

# DER Cybersecurity R&D

Tami Reynolds and Anuj Sanghvi,  
National Renewable Energy  
Laboratory

Distribution  
Conference  
October 4-5, 2022

# Cybersecurity Assessments for Distributed Energy Resources



- The National Renewable Energy Laboratory (NREL) conducted more than 30 assessments for utilities across the United States with a cybersecurity assessment tool based on the U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and focused on business process.
- With funding from the DOE Office of Renewable Energy and Energy Efficiency Federal Energy Management Program, NREL modified the current cyber governance assessment tool to include an assessment process specifically for distributed energy resources (DERs).



The Distributed Energy Resources Cybersecurity Framework (DER-CF) was developed to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

# Assessing Three Key Areas for Cybersecurity




## **Pillars:**

- Cybersecurity governance
- Technical management
- Physical security.

## **The DER-CF uses the following standards and/or frameworks:**

- DOE C2M2
- NIST 800-53, 800-30, 800-82, CSF
- U.S. Department of Homeland Security cyber assessments of industrial control systems
- North American Electric Reliability Corporation Critical Infrastructure Protection
- International Electrotechnical Commission 62351
- Executive Order 13800.

# Domain— Sub-Domain Model

 <b>Cyber Governance Security Assessment</b>	 <b>Cyber-Physical Technical Management Security Assessment</b>	 <b>Physical Security Assessment</b>
<p>Domains</p> <ul style="list-style-type: none"> <li>• Risk Management</li> <li>• Asset, Change, and Configuration</li> <li>• Identity and Access Management</li> <li>• Threat and Vulnerability Management</li> <li>• Situational Awareness</li> <li>• Information Sharing and Communication Management</li> <li>• Incident Response</li> <li>• External Dependency Management</li> <li>• Cybersecurity Program Management</li> </ul>	<p>Domains</p> <ul style="list-style-type: none"> <li>• Account Management               <ul style="list-style-type: none"> <li>– Authentication, authorization, and accounting</li> <li>– Role-based access control</li> <li>– Remote access</li> <li>– Monitoring and logging</li> </ul> </li> <li>• Configuration Management               <ul style="list-style-type: none"> <li>– Change management</li> <li>– Access control</li> <li>– System settings</li> <li>– Cloud security</li> </ul> </li> <li>• Systems/Device Management               <ul style="list-style-type: none"> <li>– Software integrity</li> <li>– Cryptography</li> <li>– System protections</li> </ul> </li> </ul>	<p>Domains</p> <ul style="list-style-type: none"> <li>• Administration Controls               <ul style="list-style-type: none"> <li>– Audits</li> <li>– Awareness training</li> <li>– System security testing</li> <li>– Operational management</li> <li>– Security plan</li> <li>– Secure data</li> </ul> </li> <li>• Physical Access Controls               <ul style="list-style-type: none"> <li>– Perimeter security</li> <li>– Building security</li> <li>– Lighting</li> <li>– Signage</li> <li>– Intrusion alarm/motion detector</li> </ul> </li> <li>• Technical Controls               <ul style="list-style-type: none"> <li>– Intrusion Detection/prevention assets</li> <li>– Smart card/keying/badges</li> <li>– Sensor system/proximity reader/radio-frequency identification</li> <li>– Communication system</li> <li>– Closed-circuit television</li> </ul> </li> </ul>

# Unique Features

## DER-CF:

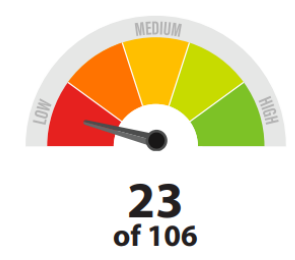
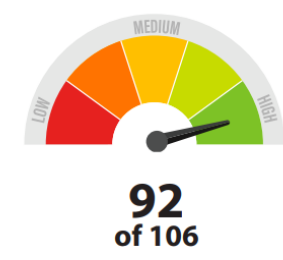
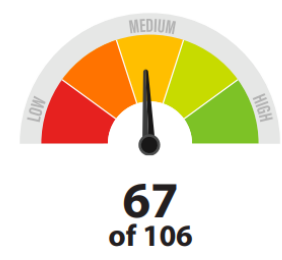
- Dynamic, content-driven approach
- Internal-facing application to aid researchers based on user behavior
- User experience-focused application, encourages reuse
- Data secured to meet Federal Information Processing Standards 199, medium level.

### Governance

### Technical Management

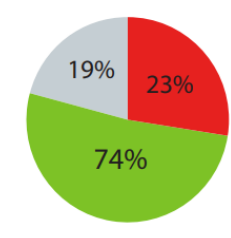
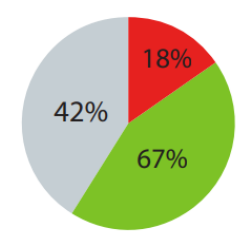
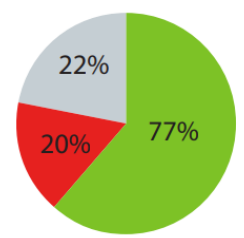
### Physical Security

Maturity Levels: Number of Implemented Controls



The pie charts below represent the number of implemented, unimplemented, and unanswered controls.

■ Unanswered ■ Unimplemented ■ Implemented



# Overview

- Publicly available, interactive version of the DER-CF
- User-focused assessment
- Detailed results and action items
- User base: Site operations, energy managers, executive managers
- Tailored assessment to individual sites.

The screenshot shows a registration page for the NREL Cybersecurity Assessment Tool for Distributed Energy. The page is split into two main sections: a dark blue left panel and a white right panel. The left panel features the NREL logo at the top, followed by the title 'Cybersecurity learning management system' and a sub-header 'Assess the cybersecurity maturity of your distributed energy resources. Let's get started!'. Below this are three icons representing 'Standards', 'Controls', and 'Encryption'. The right panel contains the registration form with the title 'Cybersecurity Assessment Tool for Distributed Energy' and the instruction 'Fill in your details to create your account.'. The form includes fields for 'First Name' (John), 'Last Name' (Doe), 'Email' (John.Doe@nrel.gov), 'Password', and 'Password Confirm'. A 'Sign in instead' link and a blue 'SUBMIT' button are located at the bottom of the form.

Hosted by NREL at [www.dercf.nrel.gov](http://www.dercf.nrel.gov)

# Future Work



Photo by NREL

NREL's ARIES cyber range provides an innovative way to research and analyze energy systems, and it can replicate a federal site through data visualization. Combined with the integration of data from the DER-CF, the cyber range can help merge the two complex cybersecurity topics of policy and technology by providing an integrated way to interact with cybersecurity logs and alerts.



## Cybersecurity Value-at-Risk Framework

- Leverages the architecture of the DER-CF ([www.dercf.nrel.gov](http://www.dercf.nrel.gov))
- Targets the risk management process to prioritize action items and associated investments
- Considers various impact factors, such as environmental, economic, safety, and operation risks
- Calculates risk, impact, and cyber-resilience scores to determine value at risk
- Prioritizes risk-based recommendations to enhance decision making.

# Step 1: Hydropower- Focused Operations and Assets

Hydropower Operations	Discipline and Assets	Critical Cyber Assets
<b>Water conveyance operation</b>	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
<b>Generator</b>	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
<b>Turbine</b>	Mechanical-turbine, electrical-turbine sensor	Speed sensor, hydro turbine control system, turbine shaft vibration monitoring system
<b>Automation, control, and protection</b>	Supervisory system, networking equipment, human-machine interface, emergency shutdown system	Speed control and brake monitoring system, routers, switches, gateway devices (firewall, intrusion detection system/intrusion prevention system), controller communication modules, fire and overspeed protection
<b>Substation operation</b>	Circuit switches, surge arrestor, transformers, line switches	Remote terminal unit, programmable logic controller, protective device, human-machine interface, gateway device
<b>Plan auxiliary system</b>	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

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

## Step 2: Impacts and Likelihood Categories

### 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).

Are the **operation technology-specific data encrypted or at least password protected**? Examples include schematics, diagrams, control system layouts, etc., stored on either workstations or databases.

Are control system devices' **default credentials changed to more secure credentials** before being deployed in a production environment?

Are there **robust patch management policies** and controls in place where patches to operation technology/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? Examples include code signing, encryption of sensitive information, and restriction of files and directory permissions.

Are operational servers and other critical functional components **regularly backed up**? Are those backups offline or off-site, and do you regularly **prove the ability to restore** operations?

### Impact categories:

- Safety
- Environmental
- Economic
- Operation.

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 depends on operation modes
- MITRE's ATT&CK<sup>1</sup> for industrial control systems  
*Tactics, techniques, and procedures* → *assets* → *vulnerability* → *mitigation*
- Impact considerations to address priorities
- Value-at-risk calculation to inform the need to invest resources.

# Risk Intelligence Graph

The screenshot displays the 'ICS ATTACK GRAPH' interface. At the top, there are navigation icons (hamburger menu, home, shield) and the title 'ICS ATTACK GRAPH'. The main area is a network graph with nodes of various sizes and colors (yellow, blue, red, purple) connected by thin lines. A tooltip box on the left provides an 'Attack pattern description' for 'Program Upload'. On the right, a 'Program Upload' panel lists various controls that 'mitigates' this attack pattern. At the bottom, there is a navigation bar with a settings icon, 'Program Upload', 'attack-pattern', and a 'HOME' link.

**ICS ATTACK GRAPH**

**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**

- Shovel 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

Program Upload attack-pattern

HOME →

- Advancements through hydropower operational threat simulation and impact analysis
- Hydropower cyber risk solution and evaluation using NREL's Advanced Research on Integrated Energy Systems (ARIES) cyber range
- Expansion of natural language processing to accurately identify threats at a larger scale
- Cost-benefit analysis for recommended mitigations with regard to potential cyber-attack consequences.

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 the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program 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.

NREL/PR-5R00-83766