The Cybersecurity Value-at-Risk Framework: Informing Cybersecurity Decisions

Anuj Sanghvi, MD Touhiduzzaman, and Paul Wand

August 5, 2021

Contents

Cybersecurity Value-at-Risk Framework Project Overview

- Leverages the architecture of the Distributed Energy Resources Cybersecurity Framework (DER-CF) – www.dercf.nrel.gov
- Targets the risk management process to prioritize action items and associated investments
- Considers various impacting factors such as environmental, economical, safety and operations risks
- Calculates risk, impact, and cyber-resilience scores for determining value at risk
- Prioritizes risk-based recommendations to enhance decision-making

Research Approach

Literature review, scoping, and asset identification

Resources

- Institute of Electrical and Electronics Engineers (IEEE) 1020, *Guide for Control of Small Hydroelectric Power Plants*
- IEEE 1010, *Guide for Control of Hydroelectric Power Plants*
- International Electrotechnical Commission (IEC) 31010, *Risk Assessment Techniques*
- IEC 62270, *Guide for Computer-Based Control for Hydroelectric Power Plant Automation*
- *Dams Sector Cybersecurity Capability and Maturity Model*

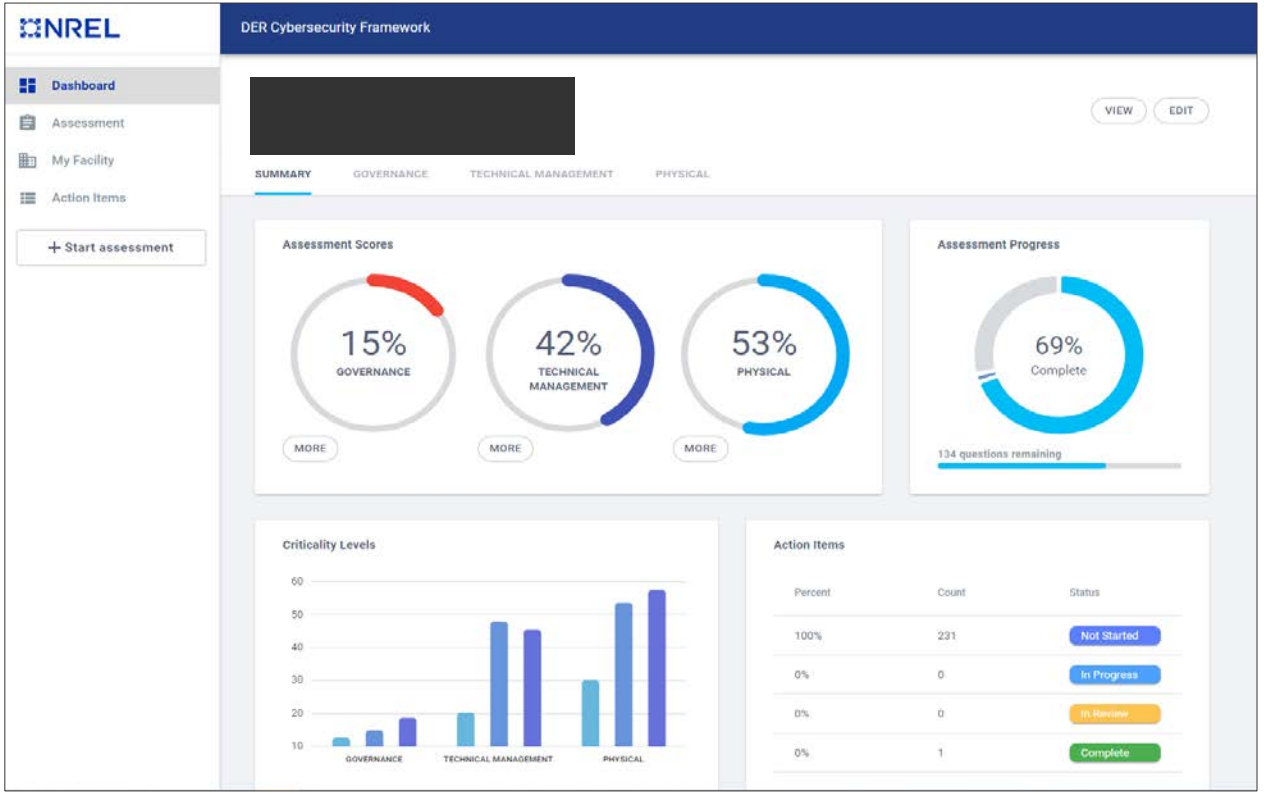
Advancing Cybersecurity Risk Assessment

Moving from maturity-based scoring to semiquantitative risk calculations

DER-CF

Pillar → Domain → Subdomain Model

Answer types/follow-ups and recommendations



Step 1: Hydropower Focused Operations and Assets

- Identify mission-critical hydropower systems
- Highlight areas of cyber concern for hydropower plant operations
- Scope assets that may be vulnerable to cyberattacks

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 control 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 monitoring system

Step 2: Impacts and Likelihood Categories

Impact

- Safety
- Environmental
- Economical
- Operational

Generic Control Catalog
*Are commonly used **ports disabled** when not used or changed to site-specific port numbers? Examples include 80 (HTTP), 53 (DNS), 23 (TELNET), 161 (SNMP), 502 (MODBUS), 20000 (DNP3), and 44818 (Ethernet/IP).*
*Is the **operation technology (OT) specific data encrypted or at least password protected**? Examples include schematics, diagrams, control system layouts, etcetera stored either on workstations or databases*
*Are control system devices' **default credentials changed to more secure credentials** before being deployed in production environment?*
*Is there a **robust patch management policy** and control in place where patches to OT/control system devices are first tested in a sandboxed/virtual system environment to identify undiscovered vulnerabilities?*
*Are **secure coding practices** used to prevent malicious code consisting of configuration to inject project files? For ex: Code signing, encryption of sensitive information, restriction of files and directory permissions.*
*Are operational servers and other critical functional components **regularly backed up**? Are those backups offline or offsite, and do you regularly **prove the ability to restore** operations?*

Likelihood Factor	Sub-category	Description
Location	Local	Asset is within boundary/sight of equipment
	Centralized	Asset is remote from controlled equipment, but within the plant
	Off-site	Asset is in a remote location from the plant
Operation Mode	Manual	Each operation needs a separate and deliberate initiation
	Automated	Two or more operations can be started by a single command or initiation
Staff Attendance	Attended	Operator must be physically available to initiate action
	Unattended	Operator can initiate control while off-site

Likelihood Descriptions

Factors affecting the calculation of cyberattack likeliness

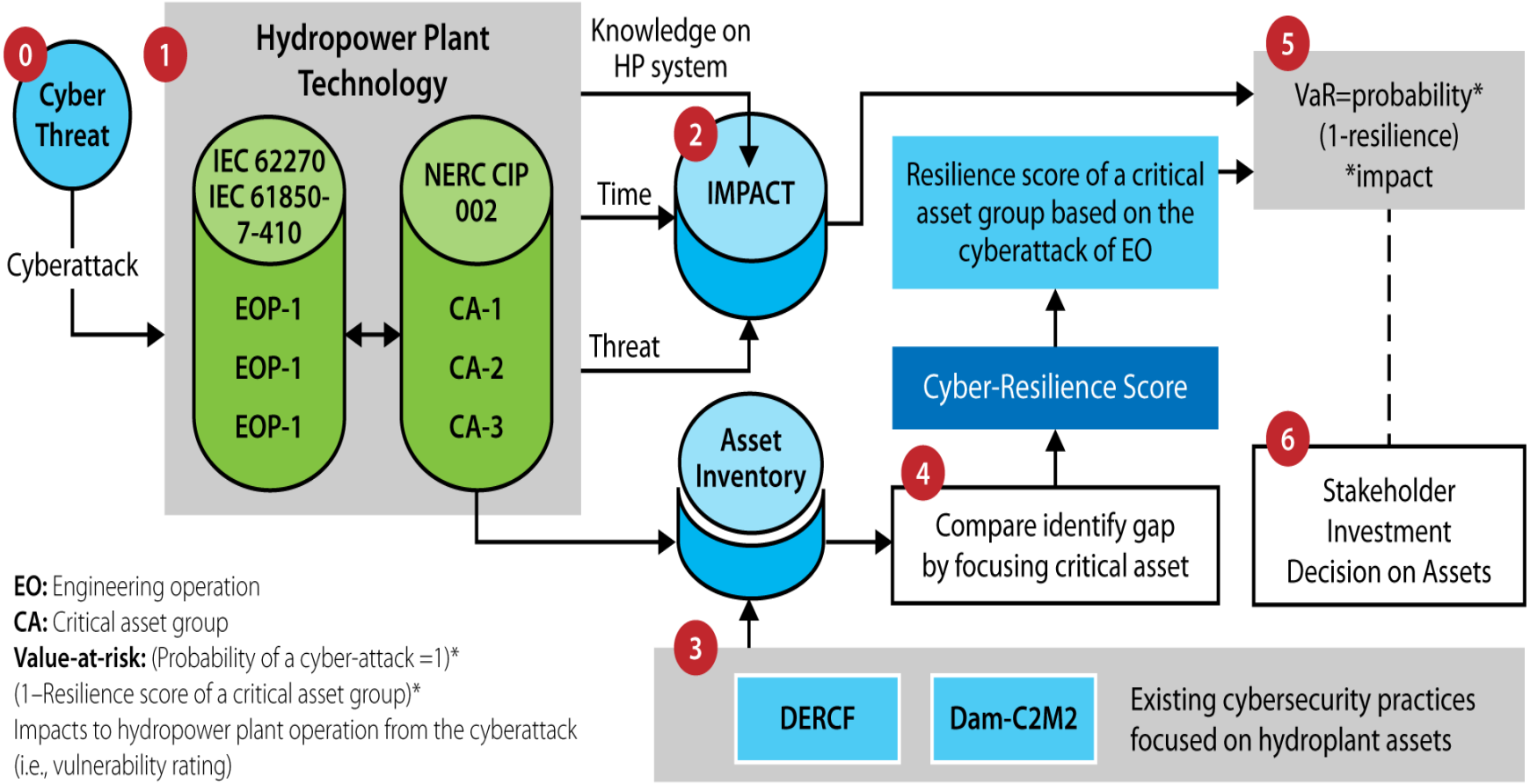
Step 3: Define, Assign, and Validate Weighted Values

Security Control Attributes and Metadata

- Establish values and associated weights
- Threat activation mechanism
- Likelihood score depending on operation modes
- MITRE's ATT&CK[1] for industrial control systems (ICS)

  Tactics, techniques, and procedures → assets → vulnerability → mitigation
- Impact considerations to address priorities
- Value-at-risk calculation to inform the need to invest resources

1. https://collaborate.mitre.org/attackics/index.php/Main_Page



EO: Engineering operation
CA: Critical asset group
Value-at-risk: (Probability of a cyber-attack =1)*
(1–Resilience score of a critical asset group)*
Impacts to hydropower plant operation from the cyberattack (i.e., vulnerability rating)

Assessment Structure

Domain expansion for hydropower assessment

Domain	Subdomain
Critical Operations	Maintenance Plant Operations Network Management Safety
Management	Risk Management Asset Management Identity Management Policies/Procedure Training Communication Networks Personnel/Leadership
Site and Service Control	Physical Protection Access Control Monitoring Information Protection
Dependencies	Grid Operation Business Endpoint Data

Technical Implementation

DER-CF Extension and Additional Functions in the Tool

Bridging Control Catalog to Risk Calculations

Risk Intelligence Server

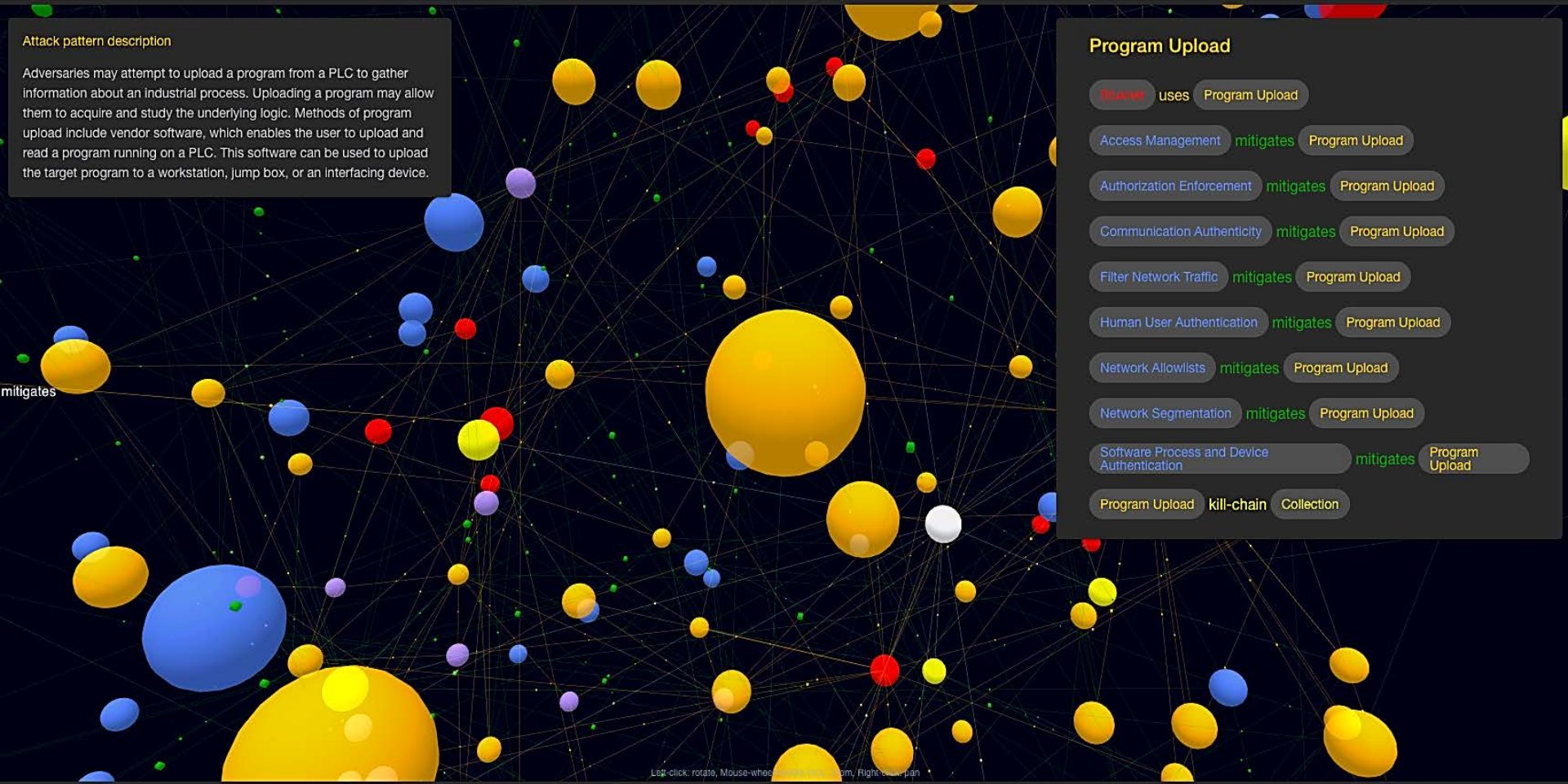
- ICS threat matrix—MITRE's ATT&CK ICS
- Additional filter for hydropower plant assets
- Development of dependent attributes
  - Controls
  - Threats and impacts
  - Scores
- Prioritization based on impact criticality

Graph Database

- What is it?
  - *Key difference in a graph is that relationships are considered a form of data rather than a foreign key*
- How do we use it?
  - *With the ability to create an edge between any two types of nodes, we can relate any attack pattern to security control or any asset type to disaster scenarios*
- How do we build from the MITRE ICS attack data?
  - *We start with well-known attack patterns and their mitigating courses of action, known malwares, and intrusion sets.*
- What is the path forward?
  - *We enrich the data with relationships of our custom control set and asset types for fine-tuned, cyber value-at-risk calculations*

Attack pattern description

Adversaries may attempt to upload a program from a PLC to gather information about an industrial process. Uploading a program may allow them to acquire and study the underlying logic. Methods of program upload include vendor software, which enables the user to upload and read a program running on a PLC. This software can be used to upload the target program to a workstation, jump box, or an interfacing device.



Program Upload

Stuxnet uses Program Upload

Access Management mitigates Program Upload

Authorization Enforcement mitigates Program Upload

Communication Authenticity mitigates Program Upload

Filter Network Traffic mitigates Program Upload

Human User Authentication mitigates Program Upload

Network Allowlists mitigates Program Upload

Network Segmentation mitigates Program Upload

Software Process and Device Authentication mitigates Program Upload

Program Upload kill-chain Collection

Outlook

- Generation of semi-quantitative scores indicative of ‘value-at-risk’
  - Assessment maturity using answer weightage
  - Impact severity and score
  - Likelihood of cyber-attack
- User interface to navigate valuation methodology
  - Threat selection using Risk Intelligence Server
  - Cyber-Resilience logic and scoring

Q&A

www.nrel.gov

Anuj.Sanghvi@nrel.gov
MD.Touhiduzzaman@nrel.gov
Paul.Wand@nrel.gov

NREL/PR-5R00-80645

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the Department of 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.