Pacific Northwest
NATIONAL LABORATORY

PNNL-31483

# Hydropower Cyber-Physical Configurations

## A typology for understanding the fleet of hydropower plants

September 2021

Kenneth D Ham, Ph. D.
Crystal Eppinger
Darlene Thorsen, CISSP
Charisa Powell
Paul Boyd
Abhishek Somani, Ph. D.
Michael Ingram, P.E.
Vladimir Koritarov

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

**DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
*operated by*
BATTELLE
*for the*
UNITED STATES DEPARTMENT OF ENERGY
*under Contract DE-AC05-76RL01830*

**Printed in the United States of America**

**Available to DOE and DOE contractors from the**
**Office of Scientific and Technical Information,**
**P.O. Box 62, Oak Ridge, TN 37831-0062;**
**ph: (865) 576-8401**
**fax: (865) 576-5728**
**email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service**
**5301 Shawnee Rd., Alexandria, VA 22312**
**ph: (800) 553-NTIS (6847)**
**email: orders@ntis.gov <https://www.ntis.gov/about>**
**Online ordering: http://www.ntis.gov**

PNNL-31483

# Hydropower Cyber-Physical Configurations

A typology for understanding the fleet of hydropower plants

September 2021

Kenneth D Ham, Ph. D.[1]
Crystal Eppinger[1]
Darlene Thorsen, CISSP[1]
Charisa Powell[2]
Paul Boyd[1]
Abhishek Somani, Ph. D.[1]
Michael Ingram, P.E.[2]
Vladimir Koritarov[3]

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

[1] Pacific Northwest National Laboratory, Richland, WA 99354
[2] National Renewable Energy Laboratory, Golden, CO 80401
[3] Argonne National Laboratory, Lemont, IL 60439

# Abstract

The U.S. Department of Energy's Water Power Technologies Office funded Pacific Northwest National Laboratory, Argonne National Laboratory, and the National Renewable Energy Laboratory to develop a typology to characterize the variety and pervasiveness of cyber-physical configurations across the nation's hydropower fleet. Outreach to plant operators returned configurations for 275 hydropower plants or approximately 12% of the fleet. Components (OT and IT), systems, and connections among systems differed among plants according to function, age, position in the river cascade, and many other factors. Nine cyber-physical configuration types labeled A through I, each including from 6 to dozens of plants. They were differentiated by how pervasive data and control connections were among cyber-physical components and how frequently control signals paired with data signals in a feedback loop. The flow of data and control within each type implies what cybersecurity vulnerabilities may exist and the most effective mitigation actions. A self-assessment approach allows plant operators to identify the configuration type like their plant and link to the lessons learned and best practices information. The cyber-physical typology reinforces the idea that hydropower facilities vary widely, but it also identifies groups that highlight similarities in how their cyber-physical components interact. These groups help address fleetwide cybersecurity needs by identifying a reasonable number of configuration types that share risks, vulnerabilities, and potential mitigations.

# Acknowledgments

The Department of Energy's Water Power Technologies Office funded this research. The team thanks Mark Christian and Tim Welch, the DOE program managers for this work. Their sage advice and guidance facilitated connections with prominent hydropower plant operators critical to project success. We appreciate those operators who contributed their time and effort in responding to our questionnaires on the cyber-physical configurations of their hydropower plants. Lastly, we thank Steve Wenke, co-chair of the National Hydropower Association's (NHA) Waterpower Innovation Council, and Luciana Ciocci, NHA Manager of Technical Services, for increasing the awareness of the project objectives and the coordination of our questionnaire through NHA member groups.

# Acronyms and Abbreviations

| | |
|---|---|
| CCNG | Combined-Cycle Natural Gas |
| EMS | Energy Management System |
| ES-C2M2 | Electricity Subsector Cybersecurity Capability Maturity Model |
| FERC | Federal Energy Regulatory Commission |
| IEC | International Electrotechnical Commission |
| IT | Information Technology |
| MW | Megawatt |
| NIST | National Institute of Standards and Technology |
| NREL | National Renewable Energy Laboratory |
| OT | Operating Technology |
| OUO | Official Use Only |
| PNNL | Pacific Northwest National Laboratory |
| RTU | Remote terminal unit(s) |
| SCADA | Supervisory control and data acquisition |

# Contents

# Figures

# Tables

# 1.0 Introduction

An increasingly dynamic electrical grid increases the need for generating plants to respond rapidly to fluctuating demand for electricity and other grid services. Hydropower plants must modernize, automate, and become more connected to deliver those services, serve new purposes, and produce additional value. Interconnectivity brings the unintended side effect of increasing exposure to new and unfamiliar cyber threats to safe and reliable operations. Operators need accurate and secure information that allows them to understand and mitigate the risks to their systems as they consider whether and how to access new value streams. Several models and tools exist that facilitate cybersecurity assessments to address the threats to an organization. The National Institute of Standards and Technology [NIST] Cybersecurity Framework, Energy Sector-Cybersecurity Capability Maturity Model (ES-C2M2), Buildings-C2M2, Federal Energy Regulatory Commission [FERC] Hydro Cyber/SCADA[1] Security Checklist – Form 3 and others are available to help users achieve a more secure cyber posture. Still, it would be more beneficial to begin those exercises with context from similar plants.

Hydropower projects differ in ways that reflect their authorized uses, age, role in the power system, water management, etc. Despite the diversity of plant purposes, the cyber-physical configuration of each plant involves a finite number of components and the connections among them. This research reached out to plant operators throughout the hydropower fleet to develop a library of cyber-physical configurations. A sample of 275 plants revealed nine distinct groups, establishing a cyber-physical typology.

A plant's cyber-physical type encapsulates how data and control signals flow among components, providing insight into the potential risks and possible mitigations. By assessing their plant configuration, operators can identify the most similar type and leverage this as a starting point for developing an approach to cybersecurity that fits their project's needs.

[1] Supervisory Control and Data Acquisition

# 2.0 Project Goals and Objectives

This research aims to simplify and accelerate the evaluation and mitigation of cybersecurity risks to the hydropower fleet by understanding the variety and pervasiveness of cyber-physical configurations. Categorizing those configurations into groups that share similar cyber-physical components, systems, and communication pathways (all of which define a cyber-physical type) highlights cybersecurity concerns they share and approaches for mitigating those concerns. The pervasiveness of configurations helps understand risks, identify trends as the hydropower fleet responds to the evolving electrical system, place hydropower needs in the context of other energy sectors (e.g., Combined Cycle Natural Gas [CCNG]), and prioritize efforts to mitigate risks.

The objectives were to:

1. Develop a reference framework for evaluating the cyber-physical configuration of dams based on standardized cyber-physical components, systems, and communication pathways.
2. Apply the reference framework to identify common and critical cyber-physical types and their pervasiveness across the hydropower fleet.

The information developed in this project will help dam operators collaborate to understand and improve cybersecurity and drive or inform future research needs.

# 3.0 The Hydropower Cyber-Physical Reference Framework

This project builds upon components defined in IEC[1] 62270 (IEC 2013) and extends the grid-level diagram presented in NISTIR-7628 (NIST 2014) to provide a reference framework for hydropower plants.

## 3.1 Creating the Framework

This study developed an initial conceptual diagram representing the reference framework to spur discussion, arranging common component types to represent a broad range of potential configurations. Outreach to dam operators used this initial diagram to elicit information about individual dams' components and connections.

## 3.2 Components

Generalized operating and information technology components are needed to create diagrams that capture important hydropower plant activities and control schemes. Several types of equipment are involved with the production and transmission of power:

1. Turbine – A machine that produces power in which a wheel or rotor revolves by a fast-moving water flow.
2. Governor – A device that measures and regulates turbine speed by controlling wicket gate angle to adjust the water flow to the turbine.
3. Generator – A device that converts the rotational energy from a turbine to electrical energy
4. Exciter – An electrical device that supplies direct excitation to the generator field during the startup of the unit
5. Breakers – A switching device that is capable of closing or interrupting an electrical circuit
6. Switchgear – The switches, breakers, and other devices used for opening or closing electrical circuits and connecting or disconnecting generators, transformers, and other equipment
7. Transformer – A device for changing alternating current (AC) to higher or lower voltages.

Additional equipment controlling or supporting the production of power:

1. Control systems
    a. SCADA
    b. Plant Control
    c. Unit Control
2. Water level and flow control.
    a. Waterway control
    b. Gates and outlets

[1] International Electrotechnical Commission

   c. Environmental releases.
3. Protection systems – Systems that monitor, alarm, or interrupt operation to maintain operating conditions of generating equipment within acceptable ranges
   a. Electrical Protection
   b. Generator Protection
   c. Transformer Protection
4. Auxiliary systems – Systems required to maintain and operate the plant
   a. Fire Protection
   b. Plant Security
   c. Backup Power Systems
   d. Maintenance Systems
5. Data equipment
   a. Networking
   b. Data Storage

## 3.3 Control

In addition to components and systems, the reference diagram included several possibilities for the implementation of control:

1. **Local Control**: At the controlled equipment or within sight of the equipment.
2. **Centralized Control**: Remote from the controlled equipment, but within the plant.
3. **Off-site Control**: Remote from the plant.

These variations on control inform the cyber-physical configuration typology because they influence how components are connected. Centralized and off-site control drives how plant control systems or supervisory control and data acquisition (SCADA) systems connect to the operating equipment to allow control across digital networks.

## 3.4 The Conceptual Reference Diagram

The conceptual reference diagram represents information technology (IT) and operational technology (OT) components and the communication pathways found at hydropower plants. In simple terms, IT components deal with data and the flow of information, and OT components deal with operational processes carried out by machines. The distinction between these two types has been helpful when considering cybersecurity. OT networks and protocols were traditionally separated from those common in IT, though that separation is diminishing. Figure 1 illustrates the components and connections of the conceptual reference diagram. Individual plant diagrams would show only those components and links found at the plant. Items outside the plant boundary are connection points for the grid level diagram in NISTIR-7628 (NIST 2014).

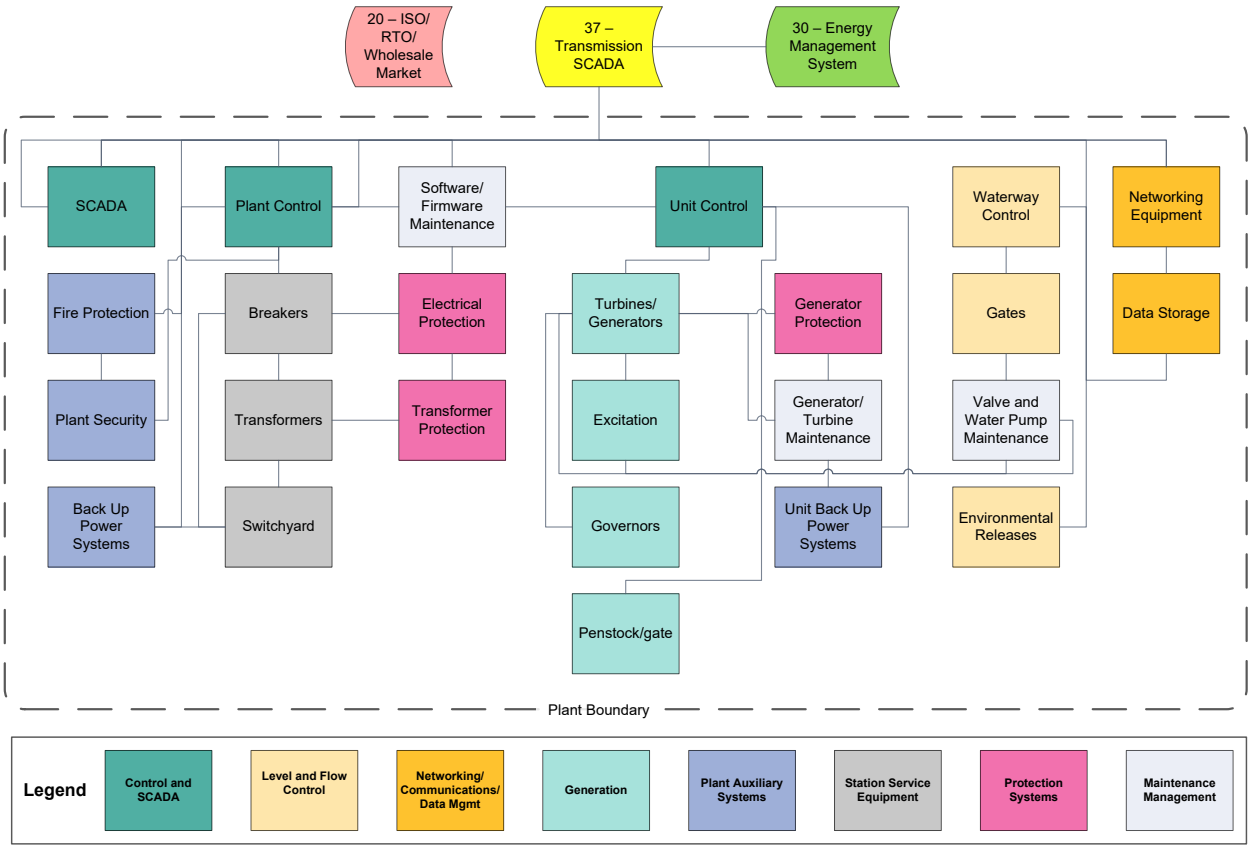


Figure 1. Conceptual Reference Diagram

# 4.0 Surveying the Hydropower Fleet

Identifying the types of cyber-physical configurations and their pervasiveness across the hydropower fleet required a broad outreach to operators. The plant configurations they supplied helped identify similar, common types that provide insight into the fleet.

## 4.1 Developing the Questionnaire

A simple 2-page questionnaire was developed based on the reference diagram to allow operators to provide plant configuration information. The objectives were to:

1. Keep things simple and at the level needed for this analysis
2. Minimize the operators' time spent filling out the questionnaire
3. Provide a straightforward way to tabulate components
4. Allow connections without restricting pathways to the preconceived diagram
    a. Data
    b. Control
5. Characterize the overall plant and its grid role
    a. Size
    b. Generating type (peaking, run-of-river, pumped storage, etc.)
    c. Services provided to the electrical grid (spinning reserves, frequency response, and regulation, etc.)
6. Provide a secure way to return filled questionnaires
7. Allow the respondent to identify data protection needs (Official Use Only, Commercial Proprietary).

Page 1 of the questionnaire asked the respondent to indicate how to protect the data, the plant's size, its roles in the water and energy systems, and how control is implemented (Figure 2). In those cases where respondents preferred not to fill Project Name and Project Owner fields, they were encouraged to provide an alternate obfuscated entry so that it would be possible to communicate with them about any questions about the returned data. The accompanying email encouraged respondents uncomfortable with providing the information requested by a question to leave it blank.

Page 2 asked respondents to tabulate component types present at the plant by indicating a quantity in the first column (Figure 3). Respondents entered lists of components receiving data from (column 2) or sending control signals to (column 3) the component type in each row. This matrix of information defined the cyber-physical configuration of a plant.

Operators of multiple similar plants sometimes responded with a questionnaire for each distinct cyber-physical configuration within their fleet, indicating how many individual plants that questionnaire represented. This approach allowed those operators to avoid an undue burden in responding, which might otherwise have discouraged them from returning any questionnaires.

## 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

Figure 2. Page One of the Plant Configuration Questionnaire

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_____ | | | |

Figure 3. Page Two of the Plant Configuration Questionnaire

## 4.2 Coordinating Outreach and Responses

Getting plant configuration information was not merely a matter of sending out questionnaires and awaiting replies. Plant operators are understandably cautious about sharing cyber-physical characteristics of plants. They must be confident that the effort involved in sharing is worthwhile and that their data will be safe.

### 4.2.1 Hydropower Owners and Operators

The laboratories conducting this study and the Water Power Technologies Office have extensive ties to power plant operators, industry associations, and persons involved in hydropower development and refurbishment. Those ties helped identify plant operators that could consider the request for information about plant configurations. Outreach to those individuals included sharing the project's objectives, the information needs and level of detail, and the data protection approach. These outreach activities were extensive and extended beyond our expected timeline, at least in part due to the disruptions to office work caused by the SARS-CoV2 pandemic. Approximately two-thirds of organizations contacted agreed to return questionnaires. Around half of those organizations ultimately returned questionnaires. Despite the sensitivity of the information requested, the response rate was similar to the average of 35% for research surveys in general (Baruch and Holtom 2008).

Distributing outreach efforts across size classes, with a specific push to include pumped storage, resulted in responses spread across various categories of plants. Prioritizing organizations with several plants proved time- and cost-effective but resulted in the underrepresentation of small hydro plants. Returned questionnaires encompassed 275 plants, distributed across various sizes and types (Table 1). That number represents approximately 12% of the 2298 plants included in the database: Existing Hydropower Assets for 2020 (Johnson et al. 2020).

Table 1. Number of Plant Responses by Size and Type

| 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 |

## 4.3 Securing Information

The information we sought about hydropower plants needed to be protected to keep it out of the hands of those with ill intent. A multi-pronged data security approach built on a foundation of organizational security practices and added project-specific processes to secure data in transit

from the respondent to us and in our information system. Requiring reviews before release ensured that analysis products or discussions developed from the original data did not reveal sensitive information.

Encryption and passwords secured data during transit. Respondents filled out a form for each plant using a password and emailed those back to the project manager at Pacific Northwest National Laboratory (PNNL). Where respondent policies prohibited data transmission through email, we provided alternate means to submit forms through encrypted channels.

A secure server qualified to contain OUO information was stood up at PNNL to serve the project's needs. Project staff transferred questionnaire data to this server, which also hosted project documents. Project staff located at Argonne National Laboratory or the National Renewable Energy Laboratory accessed the server using secure tokens for authentication. This approach allowed staff to share links to items on the server, eliminating emailing documents or information among project personnel. Analyses and reporting also incorporated data protections. Classification experts reviewed each product or deliverable to avoid inadvertently releasing sensitive information.

## 4.4 Compiling Questionnaire Data

The layout of the questionnaire as a matrix of connections among components made filling it out both quick and easy. The questionnaire allowed data and control connections in either direction between any two elements. Many links not found on the original conceptual diagram (Figure 1) appeared in the cyber-physical configurations defined by respondents. A total of 616 unique connection types (out of a possible 2048) arose in the returned questionnaires. This variety of connections was a key source of information on how configurations differed among plants. Combinations of components varied less across the plants. Responses included 57 combinations of component types (presence or absence) out of a possible 1024.

Converting the questionnaires into data for analysis was also straightforward. First, the filled, returned questionnaires were converted into spreadsheet form and pivoted for loading into a relational database. Then, within the database, the tabulated responses were grouped and arranged as needed for analysis.

The matrix of components and connections identified in a questionnaire response defined the cyber-physical configuration. The following section aimed to identify characteristics of those configurations that defined similar groups of plants.

### 4.4.1 Reducing the Influence of Rare Responses

For ease of filling out the questionnaire, respondents could identify any possible connection among components. Infrequently identified connections could be due to unique interpretations of components or connections, or they could be consistent interpretations and yet truly rare. In either case, uncommon connections are not ideal for creating a typology for wide application. To narrow the number of connections included in the analyses and focus on those that occurred more broadly, we 1) eliminated connections from a component to itself, 2) eliminated components rarely included in connections, and 3) retained only those connections in at least five questionnaires and across at least three responding organizations. Those criteria eliminated rarely identified connections but left 163 connection types common across many plants and organizations as raw material for developing the typology.

# 5.0 Developing a Hydropower Cyber-Physical Typology

This section details the process of defining a typology of cyber-physical configurations to organize the wide variation across the fleet into an understandable structure.

## 5.1 Identifying Common Cyber-Physical Configuration Types

To develop a set of cyber-physical configurations across the fleet, we sought to aggregate individual plant configurations with similar combinations of components and connections into groups. The inputs were the selected data or control connections at each plant. A joining technique (Tree clustering) in Statistica software (Statsoft) grouped similar plants on the presence or absence of control and data relationships among components. A balanced grouping resulted from choosing a linkage distance that avoided singular or huge groups. The resulting nine configuration types were labeled A through I, the order of which is not meaningful. The following sections detail the distinctions among these configuration types.

### 5.1.1 Component Functional Classes

Grouping components into classes according to their higher-level functions (Table 2) helps understand where control and data signals flow. The nature of communications among these groups aid in recognizing control and feedback schemes in the network diagrams for types in the following sections. These groupings are self-explanatory, apart from Input/Output, which focuses on controlling water (input) and the delivery of electricity to the grid (output).

Table 2. Functional Classes of Components

| Control | Data/Communication | Generation | Input/Output | Protection |
|---|---|---|---|---|
| Motor Control Centers | Data Storage | Excitation | Penstock/Gates | Annunciation System |
| Plant Control | Networking Equipment | Governors | Switchyard | Electric Protection |
| SCADA | | Turbines | Transformers | Generator Protection |
| Unit Control | | | | Transformer Protection |
| | | | | Fire Protection |
| | | | | Breakers |
| | | | | Back Up Power System |

### 5.1.2 Operational Characteristics

Respondents identified several operational characteristics of the plant. These responses were not used in grouping the plants into cyber-physical configuration types. Still, they can help understand what plant requirements may be driving the connections among cyber-physical components.

#### 5.1.2.1 Capacity and operational class

Respondents assigned each facility to either large (> 30 MW), medium (10 < MW < 30), or small (< 10 MW) capacity. They classified the mode of operation for each facility as either Run-of-river, Storage, Pumped Storage, or other.

#### 5.1.2.2 Grid services

Respondents could indicate that a plant supplied any combination of the following grid services:

- Frequency Response and Regulation
- Spinning Reserves
- Non-spinning Reserves
- Ramping and Load Following
- Voltage and Reactive Power Support.

#### 5.1.2.3 Changes in generation

Respondents could indicate that changes in generation occur manually, automatically, or both. Respondents also identified the source of operational inputs:

- Locally, at the equipment
- Centralized, remote from the equipment, but within the plant
- Off-site, remote from the plant.

#### 5.1.2.4 Facility operation

Respondents could select one of the following to indicate whether operators were present some, all, or none of the time:

- Attended: Staffed at all times
- Unattended: Unstaffed
- Partially Attended: Staffed during scheduled hours.

#### 5.1.2.5 Control system type

Respondents classified their plant's control system as one of the following:

- Traditional, hardwired supervisory control - master stations, nonprogrammable remote terminal units (RTUs)
- Open, energy management systems (EMS), SCADA – networked personal computers (PCs), user-programmable RTUs
- Closed, stand-alone systems – proprietary controllers/operator consoles.

## 5.2 The Cyber-physical Typology

This section presents the nine cyber-physical types identified in this project. Each subsection includes details on the sizes and classes of plants in the type, how data and control signals flow

among components, the plant control schemes, and the services provided. Network diagrams illustrate the flow of data and control signals for comparison among types. A force-directed (Fruchterman-Reingold) layout algorithm places highly connected components closer together to highlight associations. Component shapes and colors reflect their functional class (Table 2, above). Rose plots contrast the prevalence of control schemes or services provided by plants in the type relative to all plants surveyed.

### 5.2.1 Type A

Cyber-physical configuration Type A included seven medium and large capacity storage plants (Table 3). Control connections were prevalent among components in Type A plants, with comparatively few data connections (Figure 4). SCADA and Unit Control components fell near water management and generation, while Plant Control fell closer to electrical power output. Most communications involved the three primary control components, giving this diagram a hub-and-spoke design.

Table 3. Number of Plants by Size and Type included in Configuration Type A

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 0 | 0 |
| **Run of River** | 0 | 0 | 0 | 0 |
| **Storage** | 0 | 2 | 5 | 7 |
| **Total** | 0 | 2 | 5 | 7 |

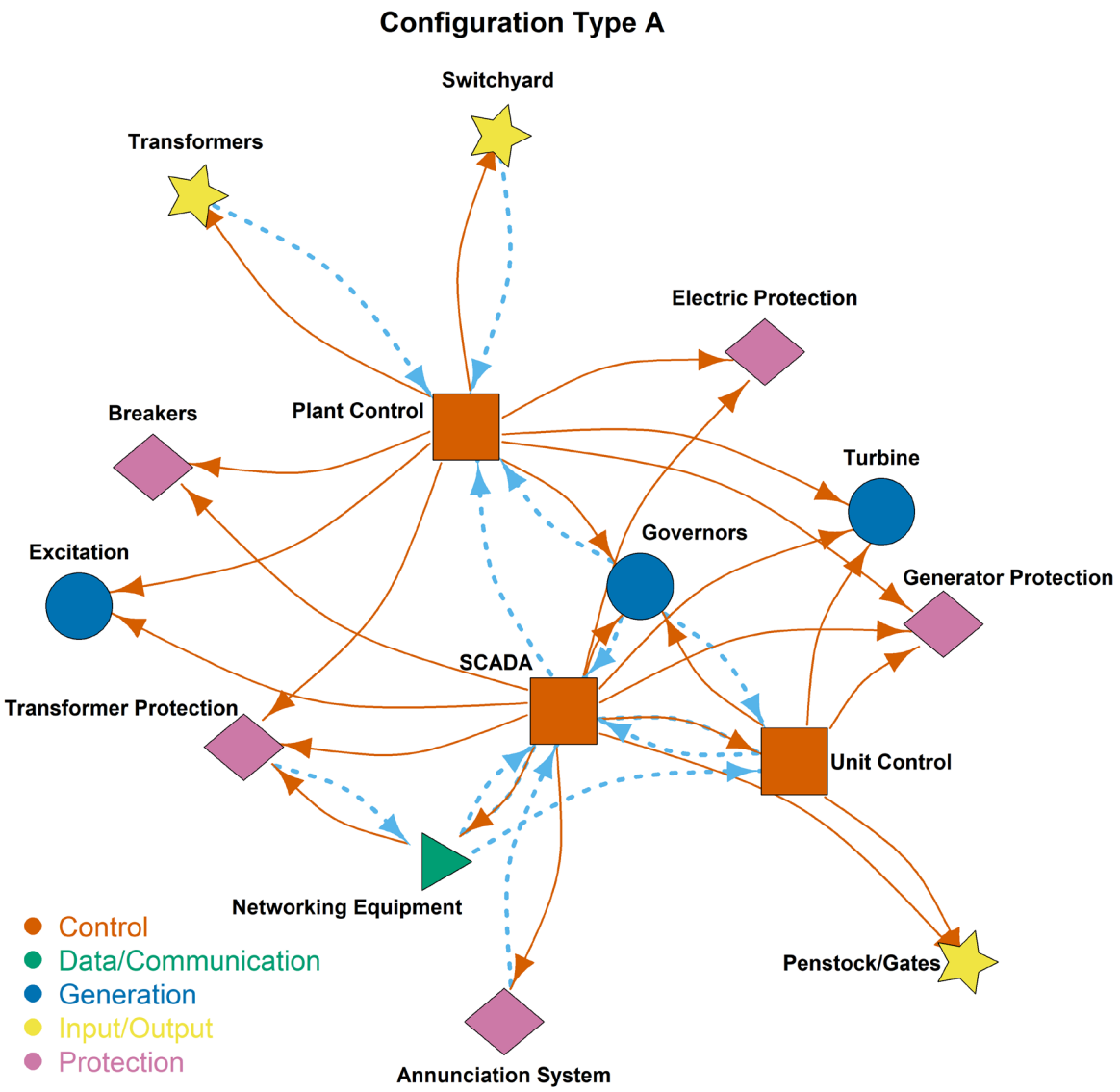


Figure 4. Network Diagram for Configuration Type A. Solid arrows indicate the flow of control among components, and dashed arrows indicate the flow of data.

Comparing the prevalence of plants' operational characteristics within Type A with the overall fleet of plants identified in this project using a "rose" plot revealed some striking differences (Figure 5). The rose plot maps higher prevalence at a greater distance from the center on the radial representing each characteristic. Prevalence ranges from 0 (=absent) at the center of the plot to 1 (=always present). Type A plants (blue line) differed from the fleet (all responses, red line) by a high prevalence of providing grid services (frequency response and regulation, non-spinning reserves, ramping and load following, spinning reserves, and voltage and reactive power). Plants of this type were operated unattended and off-site. Generation could be either automatic or manual. Attended or partially attended operations were absent, as were local and centralized control.

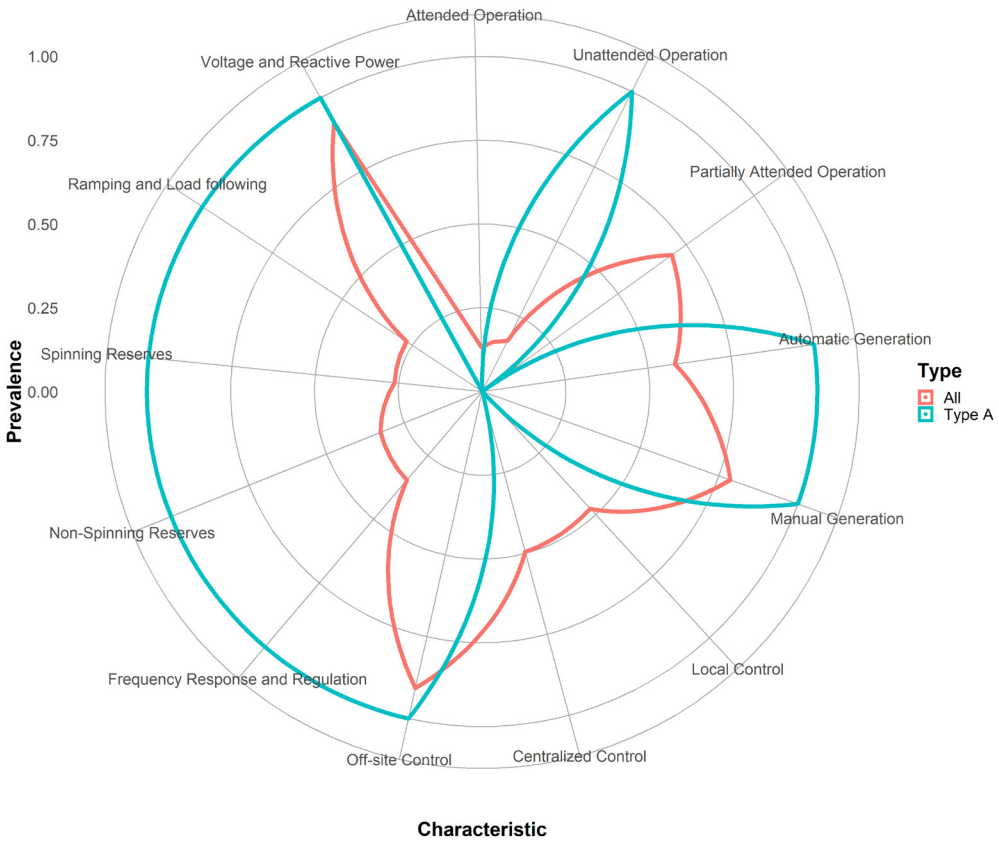


Figure 5. Prevalence of Plant Operational Characteristics for Configuration Type A

### 5.2.2 Type B

Type B includes two run-of-river plants and five storage plants, all large (Table 4). The Type B network includes control connections from SCADA and Plant Control to Data/Communication, Generation, and Input/Output components. Data flows back to the control components with numerous connections among generation and protection components (Figure 6). The network exhibits a hub-and-spoke layout centered around plant control and SCADA. However, protection components deviate from that layout, with many direct communication pathways not passing through a control component.

Table 4. Number of Plants by Size and Type included in Configuration Type B

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 0 | 0 |
| **Run of River** | 0 | 0 | 2 | 2 |
| **Storage** | 0 | 0 | 5 | 5 |
| **Total** | 0 | 0 | 7 | 7 |

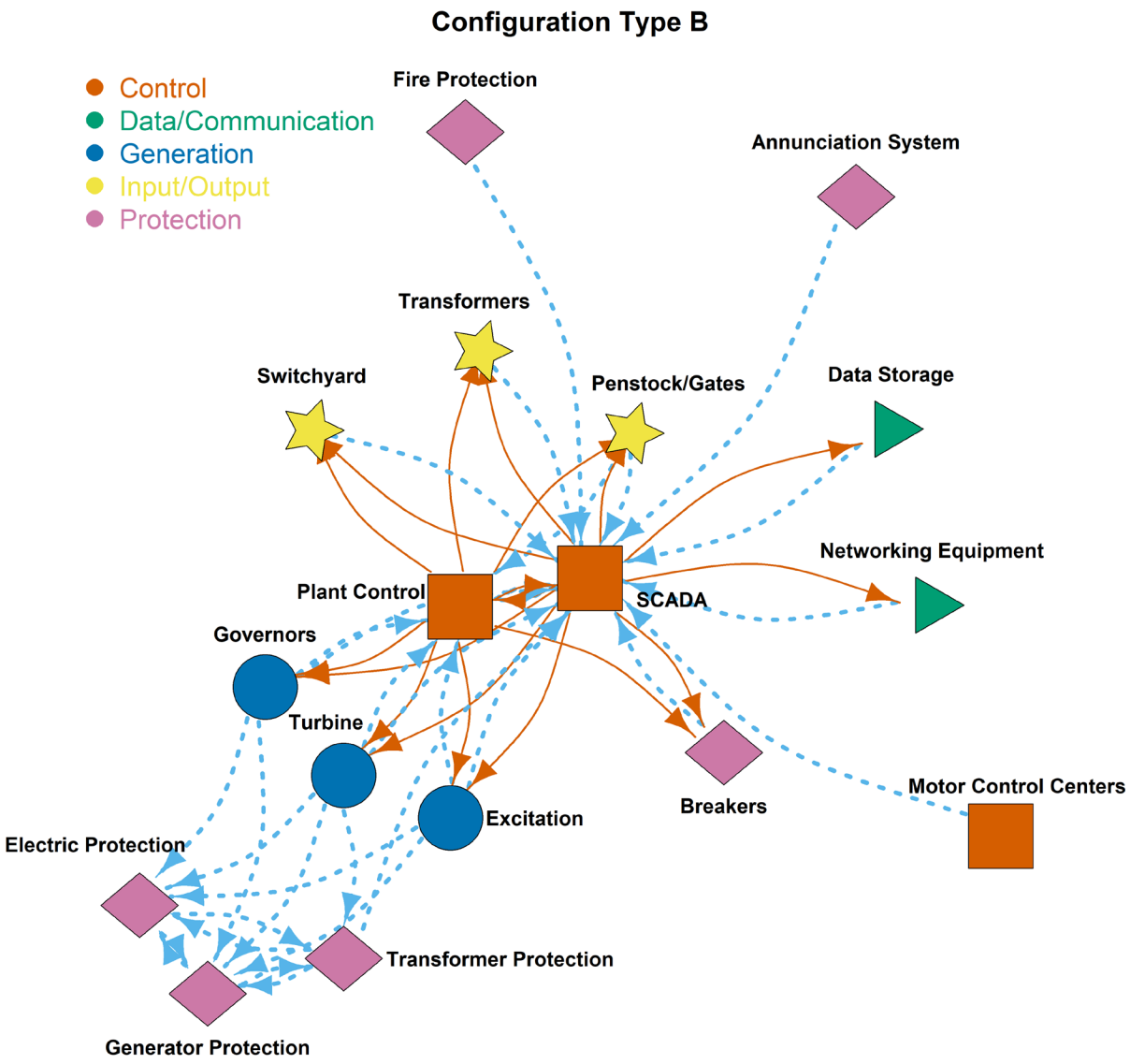


Figure 6. Network Diagram for Configuration Type B. Solid arrows are control connections, and dashed arrows are data connections.

Type B plants differed from the fleet by a higher prevalence providing grid services, except non-spinning reserves (Figure 7). Operation of Type B plants was unattended, control was off-site, and generation could be either automatic or manual.

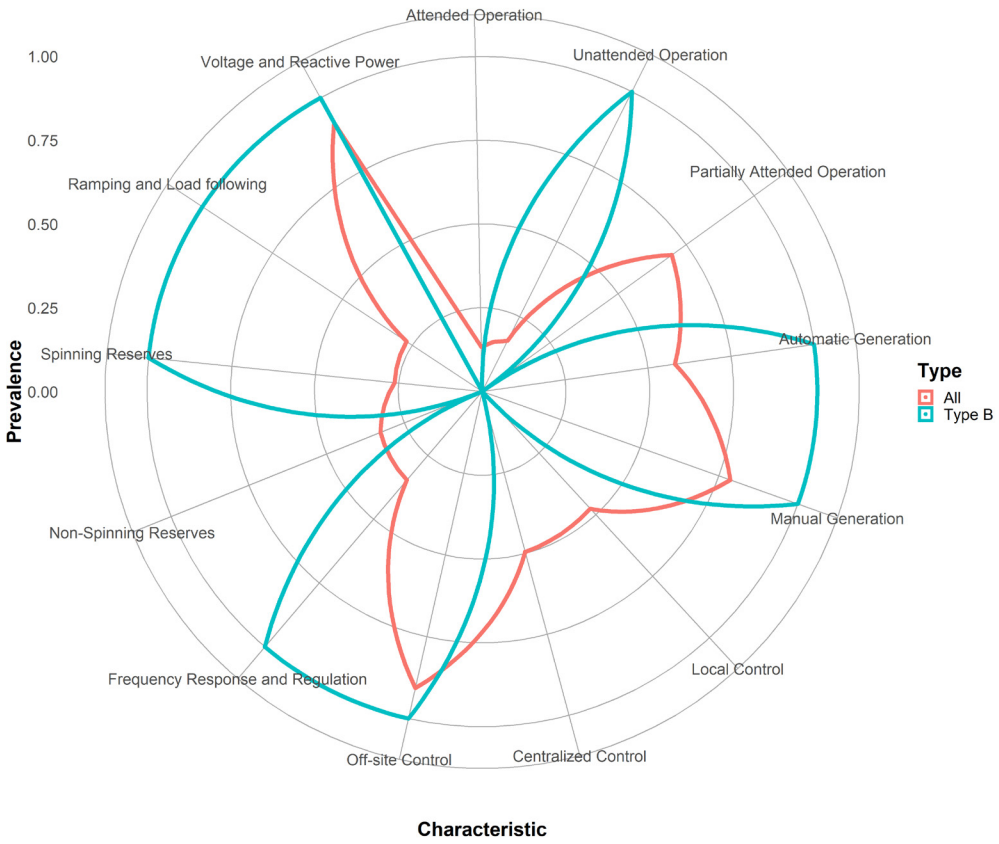


Figure 7. Prevalence of Plant Operational Characteristics for Configuration Type B

### 5.2.3 Type C

Type C includes two run-of-river and six storage plants, all large (Table 5). In the absence of Unit Control and Plant Control components, most control connections originated from the SCADA system (Figure 8). In addition, many components sent data to the Annunciation System. Thus, the network follows a hub-and-spoke layout in general, with instances of point-to-point communication involving the Generator and Generator Protection.

Table 5. Number of Plants by Size and Type included in Configuration Type C

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 0 | 0 |
| **Run of River** | 0 | 0 | 2 | 2 |
| **Storage** | 0 | 0 | 6 | 6 |
| **Total** | 0 | 0 | 8 | 8 |

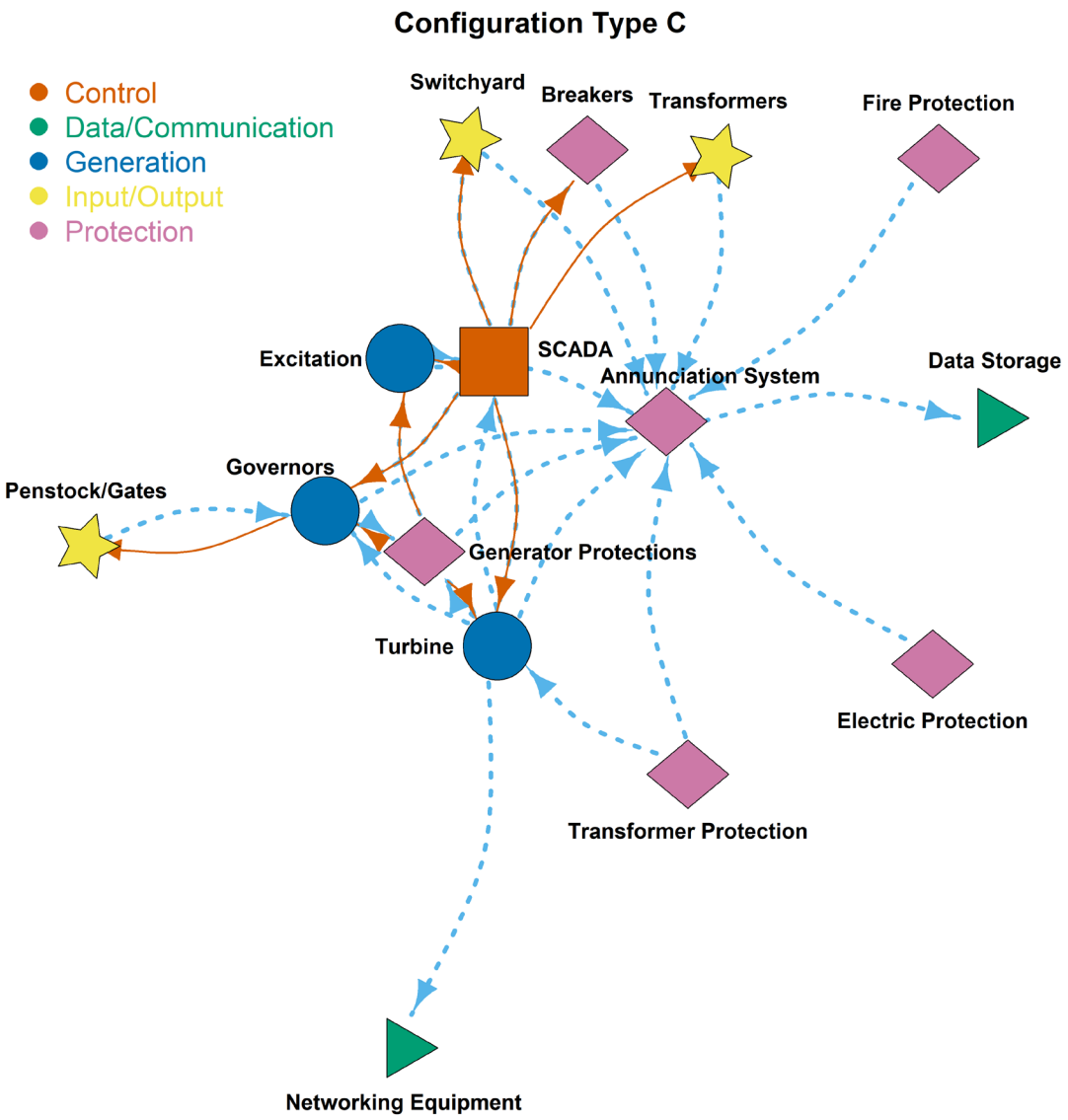


Figure 8. Network Diagram for Configuration Type C. Solid arrows are control connections, and dashed arrows are data connections.

Type C plants were distinguished from the fleet by a high prevalence of frequency response and regulation, non-spinning reserves, and voltage and reactive power services, but with no spinning reserves or ramping and load following (Figure 9). Partially attended operation was most common, along with a few attended plants. Unattended operation did not occur. Centralized control, local control, and manual generation were notably more prevalent than for the fleet.


Figure 9. Prevalence of Plant Operational Characteristics for Configuration Type C

### 5.2.4 Type D

Cyber-physical configuration Type D included 139 plants, all but five of which were small- or medium-sized run-of-river plants (Table 6). Two large pumped-storage plants, two large storage plants, and a small storage plant were the exceptions. Control connections in Type D plants were numerous, originating from various component types, often with complementary data connections (Figure 10). The variety of connections creates a point-to-point configuration.

Table 6. Number of Plants by Size and Type included in Configuration Type D

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 1 | 1 |
| **Run of River** | 80 | 53 | 2 | 135 |
| **Storage** | 1 | 0 | 2 | 3 |
| **Total** | 81 | 53 | 5 | 139 |

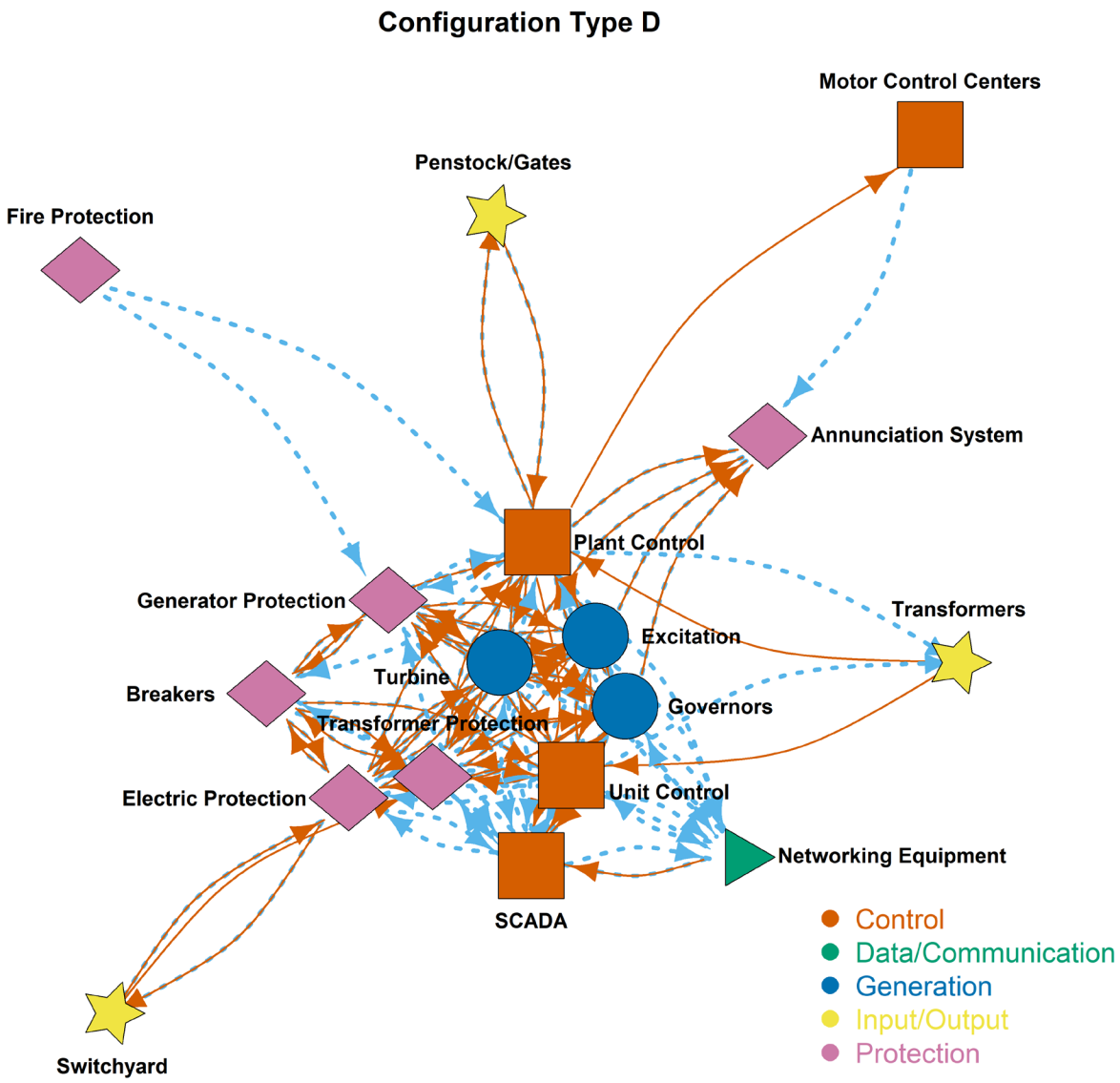


Figure 10. Network Diagram for Configuration Type D. Solid arrows are control connections, and dashed arrows are data connections.

The large proportion of plants (>50% of plants in our responses) falling into Type D means that differences among this type and the fleet were subtle (Figure 11). Off-site control and partially attended operation were more prevalent among Type D plants, along with a greater prevalence of manual generation. Type D plants provided voltage and reactive power, but none of the other grid services.


Figure 11. Prevalence of Plant Operational Characteristics for Configuration Type D

### 5.2.5 Type E

Type E included two large run-of-river plants and four large storage plants (Table 7). These plants have a sparse set of control connections originating from various component types (Figure 12). Data connections are numerous, exhibiting a point-to-point layout.

Table 7. Number of Plants by Size and Type included in Configuration Type E

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 0 | 0 |
| **Run of River** | 0 | 0 | 2 | 2 |
| **Storage** | 0 | 0 | 4 | 4 |
| **Total** | 0 | 0 | 6 | 6 |

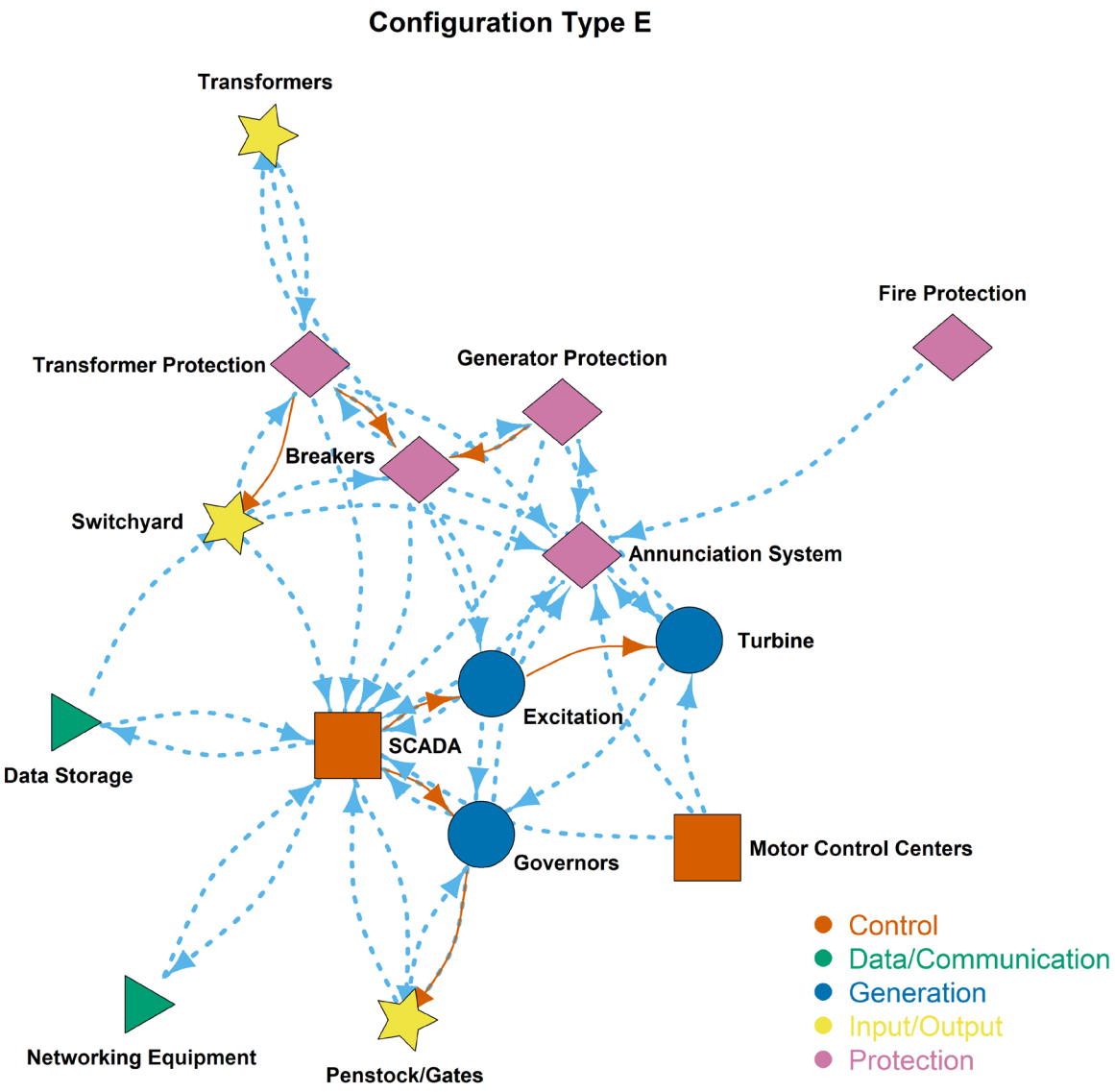


Figure 12. Network Diagram for Configuration Type E. Solid arrows are control connections, and dashed arrows are data connections.

Compared to the fleet, Type E plants were more likely to provide all types of grid services (Figure 13). Local control, partially attended operation, and unattended operation were not found among Type E plants. In contrast, attended operation, centralized control, automatic generation, and manual generation were more prevalent than the fleet.

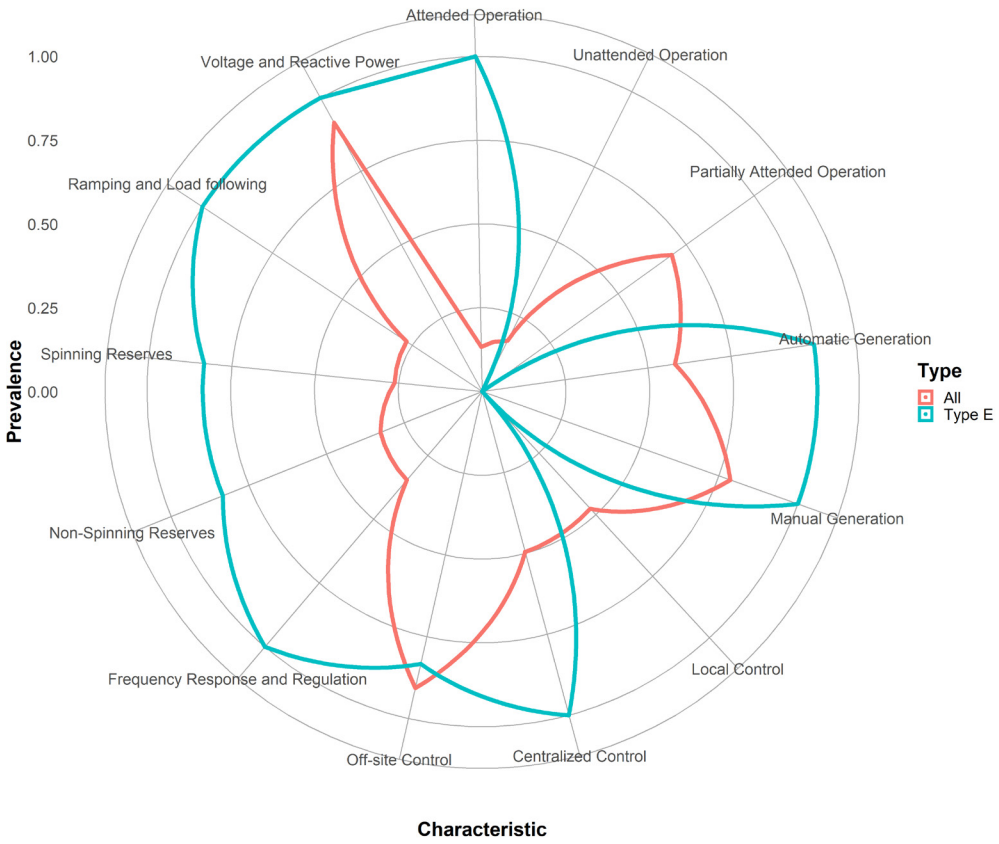


Figure 13. Prevalence of Plant Operational Characteristics for Configuration Type E

### 5.2.6 Type F

Cyber-physical configuration Type F included 11 mostly large plants across the three major classes (Table 8). Control connections among the SCADA, Unit Control, and generation components show the primary focus of control on generation, with complementary data connections providing feedback (Figure 14). Additional connections bring data from the remaining components to the SCADA. In general, this network exhibited a hub-and-spoke layout centered on the SCADA.

Table 8. Number of Plants by Size and Type included in Configuration Type F

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 1 | 1 |
| **Run of River** | 0 | 0 | 3 | 3 |
| **Storage** | 0 | 3 | 4 | 7 |
| **Total** | 0 | 3 | 8 | 11 |

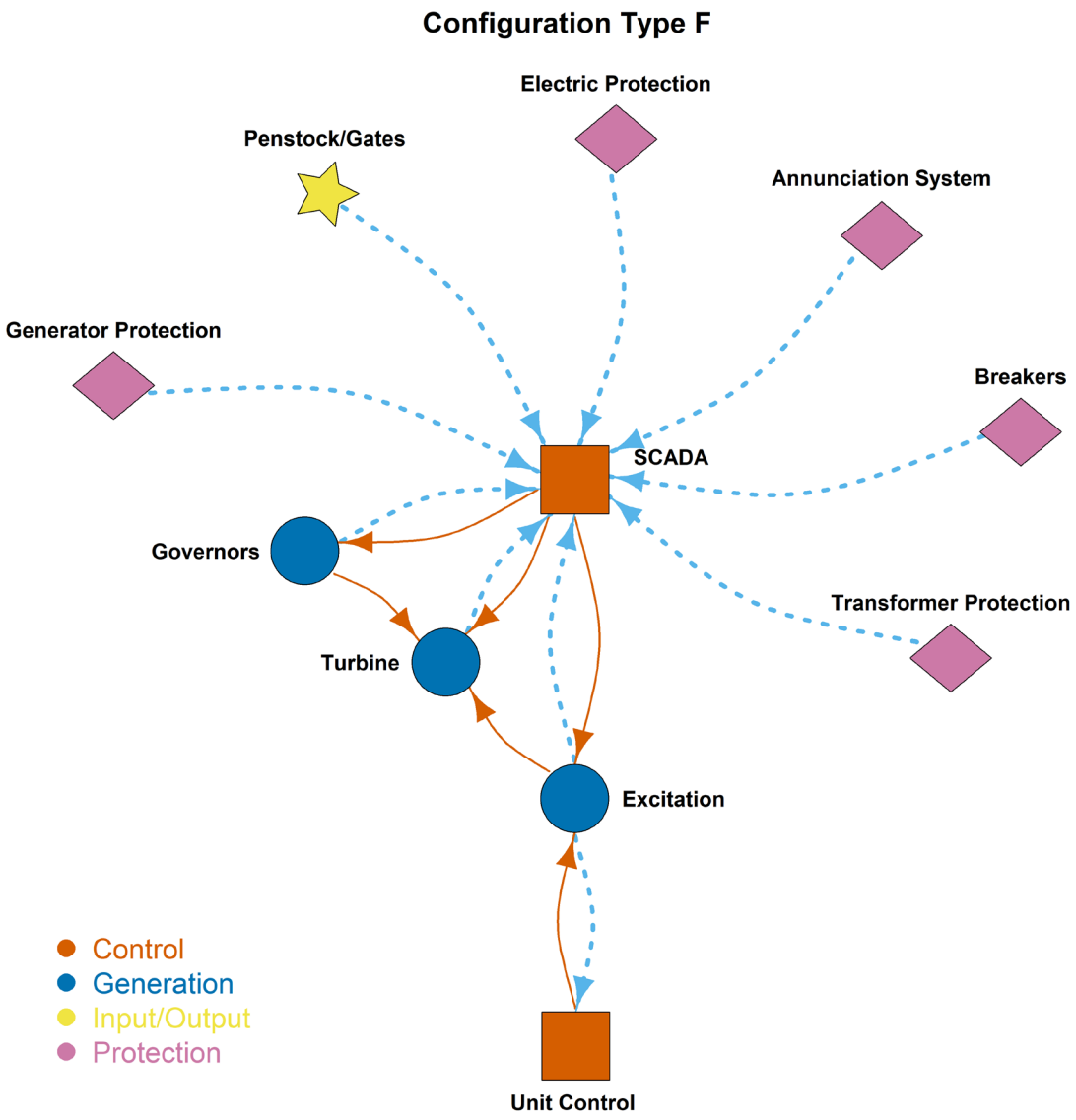


Figure 14. Network Diagram for Configuration Type F. Solid arrows are control connections, and dashed arrows are data connections.

Type F plants were more likely to provide grid services than the fleet, but a smaller proportion provided voltage and reactive power (Figure 15). These plants relied more on attended operation, but off-site control and manual generation were similar to the fleet.

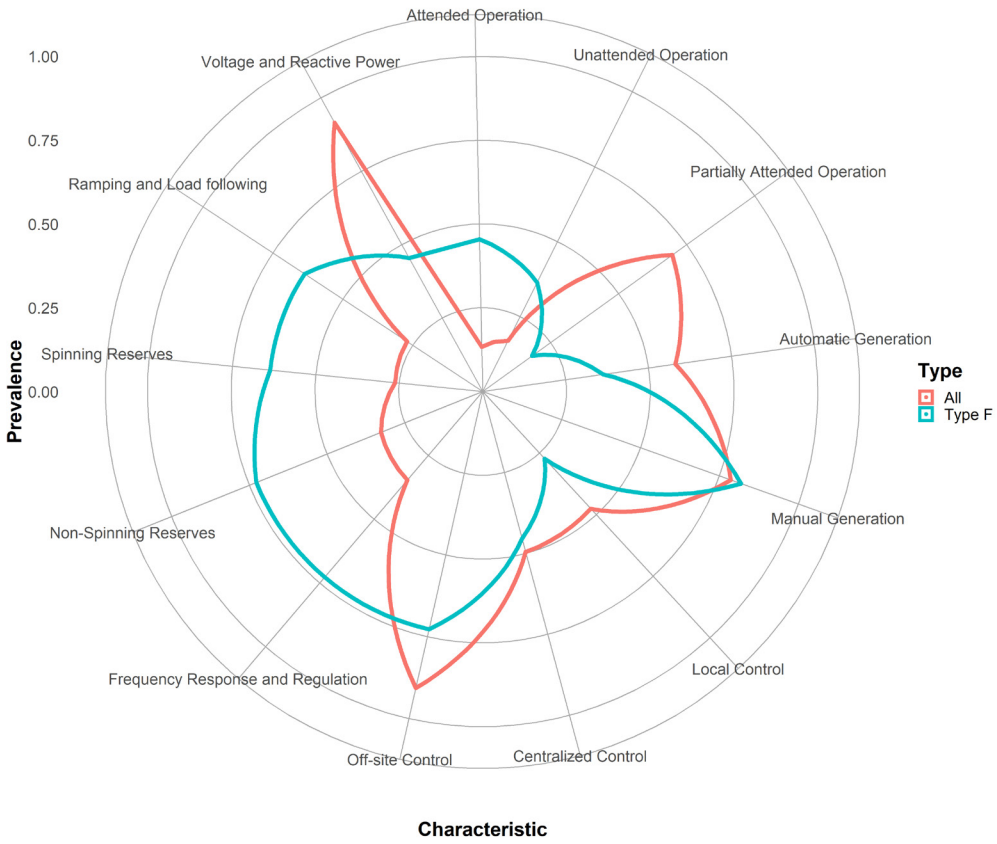


Figure 15. Prevalence of Plant Operational Characteristics for Configuration Type F

### 5.2.7 Type G

Cyber-physical configuration Type G included forty plants, with the majority falling into the run-of-river class and having medium or large capacities (Table 9). Five large plants of various classes round out the group. Control connections emanate solely from control components to generation and water inputs (Figure 16). Most data connections lead to the Plant Control, except for a few feedback loops involving Unit Control or SCADA. The network diagram exhibits a hub-and-spoke layout, with the hub encompassing all control components.

Table 9. Number of Plants by Size and Type included in Configuration Type G

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 2 | 2 |
| **Run of River** | 0 | 11 | 25 | 36 |
| **Storage** | 0 | 0 | 2 | 2 |
| **Other** | | | 1 | 1 |
| **Total** | 0 | 11 | 29 | 40 |

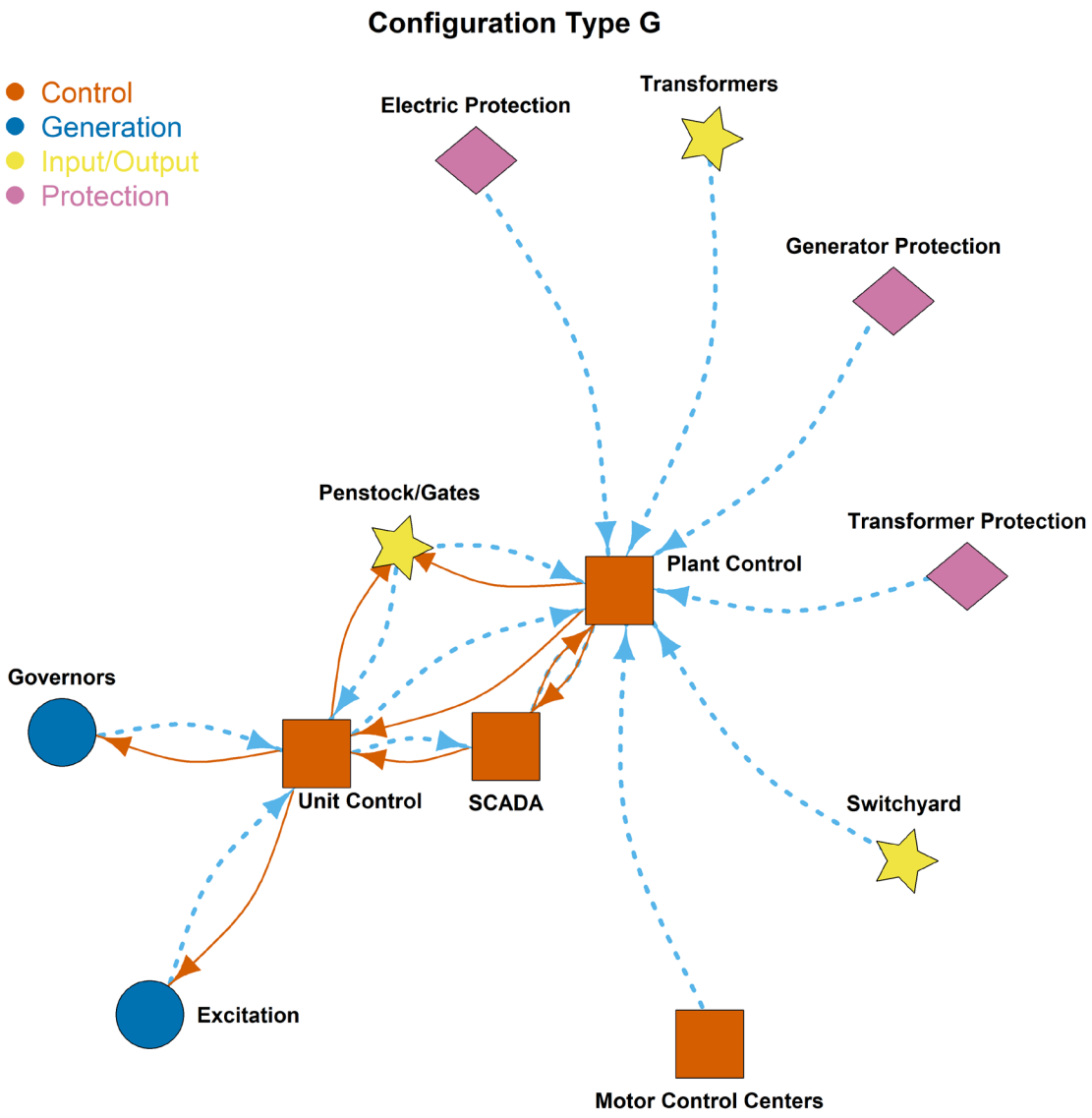


Figure 16. Network Diagram for Configuration Type G. Solid arrows are control connections, and dashed arrows are data connections.

A higher proportion of Type G plants provide grid services than the fleet (Figure 17). Generation was more often automatic and less often manual. Control was more often centralized or local relative to the fleet.


Figure 17. Prevalence of Plant Operational Characteristics for Configuration Type G

### 5.2.8 Type H

Cyber-physical configuration Type H included fifteen large plants across all classes of operation, plus one medium-sized storage and a small run-of-river plant (Table 10). Control components are curiously absent from the network diagram, with control connections most often emanating from generation components (Figure 18). This diagram suggests that generation components incorporate the ability to control other components. The network diagram exhibits a point-to-point layout with no clear hub.

Table 10. Number of Plants by Size and Type included in Configuration Type H

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 1 | 1 |
| **Run of River** | 1 | 0 | 4 | 5 |
| **Storage** | 0 | 1 | 5 | 6 |
| **Other** | 0 | 0 | 5 | 5 |
| **Total** | 1 | 1 | 15 | 17 |

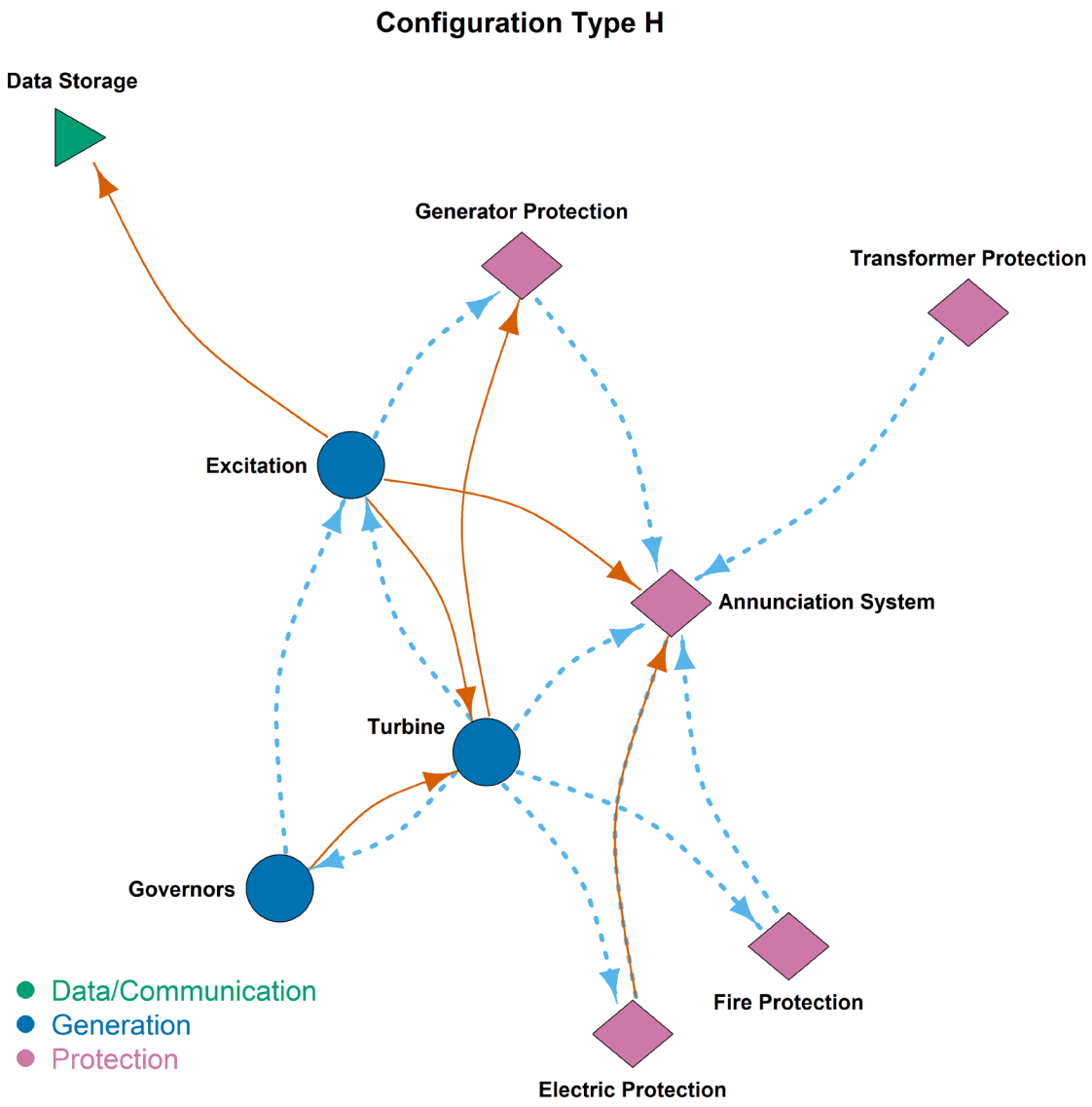


Figure 18. Network Diagram for Configuration Type H. Solid arrows are control connections, and dashed arrows are data connections.

Type H plants differ from the fleet in greater reliance on attended or unattended operation, with no plants operating as partially attended (Figure 19). Reliance on off-site control was almost non-existent, while reliance on local control was relatively high. A larger proportion of Type H plants provided frequency response and regulation or non-spinning reserves when compared to the fleet.


Figure 19. Prevalence of Plant Operational Characteristics for Configuration Type H

### 5.2.9 Type I

Cyber-physical configuration Type I included 12 large plants falling into each of the major operational classes (Table 11). Numerous control connections were often paired with a data connection in a highly connected network (Figure 20). The network diagram exhibits a point-to-point layout.

Table 11. Number of Plants by Size and Type included in Configuration Type I

| Type | <10 MW | 10<MW<30 | >30MW | Total |
|---|---|---|---|---|
| **Pumped Storage** | 0 | 0 | 2 | 2 |
| **Run of River** | 0 | 0 | 3 | 3 |
| **Storage** | 0 | 0 | 7 | 7 |
| **Total** | 0 | 0 | 12 | 12 |

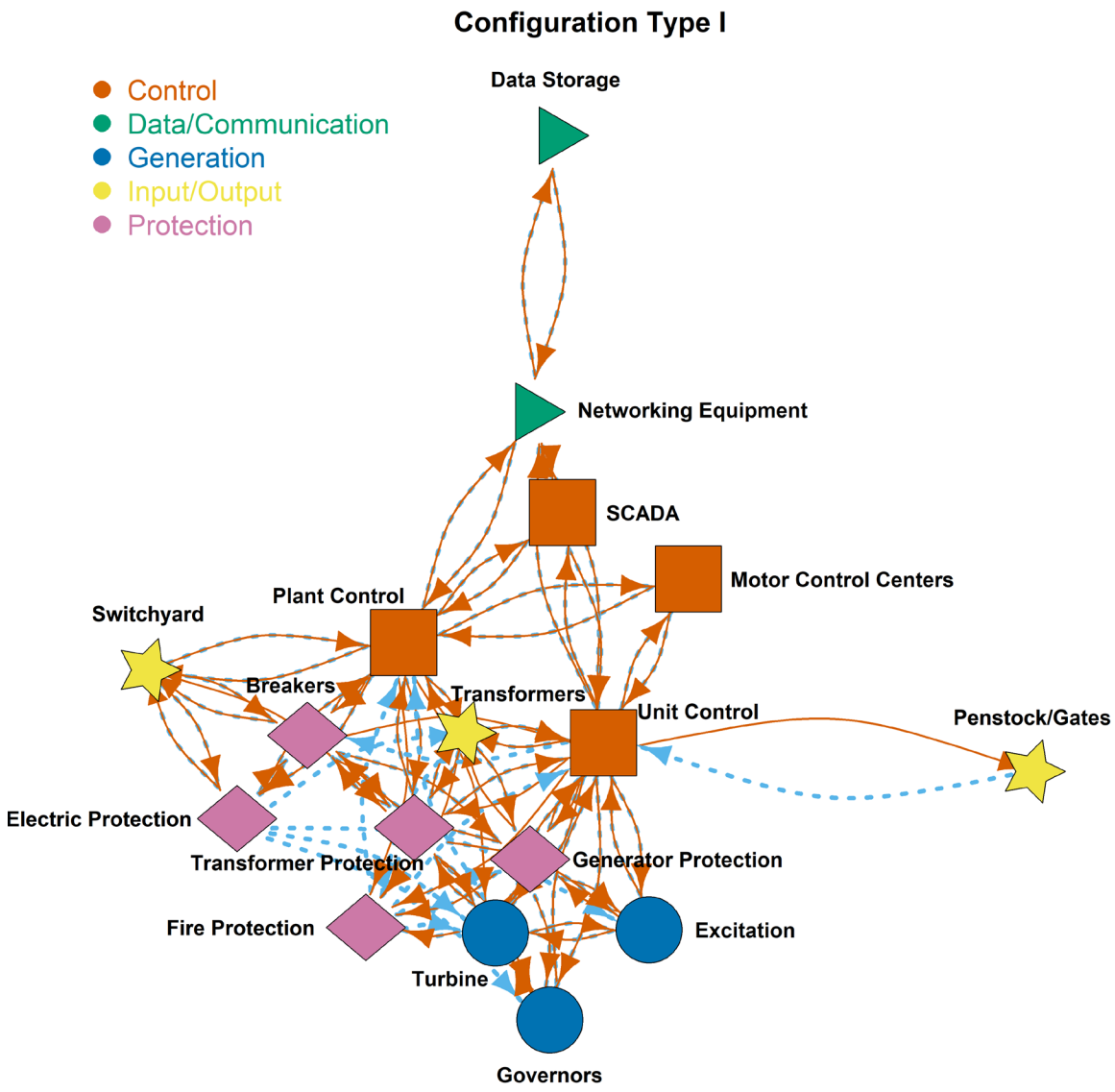


Figure 20. Network Diagram for Configuration Type I. Solid arrows are control connections, and dashed arrows are data connections.

Type I plants differ from the fleet in relying exclusively on automatic generation, with unattended operations more common than attended (Figure 21). Local control was absent, with most plants under off-site control and some under centralized control. Off-site and centralized control were less prevalent than for the fleet, which is possible because respondents can choose multiple control types for a given plant. No Type I plant provided grid services.

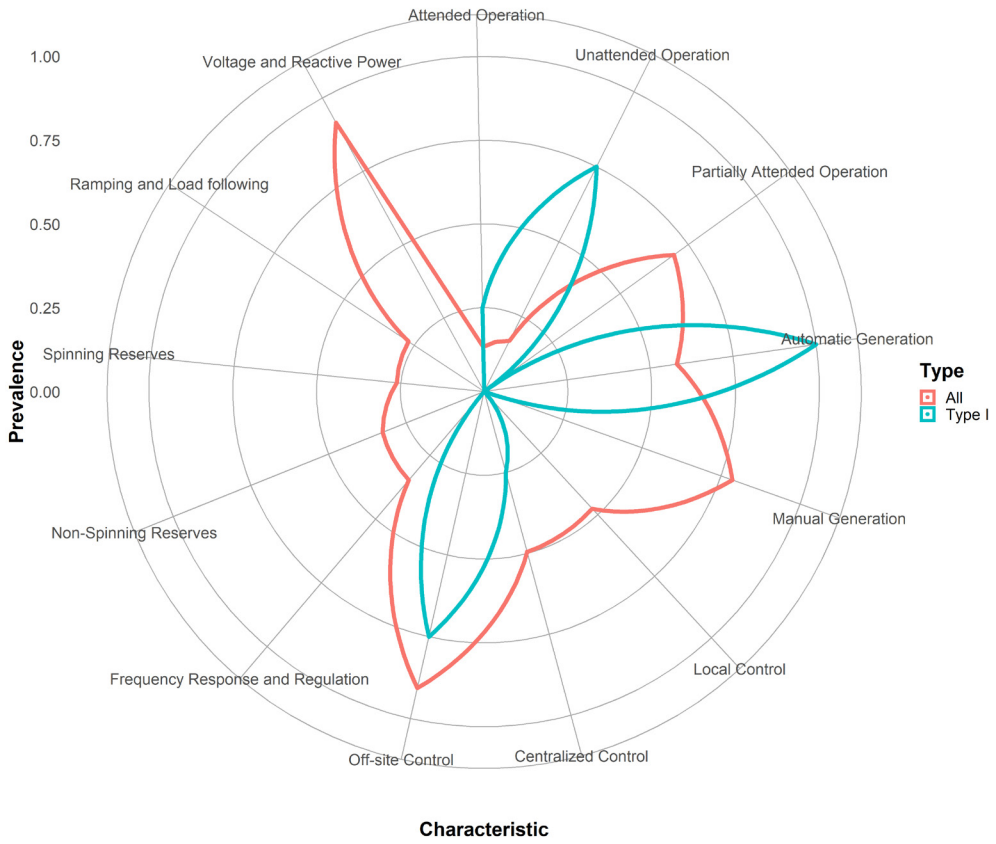


Figure 21. Prevalence of Plant Operational Characteristics for Configuration Type I

# 6.0 Common Typologies Versus Other Generation Sectors

Hydropower plants support the electrical grid in various ways, providing many of the same services as other generation sectors. However, among those varied contributions, the ability to dispatch hydropower on demand is most valued. Therefore, it makes sense to compare the configurations of hydropower plants to another generation sector that provides dispatchable power. Combined cycle natural gas (CCNG) plants often fill that role. In this section, we will examine how the operation of these two types of generation plants differ and how that might influence differences in their cyber-physical configurations.

## 6.1 Longevity

CCNG plants have an expected operating life of 25 to 30 years (Sargent and Lundy 2017). They often take on the role of "peakers," repeatedly cycling as power demand fluctuates, putting stress on the systems (Bell, Towler, and Fan 2011). As a result, refurbishment of these plants is a regularly planned activity. With refurbishment often comes modernization of the control systems. Hydropower plants have historically operated under relatively stable conditions except for pumped storage while remaining ready to follow loads up or down as needed. Under those conditions, replacing wear parts and regular maintenance has allowed hydropower plants to reach over 50 years while still going strong (Renewables First 2015). As a result, upgrades and refurbishments have been less frequent, with legacy equipment often remaining in use well beyond its design life. Hydropower licenses are another factor to consider in the cycle of refurbishment. Those licenses extend for multiple decades and impose specific requirements on the operation of the facility. Relicensing triggers negotiations that may alter a plant's scope, sometimes modifying its role within the electrical or water management system. Thus, relicensing becomes a prime opportunity to consider refurbishments or upgrades likely to provide value under a newly defined operating scope.

In recent years, hydropower plants are being called upon to respond rapidly to provide short-term balancing to fill the peaks and valleys of solar and wind energy generation (Yang et al. 2018). However, frequent ramping or starts and stops can increase wear and tear on equipment and tax older control systems, accelerating the need for refurbishment. As a result, hydropower plants are incrementally moving toward modern digital control systems, with some fully modernized and others still considering their options. As these changes occur, plant operators must increase their consideration of cybersecurity.

## 6.2 Water Management and Environmental Constraints

Hydropower facilities are as much a part of the water management system as of the electrical power system. Balancing fish needs, irrigation, recreation, water supply, or flood control often competes with water use as "fuel" for hydropower, constraining power operations. There can be constraints on the rate of change in water discharge, minimum flows, or water quality to ensure that environmental conditions are conducive to the healthy populations of fish or other biotas. Some constraints vary with ambient conditions, creating a need for information and feedback to achieve proper control and compliance. Given these requirements, we would expect hydropower cyber-physical configurations to include sensors and inputs that enable constraints to be adhered to and compliance documented.

While CCNG plants may have to consider the implications of their operation on environmental quality, there is less need for interactions with systems or actions outside the plant itself. These

plants generate electricity using technology like that of a jet engine (Langston 2013). The gas turbine burns fuel, the heat recovery system captures exhaust, and the steam turbine delivers additional electricity. Water use for generating steam does not create the same linkage to water resource management as in the hydropower plants. As a result, the control system of the CCNG plant can focus more narrowly on power considerations with fewer externalities than are needed when operating a hydropower plant.

## 6.3 Typical CCNG Network Versus Hydropower Type Diagrams

It is helpful to consider what a network diagram might include and how the different roles and constraints of CCNG would influence that network of communication among components. This project did not request questionnaires from CCNG plant operators, but descriptions of components and connections are in the published literature (Kole 2016). Diagramming a typical CCNG plant configuration enabled visual comparisons with hydropower configuration type diagrams (Figure 22).

The typical CCNG control system configuration diagram shows many data connections passing through the network and a limited number of control pathways to generation components originating from turbine control or plant control/SCADA components. Although none of the hydropower configuration types matches the network diagram for CCNG exactly, some similarities were evident. A narrow focus on the control of generation (Figure 22) appears in hydropower configuration Types C (Figure 8), E (Figure 12), and G (Figure 16). Unlike the CCNG diagram, the diagrams for those configuration types also show control connections to water management (penstocks/gates). Type F (Figure 14) most closely mirrors the CCNG configuration with control focused on generation and control components, receiving data from various component types but with no control connections to water management.

Despite playing a similar role in the electrical system, hydropower configuration types delivering an abundance of grid services often differed from the typical CCNG configuration. All plants included in Type A provide grid services (Figure 5), suggesting their operation has much in common with CCNG plants. However, the Type A network diagram (Figure 4) differs more from the typical CCNG diagram (Figure 22) than does Type F (Figure 14), in which fewer than 75% of plants provide grid services. Operational characteristics influence plant configurations, but they do not fully define them.

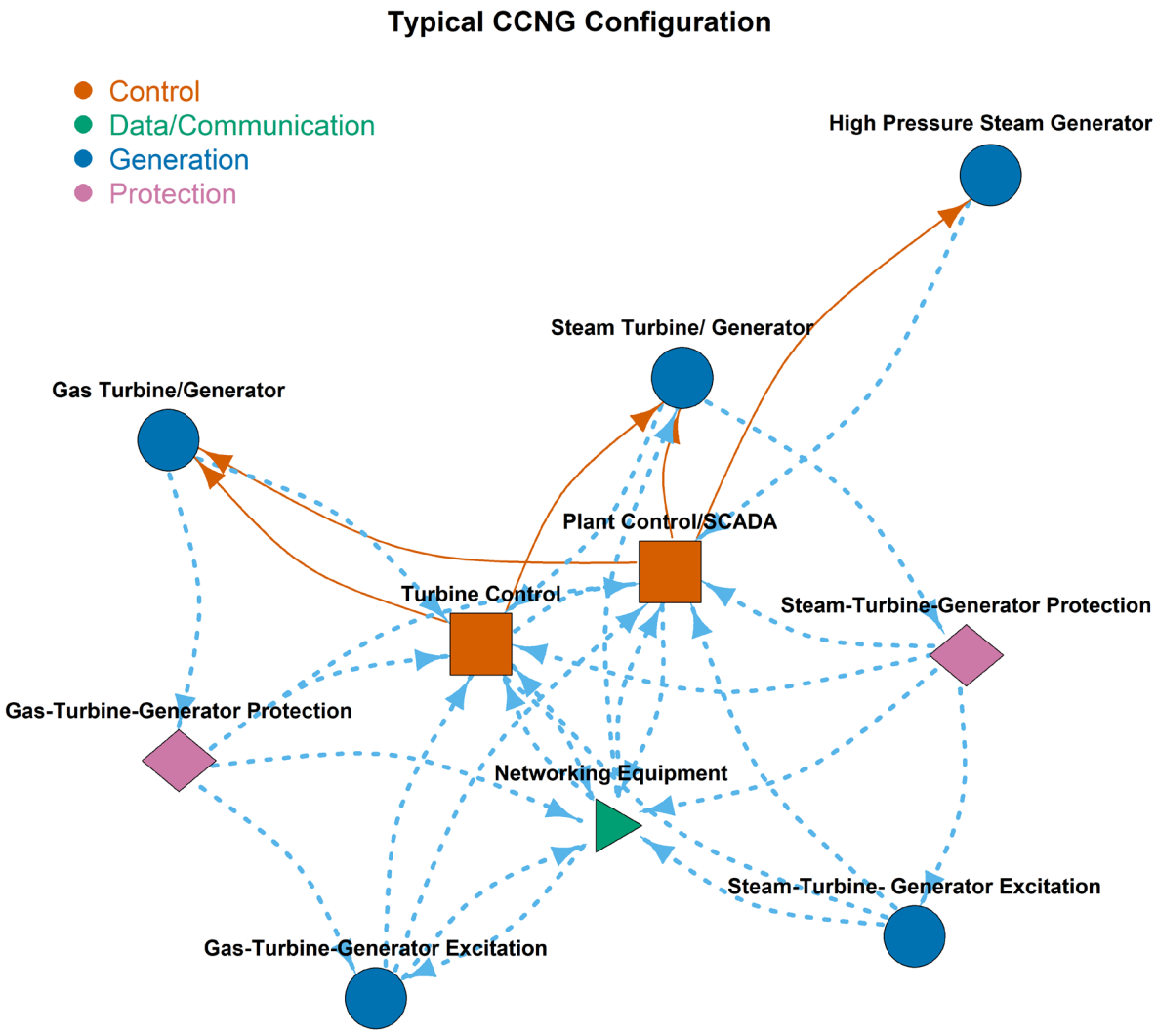


Figure 22. Network Diagram for a Typical Combined Cycle Natural Gas Power Plant. Solid arrows are control connections, and dashed arrows are data connections.

# 7.0 Self-assessment of Configuration Type

This section allows plant operators to match their plant configuration with one of the hydropower configuration types. This match creates a link to the tools and capabilities developed around the types. By identifying which configuration type most closely matches their plant, operators can access lessons learned and best practices developed for that type. Below, a dichotomous key allows an operator to identify a close match by answering yes or no to a series of questions. The key below relies on the functional classification of components defined in Table 2 of section 5.1.1 above.

## 7.1 Self-Assessment Key

Answer a few questions about data and control connections among major component groups to determine the plant configuration type most like a plant of interest (Figure 23):

Step 1: Are control signals from protection components to generation components common?
- Yes: Go to Step 2
- No: Go to Step 4

Step 2: Are data signals from generation components to protection components common?
- Yes: Go to Step 3
- No: Type I

Step 3: Are control signals from protection components to generation components present?
- Yes: Type D
- No: Type C

Step 4: Are data signals from control components to control components common?
- Yes: Go to Step 5
- No: Go to Step 8

Step 5: Are data signals from protection components to protection components common?
- Yes: Go to Step 6
- No: Go to Step 7

Step 6: Are control signals from control components to control components common?
- Yes: Type F
- No: Type B

Step 7: Are control signals from control components to generation components common?
- Yes: Type A
- No: Type G

Step 8: Are data signals from data/network components to input/output components common?
- Yes: Type E
- No: Go to Step 9

Step 9: Are data signals from generation components to control components common?
- Yes: Type F
- No: Go to Step 10

Step 10: Are data signals from control components to input/output components common?
- Yes: Type F
- No: Type H


Figure 23. Cyber-Physical Type Assessment Process Decision Tree

# 8.0 Understanding Vulnerabilities and Mitigations for Types

The cyber-physical configuration of a hydropower plant reflects the control system's nature, providing insight into potential vulnerabilities and mitigations. Classifying hydropower plants into configuration types helps overcome a perception that the site-specific nature of hydropower makes each plant unique. Nine configuration types present a manageable universe that can be better evaluated and understood than 2000 individual plant configurations.

## 8.1 Linking Configuration Type to Risks

Two primary targets of any attack on an industrial control system are the hardware/software and communications that provide these systems' foundation. An attacker must first gain access and navigate the network to exploit a device. An attack is often a multi-step process that involves more than one approach to gaining access to various portions of the system. The typology gives insight into which hardware/software components are present within each configuration type and how they communicate. A plant owner can leverage these insights with a more detailed inventory of equipment found at their facility to prioritize the risks they face.

### 8.1.1 Communication

Communication risks lie in controlling the communication between components and, most critically, controlling any external communication from your system. Cyber-attacks require initial access to cause harm. There are limited ways in which a nefarious actor can enter a hydroelectric plant. External access can include:

- A connection to an external network
- Remote services
- Hardware additions used as a vector to gain access
- Phishing to execute malicious code or to gather valid credentials
- Copying malware to removable media and installing it on a system
- A trusted relationship with access
- Valid accounts.

In an ideal world, network security will block unauthorized access to a facility's network and control systems well before they access or exploit a vulnerable piece of software or hardware. However, a continuing arms race pitting security advancements against newly discovered exploits exists in the real world. Often, these exploits are combined to circumvent network security and access equipment at some distance from an access point. The flow of data and control signals among components and the flow of information from the grid illustrated by the network diagram of each hydropower configuration type indicate whether the pathways to gain access to the target(s) of the attack are complex or straightforward and whether more than one pathway is available.

To compare connectivity among configuration types, we have provided a set of metrics that summarize various aspects of their cyber-physical networks (Table 12). A higher number of controlled components indicates more pathways for influence or control. A higher number of data sources means more information about operation may be available on the network. Both aspects are important because an attacker can alter the facility's operation by spoofing data or

issuing control messages directly. The number of feedback loops in a configuration varies with the centralization level in the control of plant operations. Feedback loops can help limit operations in unexpected ranges, but they also can be spoofed. In general, connectivity tends to follow either a hub-and-spoke or point-to-point scheme. These schemes differ in the length and variety of potential pathways from the access point to a component vulnerable to attack.

Table 12. Summary of Component Connectivity by Configuration Type

| Type | Data Sources (avg #) | Controlled components (avg #) | Feedback Loops (avg #) | Hub-and-Spoke or Point-to-Point |
|---|---|---|---|---|
| **A** | 11 | 16 | 9 | H |
| **B** | 21 | 12 | 15 | P |
| **C** | 15 | 7 | 5 | H |
| **D** | 15 | 12 | 70 | P |
| **E** | 20 | 6 | 6 | P |
| **F** | 15 | 9 | 8 | H |
| **G** | 19 | 9 | 11 | H |
| **H** | 12 | 9 | 6 | P |
| **I** | 19 | 19 | 68 | P |

Connectivity has benefits that offset its risks. The questions on the first page of the questionnaire help understand the need for communication links to receive information from the grid or internet (Table 13). Off-site control indicates a need for an internet connection to operational functions. Supplying grid services requires close coordination with the larger electric grid's needs, implying a degree of external data connectivity. Unattended or partially attended operation occurs across nearly all configuration types and suggests a certain level of automation and internal connectivity supporting limited human oversight. As the benefits of automation become more compelling, we expect facilities to move toward more connectivity. New configurations must include effective mitigations against cyber attacks.

Table 13. Drivers of Control and External Connectivity by Configuration Type

| Type | Control (Local, Centralized, Off-site) | Operation (Attended, Unattended or Partially Attended) | Grid Services |
|---|---|---|---|
| **A** | O | U | High |
| **B** | O | U | High |
| **C** | L=C=O | A<P | Medium |
| **D** | L=C<O | A=U<P | Low |
| **E** | C=O | A | High |
| **F** | L<C<O | A=U>P | Medium |
| **G** | L=C=O | U<A<P | High |
| **H** | L>C=O | A=U | Medium |
| **I** | C<O | A<U | None |

### 8.1.2 Hardware/Software

The cyber-physical typology focuses on a limited set of cyber-physical systems such as turbines, governors, etc. These systems combine the cyber-physical hardware and control software to react to an operator's or other component's commands as a coupled unit. A manufacturer or vendor tightly connects systems to enhance the hardware component's capabilities. They act as one unit providing service(s) to the plant. This tightly coupled component, including the software and hardware, is built to mitigate known system risks during design and over the component's lifecycle. Coupled components are more secure than devices not specifically designed to work together (Zhu, Joseph, and Sastry 2011).

Defining the system boundaries of these tightly coupled cyber-physical devices and their control software may be more site-specific than our polling can reveal. The communications between hardware-software combinations and others not tightly coupled by coordinated engineering pose a greater risk of being exploited, interrupting normal stable operations.

### 8.1.3 Vulnerabilities and Threats to Hydropower Facilities

Hydropower facilities face many of the same scenarios that any business or industry might face, but they must also avoid unintended operations that compromise public safety. Water management equipment, such as penstocks and gates, must operate as intended to prevent the possibility of uncontrolled releases that may damage equipment and to avoid the possibility of flooding that endangers lives and property. Avoiding dangerous water management operations must be a primary focus of protection, with ample warnings and fail-safe mechanisms to allow unintended operations to be recognized and remedied before consequences become dire. The configuration type diagrams provide a foundation for those protection activities by showing how water management equipment is connected to and controlled by other components across the plant network.

Attackers use data and control connections to gain initial access to a network, connect to components for a cyber-attack, discover network topology, exfiltrate information, escalate privileges, and impact normal system processes. Table 12 above details the number of unique data and control connections and their sources across the types. The pathways among the components indicate how distant, in a network sense, these are from an initial point used to access the network. While the intervening parts and security policies have a considerable influence on access, fewer and longer paths suggest additional work for an individual trying to gain access, assuming the network is segmented to limit unnecessary traffic. If they are blindly traversing the network, discovering the segments as they go, we can determine a generalized path an adversary might use to effect nefarious actions.

These communication pathways between components provide a highway for a cyber threat to connect to different devices on the hydroelectric plant. Malicious actors establishing persistence on a network can inspect inter-process communication to identify a hydroelectric plant's command and control framework. As such, infiltration detection is critically important. Once an attacker establishes communication pathways, malware can move across the network to discover critical components. Configuration types that contain many paths for data and control increase the risk of an adverse actor misusing these communication paths. Defining pervasive configuration types provides a window into the communication between components of the plant helps identify risks and potential mitigations.

How communication pathways are defined influences the risks they pose to cybersecurity. A one-way command connection limits adverse network communication back to the command-and-control component. A SCADA system, for example, receives specific information from any number of sources and sends control messages to a device. Limiting communication to necessary commands and tightly defined status information reduces the risk of inappropriate use of these normal system processes.

Understanding how configuration alters risk helps identify what mitigations are appropriate for plants of each configuration type.

## 8.2 Linking Configuration Type to Potential Mitigations

Brute force approaches to security such as air gapping are no longer viable as the benefits of digitalization require a secure but connected approach to instrumentation and control. The connectivity of a plant is a good starting point for planning mitigations. Eliminating external connections not identified as necessary on the configuration type diagrams limits the attack surface. Moving groups of components inside the plant requiring a high level of connectivity to a network segment can help control and restrict unnecessary communication from elsewhere.

Detailed, plant-specific information about the components can bolster the usefulness of configuration type information. An effective asset management system could help determine whether connections are necessary. This information could help recast the configuration itself, segment the network, block unneeded communication paths, and generally make an attacker's job more difficult. Asset management tools should also help to identify patches for components with known vulnerabilities, disrupting digital attack paths wherever possible.

# 9.0 Emerging Trends

The role of hydropower in the electrical grid, as well as in the larger societal context, continues to evolve. Kougias et al. (2019) describe emerging hydropower technologies that enable new levels of flexibility, reliability, safety, and environmental performance. Many of those technologies require increasing digitalization of control. As plants continue to embrace digitalization, they must secure their plants in new and potentially unfamiliar ways.

## 9.1 Adopting Digitalization

Obsolescence or a need for more effective control will force hydropower plants to update their control systems with modern digital equipment with a high degree of connectivity. The flexibility of communication among components, sensors, control systems, and external entities is necessary for effective operation in the dynamic electrical grid.

Digitalization and connectivity create a need for better management and security of the control system. Interconnected systems present more vulnerabilities that could interrupt or corrupt control. Malicious activities involving hardware and software bugs, malware, spoofing, or data modification can interrupt or alter control signals and even cause the failure of the network or components, leading to an inability to achieve control of the plant. Other activities may compromise the security of the information by collecting or retransmitting information that affords the malicious actor a business advantage.

## 9.2 The Transformation of Digitalization

A significant trend in digitalization is the rise of the “Internet of Things,” conferring increased computing power and the increased digital capabilities on remote devices. A result is a decentralized approach to networking and control, in some cases incorporating wireless communications. Increased digital capabilities allow network architects to move autonomous control to the devices themselves or remote networks. Decentralization creates both challenges and opportunities for security. Increased component capabilities allow network segmentation, which limits access to portions of the network.

Digitalization can also play a role in maintaining a secure cyber posture. System digitalization enables system administrators to replicate system architectures in virtual testbeds to evaluate patching, update management, and system improvements for mitigations on the production network. This virtual testing environment proves even more beneficial for OT systems where downtime means loss of production.

# 10.0 Conclusion

North American hydropower plant operators returned questionnaires detailing the configurations and operational characteristics of 275 plants, or approximately 12% of the fleet of hydropower assets. The sample of questionnaires contained a higher proportion of large and medium plants relative to the overall fleet, but the plants in the sample span a range of complexity that likely encompasses the configurations of most small plants. Connections among components proved to be the richest source of information for developing a set of cyber-physical types most prevalent across the hydropower fleet. Nine configuration types emerged from the analyses and were labeled A through I (Table 14). Plants within each grouping often differed in their capacities and operational schemes, but they shared similar connectivity among components.

Table 14. Overview of Component Connectivity by Configuration Type

| Type | Number | Pumped Storage | Run of River | Storage | Other | <10 MW | 10<MW<30 | >30MW | Hub-and-Spoke or Point-to-Point | Control (Local, Centralized, Offsite) | Operation (Attended, Unattended or Partially Attended) | Grid Services |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | 7 (3%) | | | 7 | | | 2 | 5 | H | O | U | High |
| **B** | 7 (3%) | | 2 | 5 | | | | 7 | P | O | U | High |
| **C** | 8 (3%) | | 2 | 6 | | | | 8 | H | L=C=O | A<P | Medium |
| **D** | 139 (56%) | 1 | 135 | 3 | | 81 | 53 | 5 | P | L=C<O | A=U<P | Low |
| **E** | 6 (2%) | | 2 | 4 | | | | 6 | P | C=O | A | High |
| **F** | 11 (4%) | 1 | 3 | 7 | | | 3 | 8 | H | L<C<O | A=U>P | Medium |
| **G** | 41 (17%) | 2 | 36 | 2 | 1 | | 11 | 30 | H | L=C=O | U<A<P | High |
| **H** | 17 (7%) | 1 | 5 | 6 | 5 | 1 | 1 | 15 | P | L>C=O | A=U | Medium |
| **I** | 12 (5%) | 2 | 3 | 7 | | | | 12 | P | C<O | A<U | None |

Type D was the most prevalent among the configurations collected for this project. A high proportion of Type D plants were small to medium capacity, operated as run-of-river, rarely provided grid services, and often operated from off-site. Type E, the least prevalent type, comprised large capacity plants, operating as storage or run-of-river, providing grid services, and had operators always present. The contrast between the diagrams of the most (Figure 10) and least (Figure 12) prevalent configurations illustrates how hydropower plants' control schemes and operational roles require tailoring cybersecurity efforts to achieve the best results.

A key finding from the grouping of plants into types was that configurations did not adhere to categories by capacity (MW) or operational mode (storage, run-of-river, pumped storage). In other words, these essential and more obvious external characteristics of a hydropower plant were not all that useful for predicting the cyber-physical configuration found inside.

CCNG plants are newer and, therefore, more modern and digitalized than the typical hydropower plant. Although the network of Type F (Figure 14) was most similar to a typical

CCNG plant (Figure 22), other types fulfilled a more similar operational niche in providing grid services such as load following. Integrating water management into the control system differentiated the network diagrams of most hydropower types from that of a typical CCNG plant.

The cyber-physical typology reinforces the idea that hydropower facilities vary widely, but it also identifies groups that highlight similarities in how their cyber-physical components interact. Fleetwide cybersecurity needs are addressed more effectively by focusing on a small number of types that share risks, vulnerabilities, and potential mitigations.

# 11.0 References


Baruch, Yehuda, and Brooks C. Holtom. 2008. “Survey response rate levels and trends in organizational research.” *Human Relations* 61 (8): 1139-1160. https://doi.org/10.1177/0018726708094863.

Bell, David A., Brian F. Towler, and Maohong Fan. 2011. “Hydrogen Production and Integrated Gasification Combined Cycle (IGCC).” In *Coal Gasification and Its Applications*, edited by David A. Bell, Brian F. Towler and Maohong Fan, 137-156. Boston: William Andrew Publishing.

IEC. 2013. *62270-2013 - IEC/IEEE Guide for Computer-based Control for Hydroelectric Power Plant Automation.* IEEE ([Place of publication not identified). https://ieeexplore.ieee.org/servlet/opac?punumber=6617649.

Johnson, Megan, Shih-Chieh Kao, Nicole Samu, and Rocio Uria-Martinez. 2020. Existing Hydropower Assets Plant Dataset FY20. ; Oak Ridge National Lab. (ORNL), Oak Ridge, TN (United States).

Kole, Alok. 2016. “A review and study on advanced control and automation functions and future control for a modern combined cycle power plant.” 2016 International Conference on Intelligent Control Power and Instrumentation (ICICPI), 21-23 Oct. 2016.

Kougias, Ioannis, George Aggidis, François Avellan, Sabri Deniz, Urban Lundin, Alberto Moro, Sebastian Muntean, Daniele Novara, Juan Ignacio Pérez-Díaz, Emanuele Quaranta, Philippe Schild, and Nicolaos Theodossiou. 2019. “Analysis of emerging technologies in the hydropower sector.” *Renewable & Sustainable Energy Reviews* 113: 109257. https://doi.org/10.1016/j.rser.2019.109257. <Go to ISI>://WOS:000483422600032.

Langston, Lee S. 2013. “The Adaptable Gas Turbine.” *American Scientist* 101 (4): 264-267. https://doi.org/Doi 10.1511/2013.103.264. <Go to ISI>://WOS:000320641000012.

NIST. 2014. Guidelines for Smart Grid Cyber Security; Technical Report NISTIR 7628. edited by The Smart Grid Interoperability Panel—Cyber Security Working Group. Gaithersburg, MD, USA: National Institute of Standards and Technology.

Renewables First. 2015. “How long do hydropower installations last?”. Hydropower Learning Centre. Renewables First. Accessed 12/23/2020. https://www.renewablesfirst.co.uk/hydropower/hydropower-learning-centre/how-long-will-hydropower-systems-last/.

Sargent and Lundy, LLC. 2017. *Combined-Cycle Plant Life Assessments.* Chicago, Illinois. https://sargentlundy.com/wp-content/uploads/2017/05/Combined-Cycle-PowerPlant-LifeAssessment.pdf.

Yang, Weijia, Per Norrlund, Linn Saarinen, Adam Witt, Brennan Smith, Jiandong Yang, and Urban Lundin. 2018. “Burden on hydropower units for short-term balancing of renewable power systems.” *Nat Commun* 9 (1): 2633. https://doi.org/10.1038/s41467-018-05060-4. https://www.ncbi.nlm.nih.gov/pubmed/29980673.

Zhu, Bonnie, Anthony Joseph, and Shankar Sastry. 2011. “A Taxonomy of Cyber Attacks on SCADA Systems.” 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 19-22 Oct. 2011.

# Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

***www.pnnl.gov***