Water Sector Cybersecurity

Risk Management Guidance for Small Systems

American Water Works Association

Dedicated to the World's Most Important Resource®

Water Sector Cybersecurity Risk Management Guidance for Small Systems

Prepared by West Yost Associates

ACKNOWLEDGEMENTS

This project was funded by the United States Department of Agriculture, Fiscal Year 2019, and managed by Todd Brewer, and Bridget Otto.

DISCLAIMER

The Getting Started Guide was supported under a grant from the United States Department of Agriculture (USDA) to AWWA to support the improvement of cybersecurity practices within small and rural water utilities across the United states.

In some cases, specific brands or products are provided as examples. These are not a recommendation or endorsement by AWWA, West Yost, or the references cited.

American Water Works Association
6666 West Quincy Avenue
Denver, CO 80235-3098
303.794.7711
www.awwa.org

Contents

INTRODUCTION

This Water Sector Cybersecurity Getting Started Guide (guide) is a supplement for small systems to the Water Sector Cybersecurity Risk Management Guidance (AWWA Guidance) and AWWA Cybersecurity Guidance and Assessment Tool (AWWA Tool). This Getting Started Guide is intended to support small rural utilities improve their cybersecurity practices. The intended users of this guide serve a population less than 10,000 people and particularly includes utilities that serve less than 3,300 people.

Internet security and data protection bkrd with padlocks cybersecurity concept/songbysummer/shutterstock.com

USING THE GETTING STARTED GUIDE

This guide was developed to adapt the AWWA Water Sector Cybersecurity Risk Management Guidance and the Tool to support small and rural water utilities. AWWA's existing resources are considered the standard best practice for water utility cybersecurity risk management, but they were designed to support compliance with America's Water Infrastructure Act of 2018 (AWIA) section 2013. AWIA is only applicable to community water systems serving more than 3,300 people. Consequently, many of the controls recommended by the Tool do not apply to the environment of many smaller utilities. This guide simplifies the output from the Tool, paring down the recommendations to the controls that are most valuable and accessible to a smaller utility.

1. Complete the online Tool
2. Prioritize the tool results with the 28 controls selected for small and rural utilities
3. Answer seven questions to identify controls to increase security
4. Obtain USDA funding

This guide will follow a four-step process, beginning with the completion of the 22 question AWWA tool, which will generate an extensive list of cybersecurity controls with priorities from 1–4. These controls use the 22 questions to exclude certain controls that will not apply and assign priorities to the ones that remain. (For a detailed explanation of this tool and its use in AWIA compliance, see the Water Sector Cybersecurity Risk Management Guidance document). Under step 2, this document includes a list of 28 controls selected for small and rural water utilities. The utility should prioritize any of the controls in their individually generated list that are represented in the 28 selected controls. Step 3 will help the utility further refine their cybersecurity practice. The utility will answer seven questions that will generate a further list of applicable controls that the utility may choose to implement. These controls will increase the maturity of the utility's system. After developing their cybersecurity improvement plan, a utility may need to seek funding for implementation.

STEP 1: COMPLETE THE ONLINE TOOL

Regardless of size, each utility should start by answering the 22 introductory questions in the AWWA Tool to generate the list of recommended cybersecurity controls. Answering these questions allows a utility to generate a list of controls specific to how they use technology. This list will be provided in a Microsoft Excel template, automatically generated by the AWWA Tool. A detailed summary of the AWWA Tool is included in the Guidance document.

STEP 2: BASELINE CYBERSECURITY CONTROLS

The AWWA tool-generated Microsoft Excel file will provide up to 100 individual cybersecurity controls. Twenty-eight of these are considered baseline controls and provide a starting point for any utility working to improve cybersecurity practices. These 28 baseline controls are where small and rural utilities should focus efforts. The relative importance of these baseline controls is based on the professional experience of water sector cybersecurity practitioners, input from subject matter experts, and the Center for Internet Security (CIS) Top 20 Controls and Resources[1].

The 14 practice areas provided in the AWWA Guidance document are reduced to six categories as listed here:

1. Training Staff to be Cybersecurity Aware
2. Knowing What Hardware and Software are Connected to and Operating on Your Networks
3. Protecting Systems from Unauthorized Access or Use
4. Maintaining Data Security Compliance
5. Physical Security
6. Good Network Design

The 28 baseline controls and supporting details are included in the following sections. These details include examples and resources to support scoping and implementation. The examples provided are not exhaustive of a single control's potential implementations. For example, a control may refer specifically to an operator's workstation in the example, but the control could be applicable to all workstations in the water utility's network. A summary of the controls in each category is provided in Appendix A. An illustration is included in Appendix B that shows visually where in a water utility each control will apply.

Depending on a utility's use of technology as characterized by answering the 22 up-front questions in the AWWA Tool, not all 28 controls may be applicable. The utility should prioritize any controls in this list of 28 that appear in their list generated by the AWWA Tool.

1 *The 20 CIS Controls & Resources. www.cisecurity.org/controls/cis-controls-list/.*

Category 1: Training Staff to be Cybersecurity Aware

Training staff to reduce the risk associated with a cyber-attack. Training should be based on staff members' roles and responsibility within the organization. In addition, training may be informed by the current situational awareness provided by intelligence and law enforcement agencies.

BASELINE CONTROL: AT-1

A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures.

- **What it means:** A utility has a cybersecurity training program that educates staff on how to identify a potential cyber-attack, who to report to, and what immediate actions to take.
- **Examples:**
  - Staff can identify a cyber threat.
  - Staff know who to notify in the event of a cyber threat/attack.
  - Staff know what immediate actions they can take to isolate their workstations from the outside world.
  - Routine staff training includes information on reporting cyber threats/attacks.
- **Resources:**
  - CIS Control 17: Implement a Security Awareness and Training Program.
  - CIS Control 19: Incident Response and Management.

BASELINE CONTROL: AT-2

Job-specific security training including incident response training for employees, contractors, and third-party users.

- **What it means:** A utility has a cybersecurity training program that educates staff on how to identify a potential cyber-attack, who to report to, and what immediate actions to take.
- **Examples:**
  - Written response procedures that define roles and responsibilities for incident response.
  - A cybersecurity training and awareness program is in place.
  - Based on the training, staff know how to recognize to, and respond to, different types of attacks (e.g. phishing).
  - Staff know how to report a suspected cyber incident.
- **Resources:**
  - CIS Control 17: Implement a Security Awareness and Training Program.
  - CIS Control 19: Incident Response and Management.

BASELINE CONTROL: MA-2

Maintenance of relationships with authorities, professional associations, interest groups, etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.

- **What it means:** The utility works closely with authorities, professional associations, interest groups, etc., so that it is aware of any developments that might affect their security.
- **Examples:**
  - Develop and maintain formal relationship with local emergency response personnel, regulators, Internet service providers, and other organizations (e.g., local FBI contact, InfraGard, DHS, CISA, etc.).
  - Develop and maintain a response plan that includes coordination with external organizations.
  - Develop and maintain relationships with external organizations to stay up to date on relevant threats.
  - Shares threat and incident information with external organizations in accordance with applicable requirements and restrictions.
  - Maintain current contact information for external organizations.
- **Resources:**
  - CIS Control 3: Continuous Vulnerability Management.
  - CIS Control 18: Application Software Security.
  - CIS Control 19: Incident Response and Management.

Category 2: Know What Hardware and Software are Connected to and Operating on Your Networks

Knowing what hardware and software are present on a network is important for maintenance and security. Managing hardware and software assets helps establish a baseline for network performance that could indicate a cyberattack. In addition, conducting regular updates of hardware and software are critical for managing vulnerabilities.

BASELINE CONTROL: CM-7

Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.

- **What it means:** The utility has implemented the software/hardware to continuously monitor network traffic and server performance.
- **Examples:**
  - Continuous monitoring the performance of the network/servers via an automated hardware/software solution.
  - Establish network baselines against which to compare continuously generated data.
  - Establish performance thresholds for the network/servers.
  - Automatic alerts are issued when the network/server performance drifts below the established thresholds.
- **Resources:**
  - CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs.

BASELINE CONTROL: PM-1

Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.

- **What it means:** The utility keeps a detailed record of all its electronic devices.
- **Examples:**
  - The utility maintains an up-to-date list of all its electronic devices and components.
  - The list includes model numbers, software/firmware versions, and any other information required to assess future vulnerabilities.
  - The utility references the list to assess vulnerabilities when they are disclosed by vendors.
  - The utility knows how to recover assets if data is corrupted.
- **Resources:**
  - CIS Control 1: Inventory and Control of Hardware Assets.
  - CIS Control 2: Inventory and Control of Software Assets.
  - CIS Control 10: Data Recover Capability.

BASELINE CONTROL: PM-4

Service Level Agreements (SLAs) for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.

- **What it means:** The utility has implemented service level agreements with all internal/external parties (contractors, service providers, vendors, etc.) who exchange software or information with the utility.
- **Examples:**
  - The utility has an SLA for each internal/external party (contractors, service providers, vendors, etc.) that exchanges software or information with the utility.
  - The utility's SLAs include defining the approved interfaces between the two parties' systems.
  - The utility's SLAs include policies and procedures for interaction between the two parties. For example, what are they approved to do?, when?, who needs to approve the actions?, etc.
- **Resources:**
  - CIS Control 14: Controlled Access Based on the Need to Know.

Privacy-information-link -Cybersecurity concept protection of private data emails/songsaboutsummer/shutterstock.com

BASELINE CONTROL: SA-1

Authorization process established for new systems or changes to existing information processing systems.

- **What it means:** A utility manages the security of information systems through an organizational risk management process.
- **Examples:**
  - Risk management process (including policies and procedures) are in place.
  - Roles and responsibilities related to risk management are properly defined and assigned.
- **Resources:**
  - CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches.
  - CIS Benchmarks for hardening.

Category 3: Maintain Data Security Compliance

Many utilities store and transmit, or contract out the storage and transmittal of protected data. These include payment card industry (PCI) data, personally identifiable information (PII), and personal health information protected under the Health Insurance Portability and Accountability Act (HIPAA). Individual states have laws establishing the requirements for protection of PII while broader standards are established for PCI and HIPAA data.

BASELINE CONTROL: DS-1

A program established to ensure compliance with the minimum PCI requirements for your associated level.

- **What it means:** The utility complies with the applicable PCI requirements and has a plan to make sure that they protect cardholder data.
- **Examples:**
  - Has the utility assessed its security needs against the PCI requirements?
  - Does the utility request current ROC (Record of Certification) from third party payment processors?
  - Does the utility maintain strong network security and access control according to PCI requirements?
  - Does the utility maintain a vulnerability management program in compliance with PCI requirements?
- **Resources:**
  - CIS Control 13: Data Protection.

BASELINE CONTROL: DS-2

A Privacy Policy as well as a Cyber Security Breach Policy are implemented.

- **What it means:** The utility has established a Privacy Policy to protect data (e.g. personally identifiable information) that the utility collects or generates. It also has a Cyber Security Breach Policy that defines the utility's required response in the event of a cyber breach.
- **Examples:**
  - Does the utility have a Privacy Policy that complies with any applicable standards?
  - Does the utility have a Cyber Security Breach Policy that complies with any applicable standards?
- **Resources:**
  - CIS Control 13: Data Protection.
  - CIS Control 19: Incident Response and Management.

BASELINE CONTROL: DS-3

A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.

- **What it means:** The utility has a plan for meeting the minimum HIPAA requirements. It has also developed a Privacy Policy to protect personally identifiable data and a Cyber Security Breach Policy that defines the utility's required response in the event of a cyber breach.
- **Examples:**
  - Does the utility have a plan to meet minimum HIPAA requirements?
  - Does the utility have a Privacy Policy that complies with any applicable standards?
  - Does the utility have a Cyber Security Breach Policy that complies with any applicable standards?
- **Resources:**
  - CIS Control 13: Data Protection .
  - CIS Control 19: Incident Response and Management.

Internet security and data protection bkrd with padlocks cybersecurity concept/songbysummer/shutterstock.com

Category 4: Protect Systems from Unauthorized Access or Use

Protection from unauthorized access to and use of systems and data protect the utility from consequences associated with misuse of the data and systems. As a background reference, AWWA prepared the document Cybersecurity Risk & Responsibility in the Water Sector.[2] This provides a summary of the importance of sound cybersecurity practices and risk management.

BASELINE CONTROL: IA-4

Access control for confidential system documentation established to prevent unauthorized access of trade secrets program source code, documentation, and passwords (including approved policies and procedures).

- **What it means:** The utility protects its sensitive system documentation and data via well-documented access control policies and procedures.
- **Examples:**
  - The utility has a well-documented access control policies and procedures for protecting its documentation (e.g. PLC programs, administrative account inventories).
  - The utility requires special account privileges to access sensitive documentation.
  - The utility uses dedicated administrative accounts. These accounts are not used for such things as internet browsing or email.
  - The utility has a well-rounded access control framework, including password policies, authorization, role-based access control, etc.
  - The utility disables any account that cannot be associated with a practice or owner.
  - The utility retires accounts after a period of inactivity.
- **Resources:**
  - CIS Control 4: Controlled Use of Administrative Privileges.
  - CIS Control 13: Data Protection.
  - CIS Control 16: Account Monitoring and Control.

BASELINE CONTROL: IA-6

Access control for networks shared with other parties in accordance with contracts, SLAs, and internal policies.

- **What it means:** SLAs specify security requirements for a vendor to connect to the control network (secure corporate VPN client, HTTPS, etc.).
- **Examples:**
  - Access control lists are maintained so that only authorized individuals can access restricted information.
- **Resources:**
  - CIS Control 14: Controlled Access Based on the Need to Know.

BASELINE CONTROL: IA-7

Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.

- **What it means:** The utility has a formal plan for ensuring the security of the wireless network that includes a guest access plan.
- **Examples:**
  - The utility has a wireless network separate from the SCADA network.
  - The utility has a separate guest wireless network.
  - The activity of wireless users/guests is monitored and audited by the utility.
  - The utility actively manages and reviews the configuration of the network and user/guest access policies.
- **Resources:**
  - CIS Control 15: Wireless Access Control.

2 *AWWA Cybersecurity Risk and Responsibility in the Water Sector; www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013*

BASELINE CONTROL: IA-9

Multifactor authentication system established for critical areas.

- **What it means:** The utility requires multifactor authentication for employees to access systems from critical areas (i.e. remote access).
- **Examples:**
  - The utility physically secures critical areas.
  - The utility requires users to present two types of authentication, such as an RFID keychain and password or a key and thumbprint.
- **Resources:**
  - CIS Control 4: Controlled Use of Administrative Privileges.
  - CIS Control 14: Controlled Access Based on the Need to Know.

BASELINE CONTROL: IA-12

Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.

- **What it means:** The utility's workstations all have session controls based on security policies.
- **Examples:**
  - Workstations automatically disconnect from network after being idle for a set period of time.
  - The utility automatically locks workstation sessions after a standard period of inactivity.
  - The workstations filter and block content from malicious or other undesirable sources.
- **Resources:**
  - CIS Control 7: Email and Web Browser Protections.
  - CIS Control 14: Controlled Access Based on the Need to Know.

Privacy-information-link -Cybersecurity concept protection of private data emails/songaboutsummer/shutterstock

BASELINE CONTROL: RA-2

Third party agreement process to ensure that external vendors and contractors use appropriate security measures for access, processing, communicating, or managing the organization's information or facilities.

- **What it means:** The utility requires third-party providers to agree with their security standards before allowing them access to the facility or giving them any sensitive information.
- **Examples:**
  - Does the utility enforce security standards on third-party service providers?
  - Are service providers restricted from access to any sensitive information or facilities until they have agreed with the utility's security policies?
- **Resources:**
  - CIS Control 14: Controlled Access Based on the Need to Know.

Category 5: Physical Security

Physically securing network components and data is important to limit the potential for unauthorized access and damage from such hazards as natural hazards, structure fires, and electrical outages.

BASELINE CONTROL: PE-1

Security perimeters, card-controlled gates, manned booths, and procedures for entry control.

- **What it means:** A utility enforces physical access control measures to any areas where the control system resides.
- **Examples:**
  - Individual's access is verified prior to entry to the facility.
  - Keys, cards, and/or combinations are used.
  - Physical access devices are audited/inventoried on periodic basis.
  - SCADA workstations are located in secure areas (i.e., locked control room).
- **Resources:**
  - AWWA Standard G430-14.
  - NIST 800-53 Revision 4 - Control PE-3.

BASELINE CONTROL: PE-4

Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.

- **What it means:** As part of a contingency plan, a utility has appropriate measures in place to continue operations in as timely a manner as possible.
- **Example:**
  - Appropriate fire suppression system in place (e.g., FM200 for server rooms).
  - Facility flood protection measures.
  - Fencing and hardened doors and windows.
- **Resources:**
  - NIST 800-53 Revision 4 Control CP-2

BASELINE CONTROL: PE-7

Physical security and procedures against equipment environmental threats and hazards or unauthorized access.

- **What it means:** A utility has an alternate processing site in place that can be used for production should the primary site be rendered unusable due to environmental hazards.
- **Examples:**
  - Appropriate fire suppression system in place (e.g., FM200 for server rooms).
  - Procedures to implement flood protection measures.
  - Policies and procedures on when and how to secure physical security components (e.g., fencing and doors).
- **Resources:**
  - AWWA Standard G430-14 .
  - NIST 800-53 Revision 4 Controll CP-7.

BASELINE CONTROL: PE-8

Physical/logical protection against power failure of equipment (UPS).

- **What it means:** A utility has a contingency plan in place in case of loss of primary means of power.
- **Examples:**
  - Uninterruptible Power Supply (UPS), generators for critical communications equipment.
  - Alternate telecommunications service in place in case of failure of primary means of communications.
  - Minimize single points of failure.
- **Resources:**
  - NIST 800-53 Revision 4 Control CP-8.

BASELINE CONTROL: PE-9

Physical/logical protection against access to power and telecommunications cabling established.

- **What it means:** A utility routes critical power and communications cabling in redundant paths.
- **Examples:**
  - Redundant paths for power and telecommunications cabling.
  - Wiring terminations located in a locked wiring closet, pedestal, manholes, etc.
- **Resources:**
  - NIST 900-53 Revision 4 Control PE-9.

Category 6: Good Network Design

Implementing a proper network design using best practices helps mitigate the potential for an attack and the consequences of an attack.

BASELINE CONTROL: SC-15

Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.

- **What it means:** The utility's industrial control network has minimal access points to any other part of the organization or external network.
- **Examples:**
  - Does the utility minimize connections between the ICS and other networks?
  - Are all connections to the ICS protected by a stateful firewall filtering on TCP and UDP, as well as a DMZ?
  - Does network design follow the NIST 800-82 guidelines?
- **Resources:**
  - CIS Control 12: Boundary Defense.
  - NIST 800-82 Revision 2.

BASELINE CONTROL: SC-16

Defense-in-depth. Multiple layers of security with overlapping functionality.

- **What it means:** A utility employs overlapping physical and cybersecurity measures to protect assets.
- **Examples:**
  - Server room is protected by means of doors under lock and key, access control authentication, unique login requirements, two-factor authentication, antivirus, firewalls, etc.
  - The following are implemented:.
    - Host-based firewalls.
    - Anti-virus applications (e.g. Symantec, Trend Micro, Windows Defender).
    - Anti-malware applications.
    - Intrusion detection applications.
    - Network traffic access controls.
- **Resources:**
  - CIS Control 8: Malware Defenses .
  - CIS Control 9: Limitation and Control of Network Ports, Protocols and Services.
  - CIS Control 12: Boundary Defense.

BASELINE CONTROL: SC-18

Minimize wireless network coverage.

- **What it means:** A utility performs a wireless survey to determine antenna location and strength to minimize broadcast range of the wireless network.
- **Examples:**
  - If it is determined that the wireless network is broadcasting too far outside the boundaries of the utility, radio transmit strength shall be reduced.
- **Resources:**
  - CIS Control 15: Wireless Access Control.

BASELINE CONTROL: SC-20

Wireless equipment located on isolated network with minimal or single connection to control network.

- **What it means:** Wireless network is on a separate network from the ICS network, with minimal (single if possible) connections to the hardwired ICS network. Any connections between wireless network and ICS network are documented.
- **Examples:**
  - The utility maintains a separate wireless network for personal or untrusted devices.
- **Resources:**
  - CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
  - CIS Control 15: Wireless Access Control

BASELINE CONTROL: SC-21

Unique wireless network identifier (SSID) for control network.

- **What it means:** The wireless network identifier (SSID) is unique for the corporate network compared to the SCADA network.
- **Examples:**
  - Implement a guest network for guests to connect personal devices.
  - Implement a wireless network for staff to connect personal devices.
  - The utility SCADA wireless network is separate from the corporate wireless network.
- **Resources:**
  - CIS Control 15: Wireless Access Control.

BASELINE CONTROL: SC-23

Wireless communications links encrypted.

- **What it means:** Wireless data-in-transit encrypted using current wireless communications best practices.
- **Examples:**
  - SCADA data transferred via radio or cellular service is encrypted when in transit.
  - Use of standard encryption like the Advanced Encryption Standard (AES).
- **Resources:**
  - CIS Control 12: Boundary Defense

BASELINE CONTROL: SC-24

Communications links encrypted.

- **What it means:** Hardwired data-in-transit encrypted using current wired communications best practices.
- **Example:**
  - Data transferred via hard-line communications links (fiber, leased circuits) between the control room and remote sites encrypted when in transit.
- **Resources:**
  - CIS Control 12: Boundary Defense.

Blue water main on asphalt_StacieStauffSmith_shutterstock_2462608099

STEP 3 — ANSWER SEVEN SMALL SYSTEMS SCREENING QUESTIONS

A set of additional screening questions was developed to provide a small and rural utility the opportunity to scale up the consideration and implementation of cybersecurity controls. These questions reflect the scale of many small and rural utilities. Incorporating additional controls based on these questions will provide a logical and stepwise process for utilities to continue to mature their cybersecurity practices. The seven questions are:

1. Does your SCADA system monitor or control two or fewer sites and have only one workstation/server?
2. Is your SCADA system used by only one person?
3. If your SCADA system was completely disabled, could you continue to operate your water system indefinitely and have you operated that way recently?
4. Does your organization have any type of documented policies and procedures for staff?
5. Does your SCADA system use only "cloud" technology (i.e., access via phone with no servers onsite)?
6. Does your organization have less than five staff members?
7. Does your organization have internal IT staff with cybersecurity experience that supports your SCADA system?

Additional details on the controls listed below can be found in the AWWA Guidance and AWWA Tool output, and a summary is provided in Appendix C.

Question 1

Does your SCADA system monitor or control two or fewer sites and have only one workstation/server?

- **Yes – The following 3 controls may be marked "Not Applicable"**
- **No – The following 3 controls may be marked "Applicable"**

CONTROLS		ADDITIONAL DETAILS
IA-5	Access control for diagnostic tools and resources and configuration ports.	PLC programming software is only available at select workstations and only accessible to SCADA technicians.
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high-risk locations.	The controls to critical equipment are only available at a local secured terminal.
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Within the SCADA system network, vendor systems are on a separate subnet.

Question 2

Is your SCADA system used by only one person?

- **Yes – The following 14 controls may be marked "Not Applicable"**
- **No – The following 14 controls may be marked "Applicable"**

CONTROLS		ADDITIONAL DETAILS
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies.
AU-3	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	Data security policy and controls are in place to prevent sharing of private or sensitive data outside of the organization.
AU-4	Information security responsibilities defined and assigned.	All staff know who they should report to if they notice suspicious behavior in the system.
CM-3	Separation of duties implemented for user processes including risk of abuse.	Operators are only given clearance to areas they are expected to work in. Supervisors have the ability and training to monitor SCADA tech activities in the PCS.
CM-4	Separation of duties implemented for development, production, and testing work.	A SCADA technician must have a second technician review changes made to production equipment before they are implemented.
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Based on their knowledge of access control policies, operators do not share passwords.
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.	Upon staff termination or resignation, login credentials are disabled as part of the Human Resources process.
IA-3	Role-based access control system established including policies and procedures.	SCADA software implements unique usernames and passwords with different levels of control based on roles.
IA-5	Access control for diagnostic tools and resources and configuration ports.	PLC programming software is only available at select workstations and only accessible to SCADA technicians.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Idle sessions on SCADA screens are logged off in 15 minutes. If no user is logged in, a read-only view is presented.
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	A third-party system integrator would need to contact IT before connecting to the system's network.
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Operators have one username and password for PCS equipment, which is managed from a central system.
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	A wireless LAN specific domain controller is in place.

Question 3

If your SCADA system was completely disabled, could you continue to operate your water system indefinitely and have you operated that way recently?

- **Yes – The following 9 controls may be marked "Not Applicable"**
- **No – The following 9 controls may be marked "Applicable"**

CONTROLS		ADDITIONAL DETAILS
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	The PCS has a testing/development environment to allow changes to be implemented without immediate effects to the production environment.
CM-5	SLAs for all third parties established, including levels of service and change controls.	A security policy that outlines that access permissions are distributed to third party employees.
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Inviting all affected parties to discussions to prevent the development of vulnerabilities in the facility.
IR-1	Incident response program established with a formal Emergency Response Plan to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events. Exercises conducted to test and revise plans and build organizational response capabilities.	Emergency Response Plan includes procedures for recovering SCADA system operation from system backup.
IR-2	A security program established with a formal Emergency Response Plan to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.	A SCADA tech believes a machine is infected and responds according to the utility's emergency response plan for cybersecurity-based incidents.
IR-3	A legal/contractual/regulatory framework established with a formal Emergency Response Plan to track legal/contractual/regulatory requirements and the efforts to meet them with respect to each important system within the organization. Another purpose of the framework is to ensure compliance of policies and procedures with privacy laws, handling cryptographic products, intellectual property rights, and data retention requirements.	The Emergency Response Plan is reviewed and updated once a year by responsible staff.
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	System backups are tested on a regular basis by completing a system restoration to the test environment.
SC-4	Intrusion detection, prevention, and recovery systems including approved policies and procedures established to protect against cyberattacks. System includes repository of fault logging, analysis, and appropriate actions taken.	Within the SCADA system network, vendor systems are placed on a separate subnet.
SC-5	Anomaly based IDS/IPS established including policies and procedures.	The IT tech monitors IDS system exception logs daily to determine if ongoing attacks are occurring and works with SCADA tech to address any issues.

Question 4

Does your organization have any type of documented policies and procedures for staff?

- **Yes – The following 25 controls may be marked "Applicable"**
- **No – Pause and return to the tool after fundamental policies and procedures are developed**

CONTROLS		ADDITIONAL DETAILS
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	The business continuity plan is revised annually. Revisions are informed by planned exercises, actual events, or documented changes.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Reviews of the organization's confidentiality/non-disclosure agreements are periodically scheduled by a responsible party.
CM-1	Policies for defining business requirements including data validation and message authenticity established to ensure that new/upgraded systems contain appropriate security requirements and controls.	Meetings are periodically scheduled between management and IT to discuss current and potential cybersecurity risks and the impact on business decisions.
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.	The Emergency Response Plan is stored in a central repository and clearly displays the version and date of when it was implemented.
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	An operator misplaces a managed phone. Based on the missing equipment policy, they contact IT to report the device lost.
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	The Emergency Response Plan is stored in a central repository that records when files are accessed and altered.
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Company policies and procedures are available in a central, secure, shared location.
PE-5	Physical security and procedures for working in secure areas.	Documentation for physical security procedures is included with new employee training and reviewed at regular training events.
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from PCS enterprise system areas.	Server room and PLC cabinets are isolated from areas that delivery personnel and customers may visit.
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	PLCs that cannot update past a specific security revision are not acceptable for use in the PCS.
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.	A utility has a network intrusion detection system (NIDS) to monitor network traffic.
PS-1	Policies and procedures for hiring/terminating processes on employees, contractors, or support companies to include background checks and contract agreements approved and implemented.	A background check on employees is required before they may be given access to the PCS system.

Table continued . . .

Question 4 (continued)

Does your organization have any type of documented policies and procedures for staff?

- **Yes – The following 25 controls may be marked "Applicable"**
- **No – Pause and return to the tool after fundamental policies and procedures are developed**

CONTROLS		ADDITIONAL DETAILS
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third-party users.	A company policy is in place limiting the access of third-party users to assets, systems, and data.
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.	Confidential documents are stored in locked file cabinets when not in use, as required by policy.
PS-4	Disciplinary process for security violations established.	An operator who props open doors to critical areas could face disciplinary action as outlined in the utility's policies and procedures.
SA-2	Change controls of systems development, outsourced development, system modification, and testing established, including acceptance criteria for new systems, monitoring of internal/outsourced development, and control of system upgrades.	A third-party system integrator is preparing to make changes to SCADA software. The SCADA tech requires the integrator to follow the change procedure and test the changes in a sandbox environment before they are deployed in production.
SA-3	Change controls of operating systems, network configuration/ topology, network security established, including changes to IDS/ IPS, traffic control/monitoring, new systems, and system upgrades.	Automatic updates to the operating system are disabled, but monthly manual updates are reviewed and applied in coordination with operations.
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.	Remote access is restricted to only the most necessary applications and only allowed through secure measures.
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communication.
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.	All external communication with the PCS is implemented via DMZ.
SC-7	Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures.	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communications.
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.	Within the SCADA system network, vendor systems are placed on a separate subnet rather than being on a single "flat" network.
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).	A water utility chooses to not allow personal mobile devices to connect to the control network. The utility does provide mobile devices managed by IT that can connect to the network.
SC-12	Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.	Remote access to the SCADA system requires two factor authentications.

Question 5

Does your SCADA system use only cloud technology (i.e., access via phone with no servers onsite)?

- **Yes – The following 8 controls may be marked "Not Applicable"**
- **No – The following 8 controls may be marked "Applicable"**

CONTROLS		ADDITIONAL DETAILS
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	A SCADA tech believes a machine is infected. Based on their training, they remove the machine from the network and report it to Information Technology Team (IT) without powering it off to avoid deleting evidence.
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Based on the company's controlled maintenance program, a utility will format network devices to factory settings before sending them out of the organization for maintenance.
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	The condition of offsite equipment and risk factors acting on the equipment are periodically reviewed and assessed via an independent party.
MP-1	Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).	When decommissioning a network device that was used in the production environment, IT is required to return it to factory conditions before it leaves the facility.
SC-10	Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).	Ports are disabled for all network devices when not in use.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Organization has a FAT procedure that requires vendors to demonstrate security of systems before they are purchased.
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	"Whitelisting" of network components is done to manage data transfer between and within network segments.
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and non-repudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.	The company selected to perform billing is compliant with pertinent laws, regulations, policies and procedures that are relevant to the utility.

Question 6

Does your organization have less than five staff members?

- **Yes – The following 13 controls may be marked "Not Applicable"**
- **No – The following 13 controls may be marked "Applicable"**

CONTROLS		ADDITIONAL DETAILS
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
AU-3	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	Data security policy and controls are in place to prevent sharing of private or sensitive data outside of the organization.
AU-4	Information security responsibilities defined and assigned.	All staff are aware of who they would report to if they notice suspicious behavior in the system.
AU-5	Risk-based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of policies and plans throughout the organization. Another purpose of the framework is to ensure consistency across plans in terms of priorities, contact data, testing, and maintenance.	The facility has a documented and tested contingency plan to operate the facility without the use of SCADA software, in the case of attack by ransomware.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Reviews of the organization's confidentiality/non-disclosure agreements are periodically scheduled by a responsible party.
CIE-1	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threats throughout the engineering life cycle including: design, implementation, maintenance, and decommissioning.	Engineering staff is fully aware of the potential for a cyber breach. They design electrical and mechanical systems to provide functionality in the case of a SCADA system compromise.
CM-3	Separation of duties implemented for user processes including risk of abuse.	Operators are only given clearance to areas they are expected to work in. Supervisors have the ability and training to monitor SCADA tech activities in the PCS.
CM-4	Separation of duties implemented for development, production, and testing work.	A SCADA technician must have a second technician review changes made to production equipment before they are implemented.
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Access to the server room is restricted to authorized staff only.
PE-3	Physical security and procedures for offices, rooms, and facilities.	Staff lock doors that allow access to PCS assets. Security guards inspect doors to make sure they are locked properly.
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies the integrator of the secure file transfer system in place.
SU-1	A supply chain risk management program.	Chain of custody documentation is required for all chemicals used in treatment.
SU-2	A supply chain risk management program that includes cybersecurity.	Preferred vendors for computer hardware, software and peripherals are identified and selected based on evaluation of their supply chain among other criteria.

Question 7

Does your organization have internal IT staff with cybersecurity experience that supports your SCADA system?

- **Yes – The following 20 controls may be marked "Applicable"**
- **No – The following 20 controls may be marked "Not Applicable"**

CONTROLS		ADDITIONAL DETAILS
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	A SCADA tech believes a machine is infected. Based on their training, they remove the machine from the network and report it to Information Technology Team (IT) without powering it off to avoid deleting evidence.
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies.
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Based on their knowledge of access control policies, operators do not share passwords.
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.	Upon staff termination or resignation, login credentials are disabled as part of the Human Resources process.
IA-3	Role-based access control system established including policies and procedures.	SCADA software implements unique usernames and passwords with different levels of control based on roles.
IA-5	Access control for diagnostic tools and resources and configuration ports.	PLC programming software is only available at select workstations and only accessible to SCADA technicians.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Idle sessions on SCADA screens are logged off in 15 minutes. If no user is logged in, a read-only view is presented.
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high-risk locations.	The controls to critical equipment are only available at a local secured terminal.
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	A third-party system integrator would need to contact IT before connecting to the system's network.
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Operators have one username and password for PCS equipment which is managed from a central system.
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.	All external communication with the PCS is implemented via DMZ.

Table continued . . .

Question 7 (continued)

Does your organization have internal IT staff with cybersecurity experience that supports your SCADA system?

- **Yes – The following 20 controls may be marked "Applicable"**
- **No – The following 20 controls may be marked "Not Applicable"**

CONTROLS		ADDITIONAL DETAILS
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
SC-9	Process isolation established to provide a manual override "air gap" between highly sensitive systems and regular environments.	A utility will physically separate a pump station from any sort of information transfer from any other network. This, however, is only a true air gap when there is absolutely no information transfer. If information is transferred though a DMZ or firewall that would not be an example of this control. In that scenario select this control as "Not Planned and/or Not Implemented – Risk Accepted".
SC-19	802.1X user authentication on wireless networks.	No "open" WiFi connections are allowed.
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	A wireless LAN specific domain controller is in place.
SC-25	VPN using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	An operator who can access the system remotely must do so through a secured VPN client configuration.
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and nonrepudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.	The company selected to perform billing is compliant with pertinent laws, regulations, policies, and procedures that are relevant to the utility.
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.	Acquired assets are inspected, assessed, and documented before implementation with existing systems.
SI-3	Interactive system for managing password implemented to ensure password strength.	When configuring a new user's password, it must meet minimum character length requirements.
SI-5	Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as enterprise system audit tools that can modify or delete audit data.	Utility has implemented tiered access so non-administrator users are unable to make changes to system security settings.

STEP 4 — OBTAIN USDA FUNDING

The final step in the process is for a utility to apply for USDA funding through their Rural Development program. Applications may be submitted through the online application system found at https://www.rd.usda.gov/programs-services/rd-apply.

Appendix A: 28 Selected Small Systems Cybersecurity Controls

CATEGORY 1: TRAINING STAFF TO BE CYBERSECURITY AWARE		ADDITIONAL DETAILS
AT-1	A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures.	An operator finds a USB media device. Based on their cybersecurity training, they know not to use it on the company network.
AT-2	Job-specific security training including incident response training for employees, contractors, and third-party users.	An operator has received what they believe to be a malicious email. They recognize that it is a phishing attack based on security training awareness programs the company has in place.
MA-2	Maintenance of relationships with authorities, professional associations, interest groups, etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.	The utility is a member of DHS's ICS-CERT mailing list to receive frequent communications on PCS vulnerabilities discovered and patches available. SCADA techs regularly review alerts to determine if the alerts are applicable to their system.
CATEGORY 2: KNOW WHAT HARDWARE AND SOFTWARE ARE CONNECTED TO AND OPERATING ON YOUR NETWORKS		**ADDITIONAL DETAILS**
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/ capabilities fall below a threshold.	IT monitors SCADA computers for processor usage that could indicate crypto-jacking activity.
PM-1	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.	A database is used to keep track of building conditions in the facility.
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	Third parties must review and sign an information exchange policy before connecting to the system.
SA-1	Authorization process established for new systems or changes to existing information processing systems.	A change management/review process is used to evaluate suggested changes to facility.
CATEGORY 3: MAINTAIN DATA SECURITY COMPLIANCE		**ADDITIONAL DETAILS**
DS-1	A program established to ensure compliance with the minimum PCI requirements for your associated level.	The company selected to perform billing is compliant with the minimum PCI requirements for the utility's associated level.
DS-2	A Privacy Policy as well as a Cyber Security Breach Policy are implemented.	An operator knows how to identify and respond to a suspected cyber breach, based on their cybersecurity training.
DS-3	A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.	Current practices are reviewed by legal counsel for legal compliance with HIPAA.

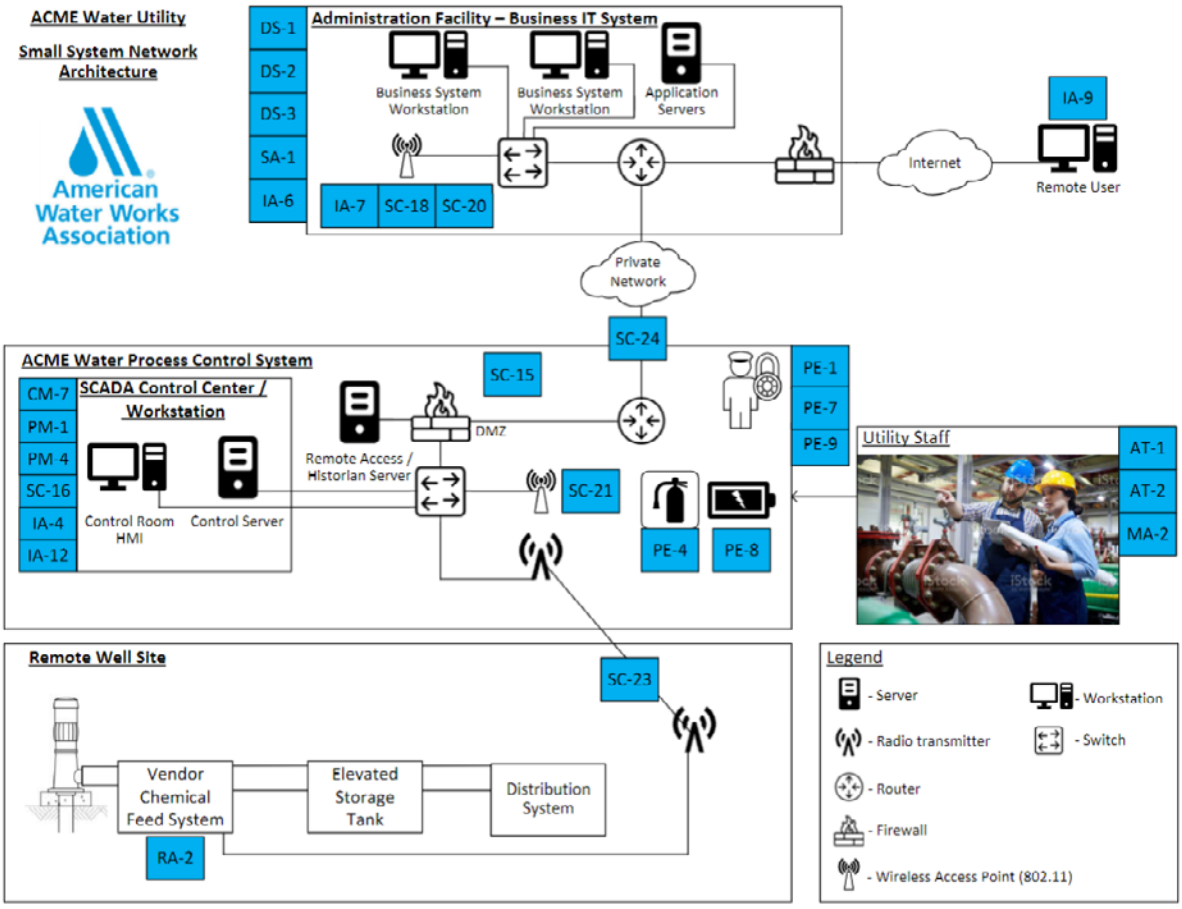
Table continued . . .

Appendix A: (continued)

CATEGORY 4: PROTECT SYSTEMS FROM UNAUTHORIZED ACCESS OR USE		ADDITIONAL DETAILS
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Contracts with third-party equipment vendors establish security requirements for remote access to equipment.
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.	To use the plant guest network, users are required to accept a user agreement.
IA-9	Multifactor authentication system established for critical areas.	Remote access to the SCADA system requires two factor authentication.
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	An operator attempts to connect to a known hacking website. The connection is blocked. The operator and IT are notified of the attempt.
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.	System integrators can only access the facility's equipment remotely from a Virtual Private Network (VPN) connection.
CATEGORY 5: PHYSICAL SECURITY		**ADDITIONAL DETAILS**
PE-1	Security perimeters, card-controlled gates, manned booths, and procedures for entry control.	Personnel are required to present a badge to access the PCS.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Fire suppression unit installed around critical equipment.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	The utility monitors facilities using security cameras.
PE-8	Physical/logical protection against power failure of equipment UPS.	Uninterruptible power supplies (UPS) are available as power backup for critical components.
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	A utility has a standby power source with separated power cabling for critical sites.
CATEGORY 6: GOOD NETWORK DESIGN		**ADDITIONAL DETAILS**
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	A utility employs multiple types of physical and cybersecurity efforts to protect assets and systems. The efforts include such things as locking doors, physical access control, and unique login requirements for each staff member.
SC-18	Minimize wireless network coverage.	Tests are conducted regularly to determine if the WiFi signals reach outside the intended area of use. If the signal reaches outside the intended area, the signal is turned down accordingly.
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.	WiFi equipment in the plant does not connect directly to SCADA network.
SC-21	Unique wireless network identifier SSID for control network.	The WiFi for the control system has a unique SSID from the business network.
SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	A wireless LAN specific domain controller is in place.
SC-23	Wireless communications links encrypted.	All data transferred via the wireless network is encrypted using current wireless communication best practices.
SC-24	Communications links encrypted.	All data transferred via the wired network is encrypted using current wireless communication best practices.

Appendix B: Small System Network Architecture

This graphic shows where each of the 28 Selected Small Systems Cybersecurity Controls apply in a water utility.



Page Intentionally Blank

Appendix C: SCADA in the Cloud: Risk and Resilience Management

TABLE OF CONTENTS

Introduction

Cloud-based technologies have grown in popularity in recent years, leading an increasing number of utilities to adopt cloud services for SCADA monitoring and control. This trend is most prevalent amongst small systems. While attractive for various reasons, utilities considering the migration to cloud-based SCADA should be aware of the risks. These risks to the security and resilience of the system must be accounted for within the life-cycle costs of the system, and the potential impacts. Therefore, any utility considering cloud-based SCADA should proceed with caution. This guide will help utilities, especially small utilities, understand some of the tradeoffs of adopting SCADA in the cloud.

Technology Background

Cloud computing technology includes a multitude of on-demand technology services where the user can use SCADA resources they need over the internet rather than having in-house (also referred to as "on-premises") resources. These cloud technologies can be adapted for use for a variety of systems, including SCADA systems. There are multiple options to support water system monitoring and operation, including

- Monitoring only – Cloud reporting/analytics tools to log and analyze data.
- Monitoring & control – Both monitoring and control capabilities so that not only are data logged and analyzed, but control of physical assets through the cloud is allowed.

THE EVOLVING PURDUE MODEL FOR INDUSTRIAL CONTROL SYSTEMS

The Purdue Model for ICS security (see Figure 1 – ISA Purdue Model for ICS) is a widely adopted network segmentation-based reference architecture for industrial control systems. It works well for on-premises process control systems that are under the complete control of asset owners; however, with the introduction of cloud services and cloud-connected devices, a hybrid model has been developed, and the flow of data is no longer strictly hierarchical.

The Purdue model still serves a purpose; however, much work is being done on revising the model for this new hybrid architecture. Figure 2 is a possible revision to support cloud services and cloud-connected devices.

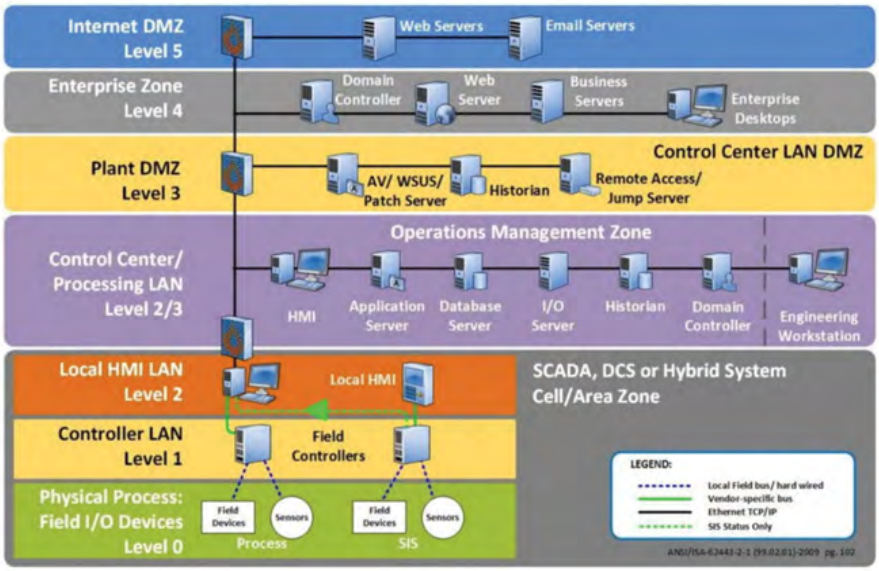


Figure 1 – *ISA Purdue Model (ISA 2009)*

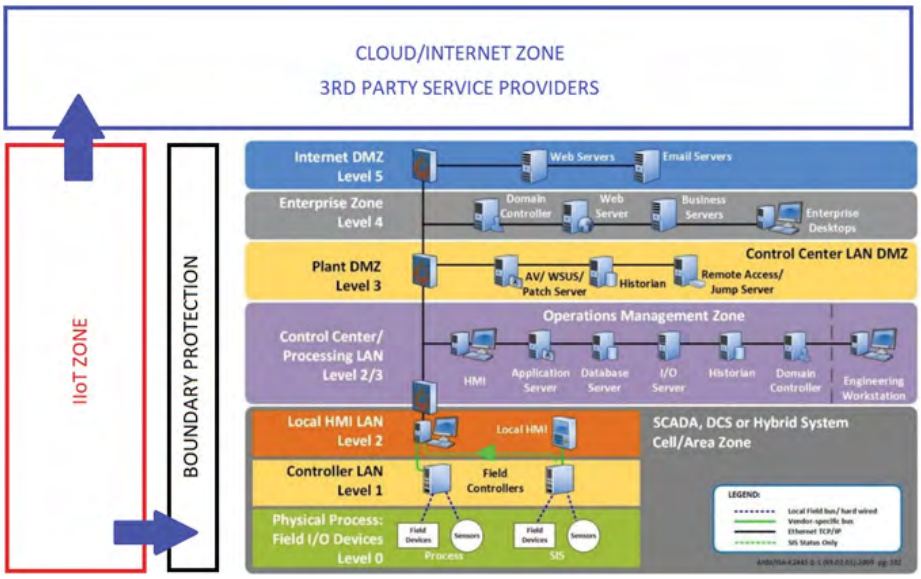


Figure 2 – *SCADA in the Cloud Purdue Model (Adapted from ISA 2009)*

Benefits of Adoption

There are many factors that contribute to the wide-spread adoption of cloud-based technologies. The following sections provide a high-level summary of these benefits.

MAINTENANCE AND EFFICIENCY

Due to the virtual nature of cloud-based technologies, the hosting of a SCADA system often results in a reduced capital expenditure. Cloud-hosted technologies, including SCADA systems, require no control centers or backup centers, allowing for the use of technologies through the internet without requiring power systems, cooling, and space for the physical storage of that technology or its data. In addition, cloud service providers for a public cloud environment tend to manage everything, including the application, data, runtime, middleware, operating system, virtualization, servers, storage, networking, and the physical security of the SCADA system, freeing up the time of in-house employees for other tasks. Many municipalities struggle to support water and wastewater SCADA systems due to the focus on first responder services (e.g., fire, police, 911).

IMPROVED CYBER HYGIENE

As a result of legacy underinvestment and the national cybersecurity skills gap, many utilities struggle to maintain good cyber hygiene within their utility. Cyber hygiene is a large concern for utilities and providers, alike. Cyber hygiene includes the steps taken by users and providers to maintain system health and improve security. Cloud service providers are expected to maintain their systems, including those containing the SCADA software and data, in a healthy manner, providing updates and patches to those systems as they are released. Additionally, cloud service providers provide routine maintenance, all of which allows the user of the service more time for other tasks. Finally, cloud service providers should have better disaster recovery/business continuity planning to respond to cyber-attacks. The utility must understand how they fit into these plans.

SCALABILITY AND COST

Due to the nature of the cloud, the resources needed for operation are easily changed, allowing for relatively easy scaling, up or down, as needed. For processing and data storage, the scaling up and down occurs automatically, making additional hardware purchases and installment for these system components unnecessary. Operational costs may be reduced, as in-house staff members are no longer responsible for hardware maintenance or backups and redundant resource costs disappear.

Risks of Adopting SCADA in the Cloud

While cloud adoption can reduce capital and O&M expenditures, there are inherent risks with implementing SCADA in the cloud. A utility considering implementing SCADA in the cloud must deal with several types of new risk. These are sorted by time scale into day-to-day risk and long-term planning risk as discussed below.

FIDUCIARY RESPONSIBILITY

Cloud-based SCADA allows utilities to contract out some of that responsibility. It must be noted that the fiduciary responsibility that utility leadership has around cybersecurity and more broadly, risk and resilience management, cannot be contracted out. Utilities are still required to do their due diligence and make best efforts to manage cyber-risk as discussed in AWWA's *Cybersecurity Risk & Responsibility in the Water Sector.*

DAY-TO-DAY RISKS

Relying on an external entity for control system operation creates new risks for the utility. This is due to an inability to implement all the security controls necessary, as many cloud providers do not allow for the implementation of outside controls and instead ask the consumer to rely on their pre-existing controls.

DEPENDENCE

A large issue with adopting SCADA in the cloud is the new dependency hazard on the cloud system. Operation of the water or wastewater system is now dependent on the cloud platform. Additionally, the reliance on the cloud-service provider will likely lead to the erosion of the knowledge and capabilities needed to successfully implement and run the water system.

INCREASING THE CYBER-ATTACK SURFACE

An inherent risk to migrating anything to the cloud is that it automatically increases the cyber-attack surface. This is due to the digital nature of the cloud, as everything is stored online and likely out-of-house, so the possibility of illegal access to operate and control systems in the cloud increases, even when controls have already been implemented.

INCREASED TARGET VALUE

Cyber-adversaries often act in a logical way. When numerous organizations rely on one service provider for services such as a SCADA in the cloud, that service provider becomes a more attractive target, (e.g. Solarwinds). As utilities adopt SCADA in the cloud from a limited number of providers, the risks of a cyber-attack on one of those providers may unintentionally increase for an individual utility.

LONG-TERM PLANNING RISKS

LIFE-CYCLE COST MANAGEMENT & "LOCK IN"

Implementation of cloud-based SCADA requires a full "rip and replace" of the existing traditional SCADA system. Coupled with the fact that the cloud-based SCADA system

hardware and software are proprietary, the utility is "locked-in" to that solution and substantial capital investment is the only way out. If utility leadership decides to change from a cloud-based SCADA service provider and return to the traditional, utility owned and operated SCADA system in the future then a whole new system will need to be designed and implemented. Also, the reliance on the cloud-service provider will likely lead to the erosion of the knowledge and capabilities needed to successfully implement and run an in-house SCADA system within the utility.

Therefore, it is critical to understand the full life-cycle costs of adopting a cloud-based SCADA solution. This not only includes the implementation of the cloud-based SCADA solution, maintenance of that solution, but the potential turn-over of the *entire* system at some point in the future to a different SCADA solution. It is recommended that this planning risk be evaluated, much like other significant hazards/planning risks for which a utility must account. Some level of financial modeling should be conducted to understand these current and future risks.

Recommendations for Utilities Considering SCADA in the Cloud

The following sections provide recommendations to support utilities with their effort to conduct due diligence and make best efforts to manage risk and resilience.

SECURITY OBJECTIVES FOR PROTECTING CLOUD INFRASTRUCTURE

SCADA in the cloud providers must implement exceptional cybersecurity practices. While most cybersecurity assessment tools are focused on on-premises systems, they can inform the practices of the cloud service providers and serve as a starting point for a utility to ask questions about cybersecurity practices.

Does the cloud service provider deploy controls/systems to provide the following?

1. **Asset Management** – automatically building an inventory and tracking the real-time status of the devices and collecting metrics such as:
    a. Device type, hardware version, software version
    b. Location
    c. Local/remote credentials
    d. Network traffic patterns (protocols, packet/byte counts, number of sessions)
    e. IP addressing information
    f. Threat level based on known vulnerabilities
2. **Application Visibility and Control** – continuous monitoring of protocols and functions that are being used between devices and alerting on abnormal communications/activities.
3. **Intrusion Detection and Prevention** – always assume cloud servers/devices may become compromised, leading to an attack. Does cloud provider deploy an intrusion prevention system (IPS) to detect and block attacks against cloud-connected devices.
4. **Network Segmentation** – how are cloud-connected devices segmented from other clients? How are control servers and remote access segmented? Is the service dedicated (not shared between clients) or a multi-tenant architecture?
5. **Logging and Monitoring** – centralized logging and monitoring of the entire cloud environment. This includes establishing baselines and providing access to logs and events that are generated from deviations to the baseline.

Many current cybersecurity assessment tools including the AWWA Guidance and AWWA Tool (AWWA 2019) are primarily applicable to on-premises SCADA systems. At the same time, the most common SCADA architecture model (the Purdue model) has not been fully adapted to integrate cloud-based technologies.

Cloud SCADA service providers may not be willing to share many of these details on their operations. The utility should conduct sufficient due diligence to ensure the security practices of the provider are consistent with risk management expectations of the utility and not rely on unverified trust.

SERVICE LEVEL AGREEMENTS AND QUESTIONS TO ASK

One of the best ways to manage the risks mentioned previously is to establish a strong service level agreement (SLA) with the cloud service provider. An SLA lays out all the information a user might need to make an informed decision on which cloud service provider to use – especially regarding responsibility of use on both the user side and the provider side. The SLA should answer all the following questions:

- **Availability –** What is the availability promised by the cloud service provider? Is there a plan in place for unexpected downtime? How are users updated on planned downtime due to maintenance and repairs?
- **Data ownership –** Who owns the data stored in the cloud? What is the data availability to the user after termination of use? How good is the cyber hygiene of the provider?
- **Disaster recovery and backups –** What is the plan in case of a disaster? Does the cloud service provider have a backup and recovery system? Does it require activation of field units? How are backups of the data taken? How often are they taken? What is plan B in case of a disaster?
- **Cloud hardware and software –** What are the specifications behind the cloud environment construction? What hardware is being used by the cloud service provider? What software is being used? What are their versions?
- **Customer (utility) responsibilities –** What is the customer liable for? What are the expectations of the customer? What type of backup operational capabilities does the utility need to maintain?

SELECT CONTRACTING TERMS TO UNDERSTAND

The following select contracting terms should be understood by the utility and negotiated to the extent possible.

1. **Data confidentiality and integrity –** Determine who holds the responsibility for data confidentiality and integrity. In most cases, the cloud service provider expects the user to be responsible for the confidentiality and integrity of data.
2. **Data storage –** Determine where the data is stored (i.e., country?) and if there are existing policies for the storage of various forms of data in secure places.
3. **Compensation –** Determine what happens if there is a failure on the side of the cloud service provider. In many cases, cloud service providers take a limited liability approach and provide no compensation in the case of negligence or failure, so it is important to understand what is provided if an incident occurs.
4. **Changes to the terms –** Determine how changes of the terms of agreement take place, as well as how the service provider will notify the user of changes.
5. **Dispute resolution –** Determine where dispute resolution is to take place in case of an issue. There are varying laws in different jurisdictions, and it is important to know the rights of the organization.

Cyber-Physical Resilience

In addition to the adapted Purdue model presented in Figure 2, process control systems should be engineered to protect physical assets and minimize the impact of a cyber event. A good framework to direct the engineering and operations efforts to improve cyber-physical resilience is Idaho National Laboratory's (INL's) Consequence-driven, Cyber-informed Engineering (CCE; INL 2021). This framework helps to identify common engineering controls such as simple and inexpensive analog devices that could minimize the impact of a cyber event. While the principles of CCE are universal in their application, it should be applied to individual implementations to ensure that any cyber-physical controls do not interfere with the proprietary hardware and software from the cloud-based SCADA service provider.

Cyber Risk

While relying on a cloud service provider for SCADA monitoring and control may be an attractive idea, there are some inherent risks that must be explored. Any monitoring and processing of data, especially sensitive or business-critical data, from outside of the business introduces risk due to the inability for that data to be processed using in-house security controls. Any control of physical assets through the cloud should be evaluated in detail and backups and physical protections must be considered.

SCADA in the cloud may be most applicable to facilities and operations where the risk of service disruption to customers, especially critical customers, such as healthcare facilities, is minimal. Regardless of the application of a cloud-based SCADA solution, a utility must do their due diligence and make well-informed efforts to manage risk.

REFERENCES

AWWA. 2019. Cybersecurity Risk & Responsibility in the Water Sector. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013. Last Accessed: September 3, 2021.

AWWA. 2019. Water Sector Cybersecurity Risk Management Guidance. https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960. Last Accessed: September 3, 2021.

INL. 2021. Consequence-driven, Cyber-informed Engineering. https://inl.gov/cce/. Last accessed: September 3, 2021.

ISA. 2009. ISA62443 – ANSI/ISA-62443-2-1 (99.02.01)-2009. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.

NSA. 2018. Cloud Security Basics. https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-cloud-security-basics.pdf. Last Accessed: September 21, 2021.

American Water Works
Association