answer assessment questions.* The Cybersecurity Value-at-Risk Framework asks more than 200 questions in a self-directed and personalized survey format.



The Cybersecurity Value-at-Risk Framework dashboard shows status and scores according to diverse criteria. Users can save their progress and analyze specific aspects of their facility.

Step 4: *Receive assessment report.* The framework calculates risk, impact, and cyber-resilience scores to determine value at risk, and delivers tailored recommendations to improve cybersecurity.

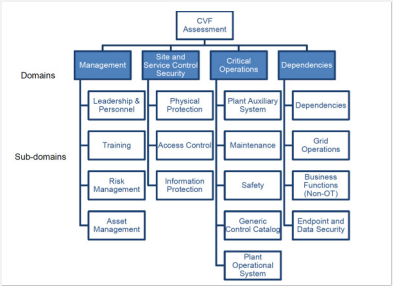
Step 5: *Repeat regularly.* User results are saved in their account, and progress in improving their cybersecurity posture can be tracked by performing regular assessments.

Assessment Approach

Assessments are structured around cybersecurity controls used at a facility. The controls map to categories developed by the National Institute of Standards and Technology's Cybersecurity Framework, such that each control is associated with relevant personnel and best practices. Domains and sub-domains of controls are shown to the right.

The Cybersecurity Value-at-Risk Framework calculates VaR scores of each control implemented by the user. The score is calculated by the following formula: VaR = L*(1-CI)*I. **L** is the likelihood of an attack or event resulting in an impact, **CI** are control implementations weighted according to unmitigated risks, and **I** is an impact score that is categorized as either low, medium, or high. The VaR score ranges from 0.001 to 1, with VaR > 0.5 representing high to extreme mitigation required.

In addition to the VaR scores, an assessment outputs recommended action items specifically tailored to the user's energy system, and valuation guidance, which articulates losses in terms of equipment damage, downtime, safety, etc.



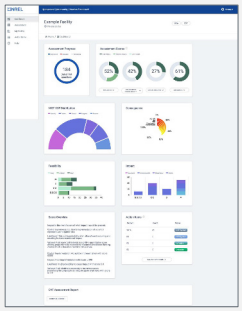
Research for the Framework

The Cybersecurity Value-at-Risk Framework was developed following a literature review of standards across a range of energy facility types. The standards influenced which controls are assessed, as did the type of energy facility. For example, a hydropower specific framework was recently completed using the most relevant standards for hydropower plant control and operations. The depth of research is evident in the following table mapping system functions to energy and cyber assets.

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

Application Dashboard

The framework features a user friendly dashboard for convenient and continued use. As the user works through the assessment the dashboard displays their progress and performance score. Their performance can be compared across different standards, and across categories within standards. This is useful for facilities, which are often obligated to follow specific standards. An example of the dashboard can be seen to the right.



Apply the Tool

The Cybersecurity Value-at-Risk Framework is publicly available at **cvf.nrel.gov**. The National Renewable Energy Laboratory offers opportunities for collaboration with utilities, facility operators, universities, government agencies, and more. If you are interested in collaborating, contact **Anuj.Sanghvi@nrel.gov.**

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.

IEEE Power and Energy Society General Meeting
Orlando, Florida
July 17, 2023
NREL/PO-5R00-86899