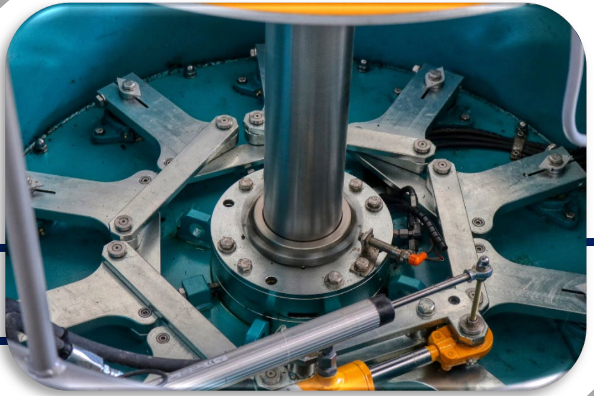
1.3.3.602 Cyber-physical Reference Framework

Kenneth D. Ham, Ph. D
kenneth.ham@pnnl.gov

28 July 2022



Pacific Northwest NATIONAL LABORATORY

Argonne NATIONAL LABORATORY

NREL NATIONAL RENEWABLE ENERGY LABORATORY

HDC

PNNL-SA-174701

Project Overview

Project Summary

Organized a sample of 275 plant configurations into nine types based on the prevalence of data and control signals among critical components. The cyber-physical configurations represented in each type inform what cybersecurity vulnerabilities may exist and potential mitigation approaches. A self-assessment tool allows plant operators to identify the type representing their plant to access relevant lessons learned and best practices information. Findings have been shared and discussed at industry conferences, summarized in a report, and shared with data contributors, MOU partners, and key industry leaders.

Intended Outcomes

- Create a mechanism to classify diverse hydropower plants by mechanical and cyber-physical systems.
- Organize the fleet into a manageable number of types
- Understand the variety and pervasiveness of cyber-physical configurations across the hydropower fleet.
- Guide and accelerate the evaluation and mitigation of cybersecurity risks

Project Information

Principal Investigator(s)

PNNL: Kenneth D. Ham, PhD;
Crystal Eppinger;
Darlene Thorsen, CISSP;
Paul Boyd;
Abhishek Somani, PhD

Project Partners/Subs

NREL: Michael Ingram, PE;
Charisa Powell
ANL: Vladimir Koritarov
USACE HDC: Mateo Mengis;
Jordan Fink, PE

Project Status

Completed

Project Duration

24 September 2019 -28 September 2021

Total Costed (FY19–FY21)

$485K

Project Objectives: Relevance and Approach

Relevance to Program Goals:

- Foundational information about the hydropower fleet and the variety and pervasiveness of cyber-physical configurations helps focus WPTO strategy.
- Types reduce the inertia of site- and age-related variation among hydropower plants as a hindrance to research, leading to more rapid progress and reduced cost.
- Organizing the fleet into types guides and accelerates efforts to develop effective cybersecurity tools to secure modern digitalized infrastructure, making the electrical system more reliable.

Approach:

- Develop a data request around a hydropower reference configuration created as an extension of the grid diagram in NISTIR-7628 (NIST 2014).
- Multi-pronged outreach to owner/operators to solicit plant configurations via secure channels.
- Classify configurations into logical groupings that form a typology to inform vulnerabilities and mitigation strategies of plants falling within each type.
- Create a self-assessment tool to allow owners/operators to match their plant(s) to a type.
- Communicate findings to key industry groups to enable the typology to inform research, demonstrations, and mitigations.

Project Objectives: Expected Outputs and Intended Outcomes

Outputs:

- Hydropower Reference Configuration
- Cyber-physical typology of nine types and associated statistics
- Self-assessment key for operators to determine their cyber-physical type
- Report detailing the collection of data, classification into types, evaluation of operational and functional roles in defining the types, and the self-assessment key.

Outcomes:

- Types have become an organizing principle for cybersecurity in hydropower
- WPTO Program planning is integrating the types
- Research is leveraging and building upon the foundational types to deliver targeted tools and mitigations
- Outreach efforts are informed by the types.

Project Timeline

FY19
- Funded Late FY19
- Hydropower configuration reference diagram

FY20
- Owner/operator plant configuration questionnaire
- Owner outreach: focused, broadcast, facilitated
- Data cleaned and loaded

FY21
- Typology Created and types evaluated
- Industry roll-out and focused outreach; Self-assessment tool
- Cyber-physical Framework Report

Project Budget

Total Project Budget – Award Information		
DOE	**Cost-share**	**Total**
$505K	$15K (in-kind contributions by HDC)	$520K

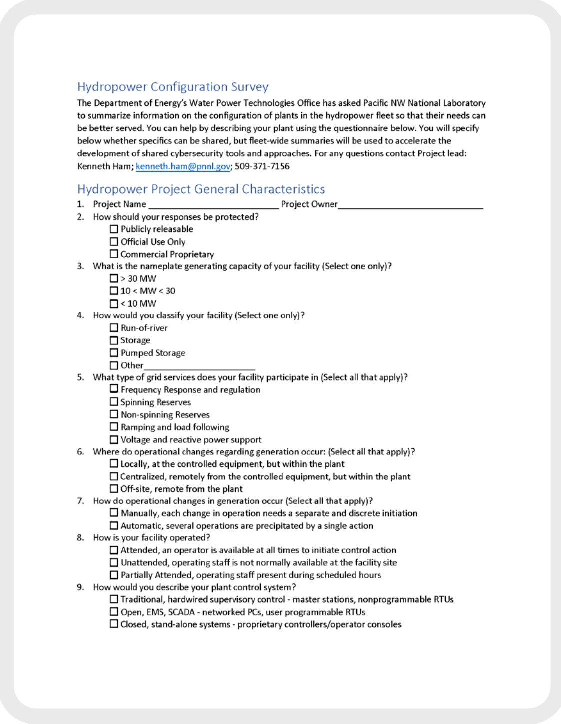
	FY19	FY20	FY21	Total Actual Costs FY19–FY21
PNNL	$0K	$118K	$130K	$248K
USACE-HDC (thru PNNL)	$0K	$0K +$5K in-kind	$25K +10K in kind	$25K +$15K in-kind
NREL	$0K	$95K	$63K	$158K
ANL	$0K	$47K	$23K	$70K
Total	$0K	$260K	$241K	$516K

End-User Engagement and Dissemination

- Getting Data:
  - Valuable guidance and assistance from the National Hydropower Association and other industry partners in crafting the messaging and facilitating a request to relevant industry forums
  - In-person outreach to industry professionals (owners and service providers) at NHA Southeastern Regional meeting (pre-covid lockdown)
  - Identify a targeted set of owners derived from the NHAAP database of hydropower plants to ensure we have coverage across a variety of sizes, functions, and owner types.
  - Personal, persistent outreach (through email and virtual meetings) communicating the value of the project and requesting plant information.
- Sharing Findings:
  - Rolled out at industry conferences (virtual due to covid restrictions)
  - Federal Hydropower MOU (DOE/EERE, Reclamation, USACE)
  - DOE-Norway Hydropower R&D MOU
  - Collaboration with new research projects

Performance: The Right Questionnaire

- Simple to respond
- Targets essential information and minimizes sensitivities
- Respectful of owner/operator’s time
- Secure data transmission to and from any agency
  - Encrypted, password-protected
- Compatible with anonymity and obfuscation
- Ease of data extraction for analysis

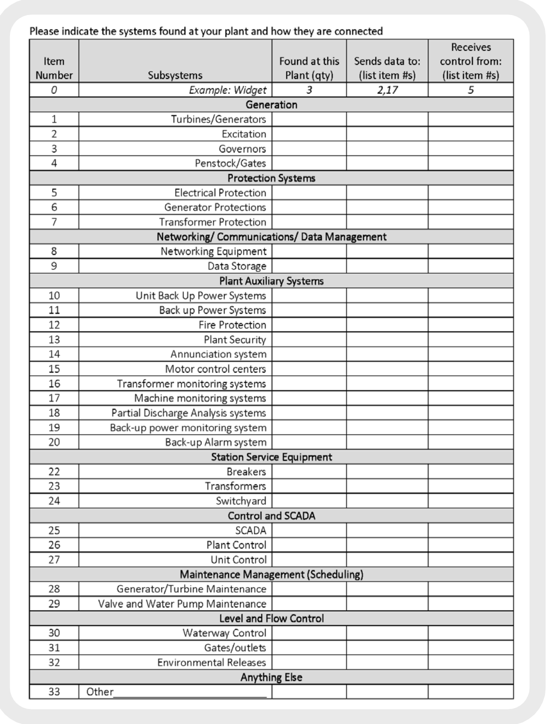


Hydropower Configuration Survey

The Department of Energy’s Water Power Technologies Office has asked Pacific NW National Laboratory to summarize information on the configuration of plants in the hydropower fleet so that their needs can be better served. You can help by describing your plant using the questionnaire below. You will specify below whether specifics can be shared, but fleet-wide summaries will be used to accelerate the development of shared cybersecurity tools and approaches. For any questions contact Project lead: Kenneth Ham; kenneth.ham@pnnl.gov; 509-371-7156

Hydropower Project General Characteristics

1. Project Name ______________________ Project Owner________________________
2. How should your responses be protected?
   - ☐ Publicly releasable
   - ☐ Official Use Only
   - ☐ Commercial Proprietary
3. What is the nameplate generating capacity of your facility (Select one only)?
   - ☐ > 30 MW
   - ☐ 10 < MW < 30
   - ☐ < 10 MW
4. How would you classify your facility (Select one only)?
   - ☐ Run-of-river
   - ☐ Storage
   - ☐ Pumped Storage
   - ☐ Other____________________
5. What type of grid services does your facility participate in (Select all that apply)?
   - ☐ Frequency Response and regulation
   - ☐ Spinning Reserves
   - ☐ Non-spinning Reserves
   - ☐ Ramping and load following
   - ☐ Voltage and reactive power support
6. Where do operational changes regarding generation occur: (Select all that apply)?
   - ☐ Locally, at the controlled equipment, but within the plant
   - ☐ Centralized, remotely from the controlled equipment, but within the plant
   - ☐ Off-site, remote from the plant
7. How do operational changes in generation occur (Select all that apply)?
   - ☐ Manually, each change in operation needs a separate and discrete initiation
   - ☐ Automatic, several operations are precipitated by a single action
8. How is your facility operated?
   - ☐ Attended, an operator is available at all times to initiate control action
   - ☐ Unattended, operating staff is not normally available at the facility site
   - ☐ Partially Attended, operating staff present during scheduled hours
9. How would you describe your plant control system?
   - ☐ Traditional, hardwired supervisory control - master stations, nonprogrammable RTUs
   - ☐ Open, EMS, SCADA - networked PCs, user programmable RTUs
   - ☐ Closed, stand-alone systems - proprietary controllers/operator consoles



Please indicate the systems found at your plant and how they are connected

Item Number	Subsystems	Found at this Plant (qty)	Sends data to: (list item #s)	Receives control from: (list item #s)
0	*Example: Widget*	*3*	*2,17*	*5*
	Generation			
1	Turbines/Generators			
2	Excitation			
3	Governors			
4	Penstock/Gates			
	Protection Systems			
5	Electrical Protection			
6	Generator Protections			
7	Transformer Protection			
	Networking/ Communications/ Data Management			
8	Networking Equipment			
9	Data Storage			
	Plant Auxiliary Systems			
10	Unit Back Up Power Systems			
11	Back up Power Systems			
12	Fire Protection			
13	Plant Security			
14	Annunciation system			
15	Motor control centers			
16	Transformer monitoring systems			
17	Machine monitoring systems			
18	Partial Discharge Analysis systems			
19	Back-up power monitoring system			
20	Back-up Alarm system			
	Station Service Equipment			
22	Breakers			
23	Transformers			
24	Switchyard			
	Control and SCADA			
25	SCADA			
26	Plant Control			
27	Unit Control			
	Maintenance Management (Scheduling)			
28	Generator/Turbine Maintenance			
29	Valve and Water Pump Maintenance			
	Level and Flow Control			
30	Waterway Control			
31	Gates/outlets			
32	Environmental Releases			
	Anything Else			
33	Other______________			

Performance: Representing the Hydropower fleet

Contributed by: Public utilities, energy companies, power agencies and administrations, and federal power operators

13% of plants in the U.S. hydropower fleet

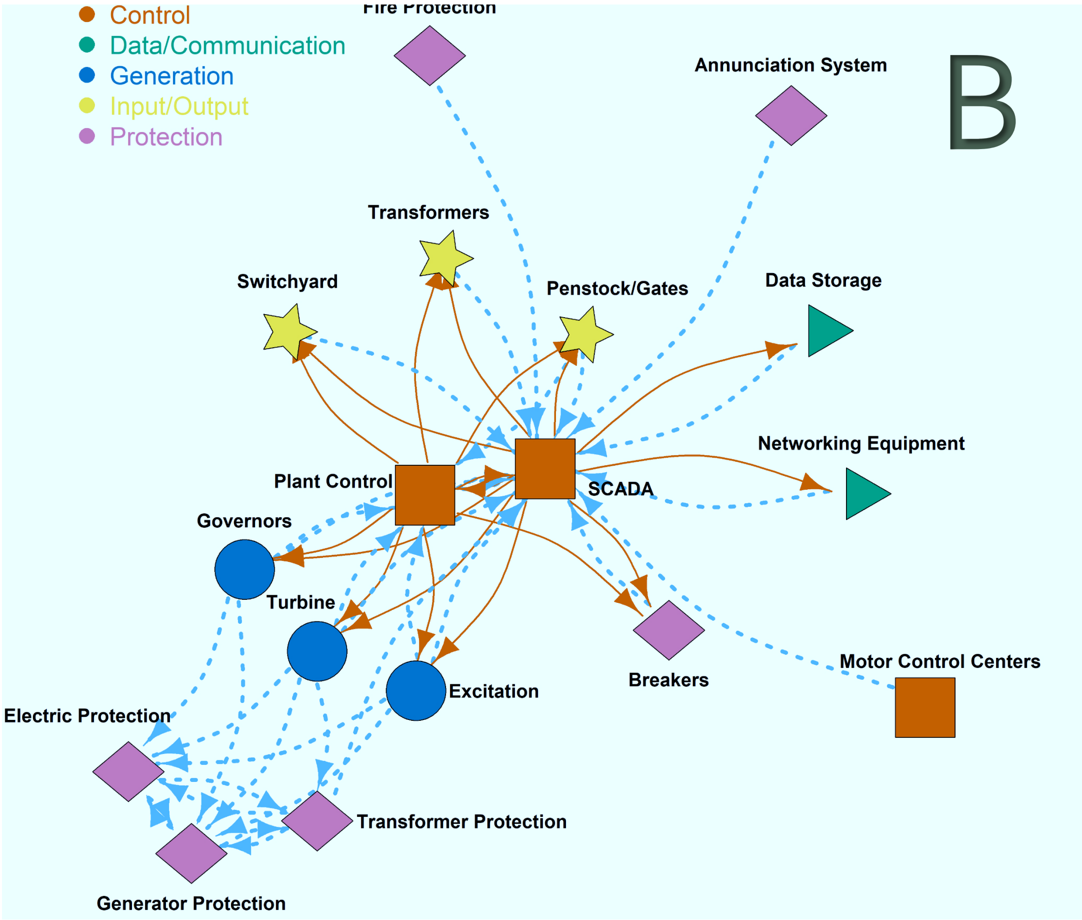
Type	Small <10MW	Medium 10<MW<30	Large >30MW	Total
Run-of-River	81	64	43	188
Storage	28	6	40	74
Pumped Storage			7	7
Other			6	6
Total	109	70	96	275

Performance: Sharing and Comparing Types

- Force-directed network diagram
  - Component classes
  - Communication or Control Links
  - Highly connected components group together

- Plants included in Type B:
- Large
- Storage and run of river

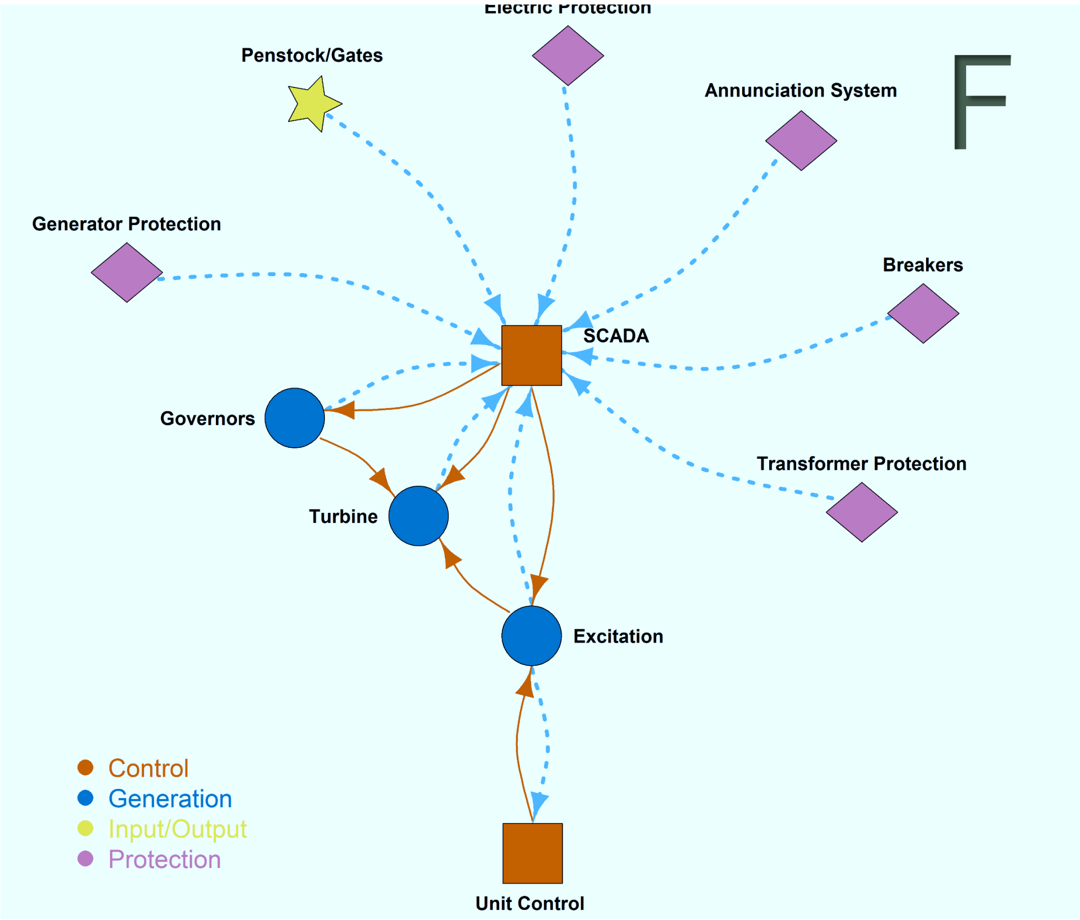
- Many feedback/ control loops
- Control integrates flow, power, and information



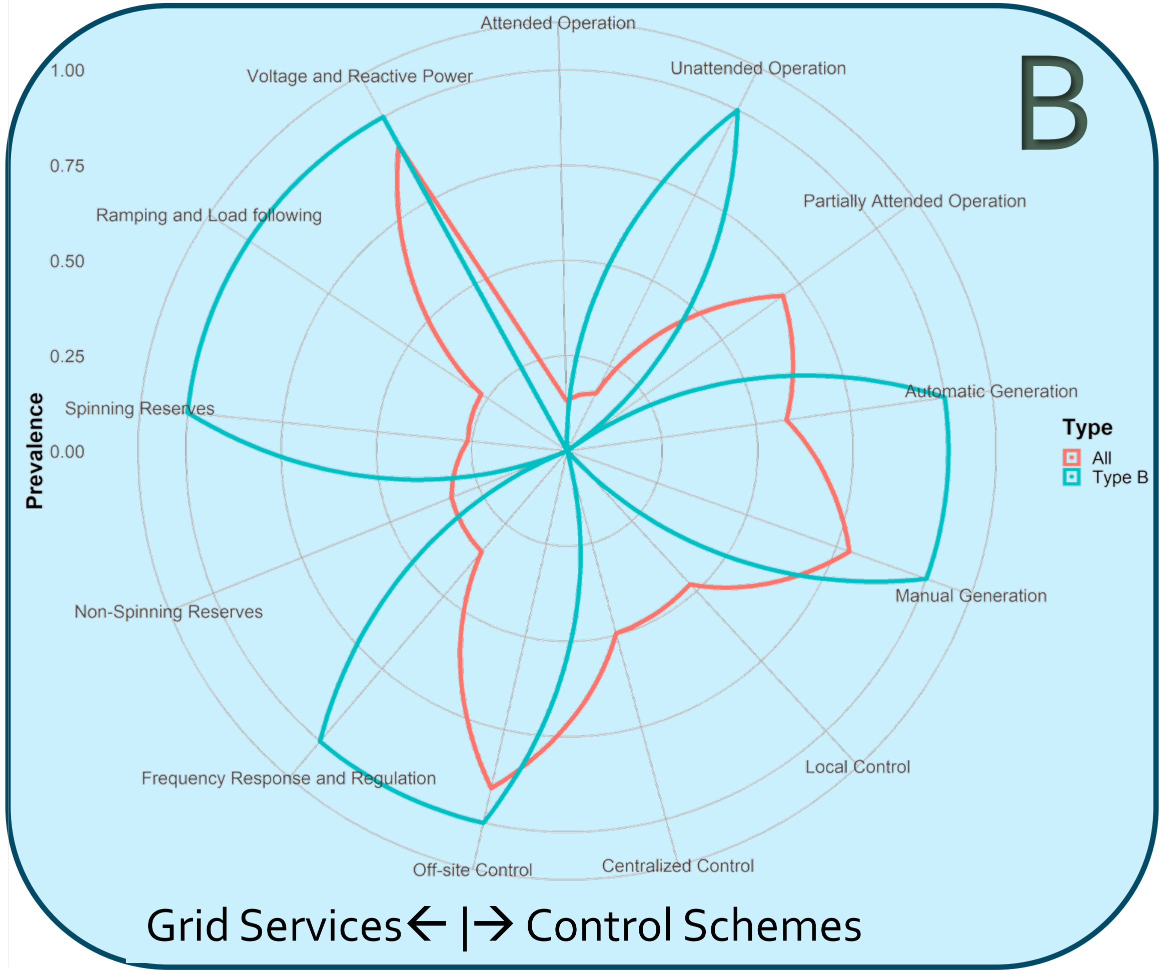
Sharing and Comparing Types, Continued

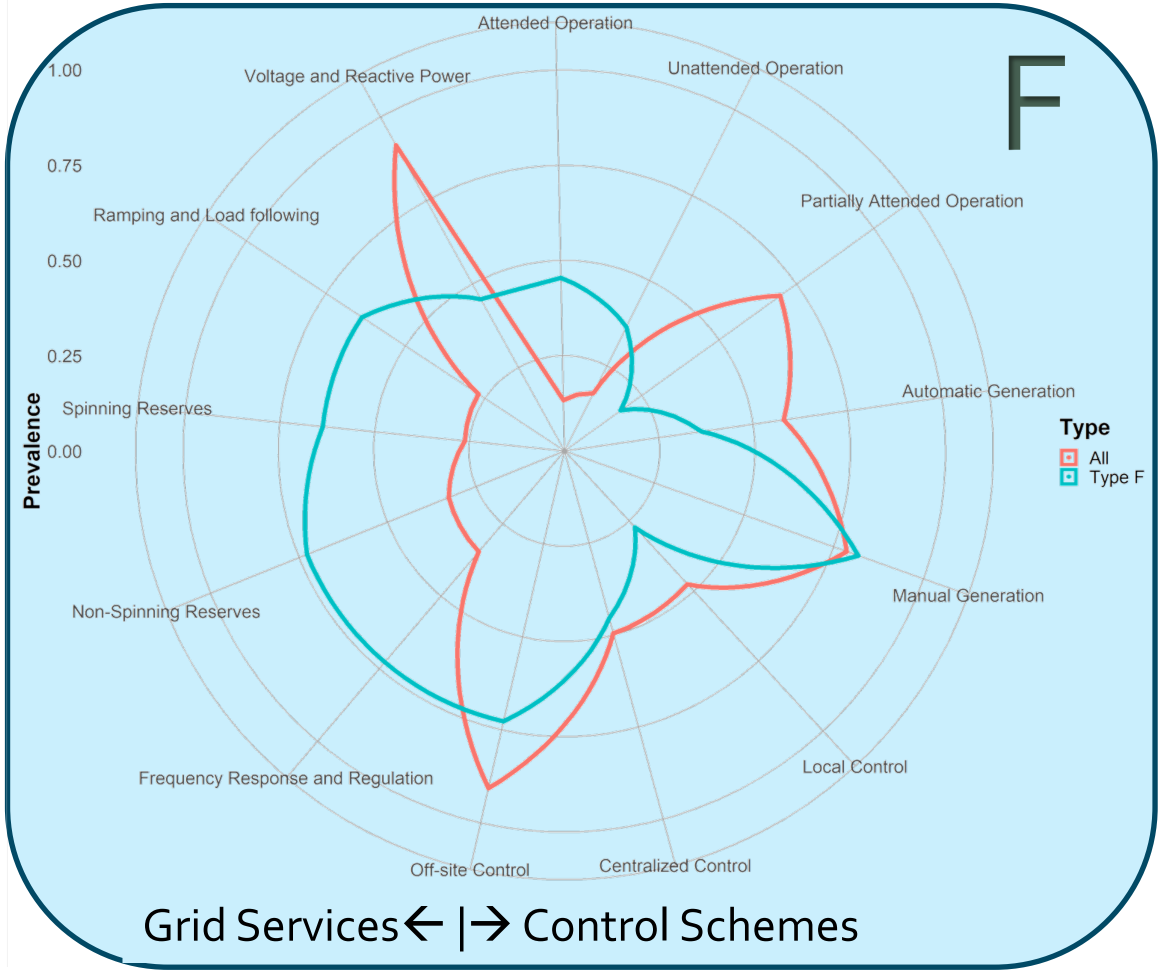
- Plants included in Type F:
- Mostly large
- Mostly storage

- Bidirectional data and control with the SCADA is common for generation components
- Because storage drives releases, not generation, control of water is only loosely integrated



Performance: Grid Services and Control Strategies by Type





Performance: Getting the word out

- Reaching back out to contributors
- Industry conferences (virtual due to covid restrictions)
- Federal Hydropower MOU (DOE/EERE, Reclamation, USACE)
- DOE-Norway Hydropower R&D MOU
- WPTO integrating types into research objectives
- Types informing DHS/CISA Scaled Hydropower Cyber Test Range development

Future Work

- Supporting WPTO Hydropower Cybersecurity Roadmap Development
- Ongoing Discussions with Federal Hydropower MOU partners
- Sharing findings in the Digitalization Track at the US-Norway Workshop on Collaborative Hydropower Research
- CISA Energy and Dams Infrastructure Sectors outreach to USACE and Reclamation
- Connecting with FERC and FEMP

Q&A