CYBER SECURITY ASSESSMENT
AND
RECOMMENDED APPROACH

STATE OF DELAWARE
DRINKING WATER SYSTEMS

FINAL REPORT

February 2016

DPH Contract #15-361

Kash Srinivasan Group

Page Intentionally blank

TABLE OF CONTENTS

TABLES

EXECUTIVE SUMMARY

Water utilities are classified as critical infrastructure under the Presidential Order issued in 2013 and the USEPA has the responsibility to establish cybersecurity requirements for this sector. Cyber attacks on water systems target the control systems that are used to monitor and control their operations. Commonly know by the acronym SCADA (Supervisory Control and Data Acquisition Systems), they are currently in use in all four of the large utilities in Delaware and six of the 31 small and medium utilities have self-identified as having these systems as well. The SCADA systems vary in complexity, as the sample of four utilities assessed in this study indicates.

The American Water Works Association (AWWA) has developed a Cyber Security Tool that offers a layered approach for utilities to address cyber threats. The security layers are arranged from least to most complex in four control levels. The AWWA recommends that utilities move initially to adopt and implement the Priority 1 Controls as a minimum level of security for utilities.

The Division of Public Health Drinking Water State Revolving Loan Fund Program initiated actions to research cyber security in water utilities within the State. This study recommends that the Division adopt a common set of controls (the full suite of 26 AWWA Priority 1 Controls) applicable to all utilities with SCADA systems in Delaware. Over the next several years, the Division should encourage utilities to formally assess their cybersecurity posture and provide resources to assist with the development and implementation of concrete actions consistent with achieving a minimum level of security.

A key finding of this study is that there are only minor differences in the control recommendations between the least and most complex utilities in the sample. Since SCADA systems provide significant operational value, it is likely that the complexity of the simplest systems will increase over time. This report therefore recommends that the State adopt a common set of controls that all utilities should implement for their systems.

Actual implementation of the AWWA controls requires utilities to reach into source documents prepared by the Department of Homeland Security, the National Institute of Standards and Technology and the AWWA. These are highly technical documents that are challenging for utility managers to read and interpret. This report offers a set of simplified guidelines that utility managers can reference as they engage with their technical teams to implement cyber security controls.

BACKGROUND

The Delaware Department of Health and Social Services, Division of Public Health (the "Division") exercises regulatory oversight over the drinking water systems in the State of Delaware. Of the 35 utilities in the State, 4 are classified as large systems (serving more than 100,000 people), 13 are classified as medium systems (serving between 3,300 and 100,000 people) and 18 are classified as small systems. Three of the large systems and one small system are privately owned. The remaining are municipally owned and operated systems.

In recognition of the growing threat of cyber intrusions into a variety of institutions in the country, a Presidential Executive Order issued in 2013[1] requires, among other actions, the development by the National Institute of Standards and Technology (NIST) of a "framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework)…[to] include a set of standards, methodologies, procedures, and processes that align policy, business and technological approaches to address cyber risks." The Order directs the Secretary of the Department of Homeland Security (DHS) to "establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities." The Cybersecurity Framework builds on a number of other reference documents developed by both the NIST and others.[2]

Because of their central role in public health protection, water systems constitute "critical infrastructure" as defined in the Order. The authority to establish cybersecurity requirements for water infrastructure is delegated to the US Environmental Protection Agency (EPA) by the Executive Order. EPA's assessment is that cyber attacks on water systems, while disruptive to facility operations, are unlikely to have regional or national impacts; EPA specifically endorses a voluntary partnership approach to reducing cyber risks.[3] EPA's path forward includes working with sector partners to encourage adoption of the NIST Framework by water utilities. One such partner is the American Water Works Association (AWWA). In 2014, the AWWA released a cybersecurity guidance document and assessment tool to "provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber attacks."

---

[1] Presidential Executive Order – Improving Critical Infrastructure Cybersecurity; http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] Framework for Improving Critical Infrastructure Cybersecurity; Version 1.0; National institute of Standards and Technology; February 12, 2014

[3] Letter to Michael Daniel (White House Cyber Security Coordinator) from Peter C. Gravatt, Director, EPA Office of Drinking Water

This is the context for the present effort by the Division, which seeks to develop an understanding of the potential scale of cyber vulnerability and, based on that understanding, develop appropriate programs and support mechanisms to improve the resiliency of the State's water systems

Vulnerabilities to cyber attacks are inherent, to various degrees, in the Process Control Systems that are used in water utilities to monitor and control the treatment and delivery of potable water. These control systems are generally referred to by the acronym "SCADA" (Supervisory Control and Data Acquisition). By providing the ability to track and report on a large number of operating and water quality parameters, SCADA systems greatly enhance the level of operator and management control that can be exercised, and help assure the delivery of safe water to the public. As a consequence, utility SCADA systems tend to evolve from stand-alone systems to more complex topologies providing information and control capabilities to all levels of a utility organization locally, through mobile devices and remotely through the Internet.

Not unexpectedly, the adoption and scope of SCADA technology by a utility depends on its size. All of the large utilities utilize these systems for monitoring and control; 5 of 12 of the medium-sized utilities currently use SCADA, however, this number is expected to grow as utilities within this range upgrade their facilities. Only one "small" utility has confirmed that it uses SCADA.

"Shodan" (www.shodan.io) is a search engine created for the express purpose of locating "devices connected to the Internet, where they are located and who is using them." *Anyone* can look for these "devices" by type and location – including industrial control systems that are connected to the Web. Essentially, the system is easily visible to hackers, who can take advantage of default user names and passwords typically bundled with these systems (like *water, water; admin, 1234*) or weak names and passwords to gain entry.

These utilities were invited to attend a one-day workshop on the topic. The presentation by Ken Eisenhart of the Virginia Department of Health (VDH) included statistics on cyber attacks on water utilities in 2012 and a discussion of early cybersecurity recommendations from the Water Information Sharing and Analysis Center. [4] Unfortunately, the workshop was poorly attended, an indication perhaps of the low priority that utilities afford this topic. Virginia is the only State in EPA Region III to have an active program of cybersecurity assessments for public water utilities. VDH has contracted with the Horsley Whitten Group to conduct on-site assessments for utilities, free of charge. While a similar approach may be an option for the Division in the future, the decision was made following the workshop to develop a high-level assessment of issues and needs. The strategy adopted uses the AWWA Cybersecurity

[4] WaterISAC, an organization formed by the major water sector organizations including the AWWA, WEF.

Tool. A discussion of the use of the tool and the findings generated for each of the participating utilities by the tool follows.

A BASIC SCADA NETWORK

The PLCs (Programmable Logic Controllers) connect to the physical operating and measurement devices (pump switches and flow meters, for example) within the water system. They provide monitoring and control functions through their internal logic settings and in response to commands from the operator control panel (the HMI or Human Machine Interface).

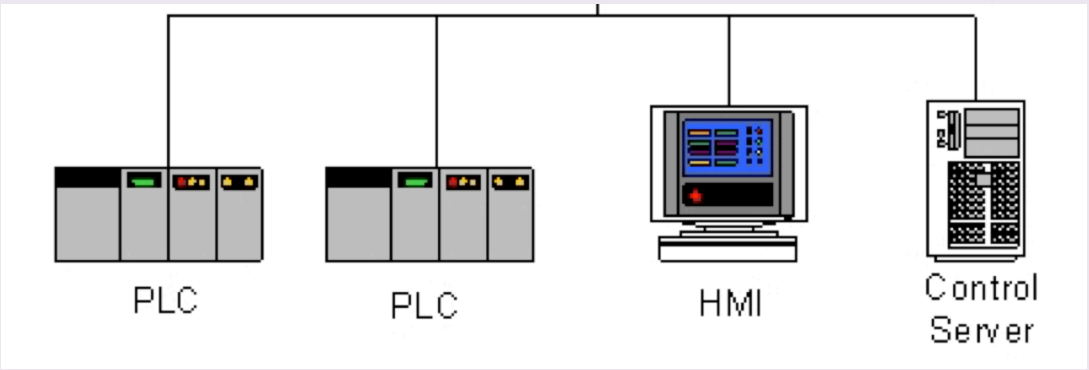


Figure extracted from the NIST Special Publication 800-82, Rev. 1

AWWA CYBER SECURITY TOOL

The Tool was developed in 2014 as a mechanism for water utilities to perform self-assessments and develop appropriate cyber protections. Utilities enter basic information about their SCADA systems, structured as "Use Cases" which are specific characteristics of the utility, defining the structure, management and methods of user interaction of the systems.[5] Once the user makes a selection of the applicable combination of Use Cases, the Tool generates a set of cybersecurity recommendations organized in priority levels 1 through 4, with level 4 representing the most complex and most robust protection level. The recommendations are cross-referenced to cybersecurity standards published by other organizations, including the NIST standards. Priority level 1 represents the minimum level of security recommended. Implementation of additional levels is based on the sophistication and needs of the individual utility.

AWWA USE CASES

Architecture

AR1	Dedicated Network
AR2	Shared WAN
AR3	Shared LAN

Network Management

NM1	Local Network Management
NM2	Plant Network Management
NM3	Remote Network Management

Program Access

PA1	[Automated] Outbound messaging
PA2	[Interactive] Outbound file transfer
PA3	[Interactive] Inbound file transfer
PA4	[Automated] Software Update
PA5	[Automated] Date exchange
PA6	[Automated] Network Monitoring

PLC Programming and Maintenance

PLC1	Local PLC programming and maintenance
PLC2	Plant PLC programming and maintenance
PLC3	Remote PLC programming and maintenance

User Access

UA1	Control system access with control
UA2	Plant system access with control
UA3	Remote system access with control
UA4	Remote system access with view only
UA5	Remote system access with web-view

Four Delaware utilities agreed to participate in the AWWA self-assessment process. The development of applicable Use Cases for each utility was accomplished through face-to-face discussions with management and knowledgeable technical staff. The Tool was then utilized to generate a report identifying cybersecurity controls appropriate for the utility, organized by priority level.
The Use Cases pertinent to each of the four utilities sampled for this assessment are shown below. The utilities differ in terms of the scopes of their SCADA systems, ranging from most (Utility A) to least (Utility D) complex in terms of configuration and the manner in which the utility uses its system. (The use of shading in the table is intended to visually highlight the differences in Use Cases among the utilities).

[5] Process Control System Security Guidance for the Water Sector, AWWA, 2014

TABLE 1. AWWA Use Cases for Sampled Utilities

Use Cases	A	B	C	D
AR1	✓			✓
AR2	✓	✓	✓	
AR3	✓	✓		
NM1	✓	✓	✓	✓
NM2	✓	✓	✓	✓
NM3	✓	✓	✓	✓
PA1	✓	✓	✓	✓
PA2	✓		✓	
PA3	✓			
PA4		✓		
PA5	✓	✓	✓	
PA6	✓	✓		
PLC1	✓	✓	✓	✓
PLC2	✓	✓	✓	
PLC3	✓	✓		
UA1	✓	✓	✓	✓
UA2	✓	✓	✓	✓
UA3	✓	✓	✓	✓
UA4	✓	✓	✓	✓
UA5	✓			

NOTE: A ✓ indicates that the Use Case applies to the utility.

The AWWA Cybersecurity Tool takes the applicable Use Cases for a utility as its input and generates a set of recommended controls, organized in four priority levels, for the utility. Priority 1 controls represent AWWA's recommended minimum level of security that the utility should achieve; Priority 2, 3 and 4 Controls represent actions providing increased levels of security, with Priority 4 affording the greatest protection against sophisticated attacks. Consistent with the approach of achieving voluntary reductions in cyber vulnerability over time, the immediate focus of the exercise is to achieve the recommended Priority 1 controls; these are tabulated below for each of our test utilities.

TABLE 2. Priority 1 Controls Recommended by the AWWA Tool

Priority 1 Controls	FACILITIES			
	A	B	C	D
Audit and Accountability				
AU2	◆	◆	◆	◆
AU3	◆	◆	◆	◆
Configuration Management				
CM7	◆	◆	◆	◆
Access Control; Identification and Authentication				
IA1	◆	◆	◆	◆
IA10	◆	◆	◆	◆
IA12	◆	◆	◆	◆
IA2	◆	◆	◆	◆
IA5	◆	◆	◆	◆
IA9	◆	◆		
Planning, Contingency Planning, Incident Response				
IR2	◆	◆	◆	◆
Physical/Environmental Protection				
PE1	◆	◆	◆	◆
PE2	◆	◆	◆	◆
PE8	◆	◆	◆	◆

◆ indicates that the control is applicable to the utility.

Table 2. (Priority 1 Controls continued)

Priority 1 Controls	FACILITIES			
	A	B	C	D
Security Assessment and Authorization Program Management				
PM3	◆	◆	◆	◆
System and Service Acquisition				
SA4	◆	◆	◆	◆
System and Communications Protection				
SC1	◆	◆	◆	◆
SC10	◆	◆	◆	◆
SC12	◆	◆	◆	◆
SC2	◆	◆	◆	◆
SC3	◆	◆	◆	◆
SC4	◆	◆		
SC6	◆	◆	◆	◆
SC8	◆	◆	◆	◆
System and Information Integrity				
SI3	◆	◆	◆	◆
SI4	◆	◆	◆	◆
SI5	◆	◆	◆	◆

◆ indicates that the control is applicable to the utility.

An examination of the collective recommendations quickly reveals that the Priority 1 recommendations are remarkably consistent across the four utilities, notwithstanding the differences in complexity of their respective SCADA systems. This is a key finding of the preliminary assessment process and suggests that the Division should craft and support a uniform approach to cyber security for all of the utilities in the State.

RECOMMENDED CYBER SECURITY PROGRAM

The Division should encourage all utilities with SCADA systems to adopt the full suite of 26 AWWA Priority 1 Controls listed in Table 2.

After utilities gain sufficient experience with these measures, additional encouragement and support should be provided to enable utilities to move up the security ladder through sequential adoption of the AWWA control priorities 2 through 4.

The Priority 2 Control recommendations for the participating utilities (see Table 3) also indicate a significant commonality of controls, suggesting that a common set of recommendations could be developed for these controls as well. Utility SCADA systems are likely to move towards greater functionality and complexity over time and will be subject to more sophisticated adversaries. A common set of control recommendations at the Priority 2 level may also be reasonable for the Division to adopt, as and when the Division decides that cyber threats warrant higher levels of protection.

Table 3: Priority 2 Controls Recommended by the AWWA Tool

Priority 2 Controls	FACILITIES			
	A	B	C	D
Awareness and Training				
AT1	X	X	X	X
AT2	X	X	X	X
Audit and Accountability				
AU1	X	X	X	X
AU4	X	X	X	X
AU5	X	X	X	X
Configuration Management				
CM3	X	X	X	X
CM4	X	X		
Access Control; Identification and Authentication				
IA11	X	X	X	X
IA6	X	X	X	
IA7	X	X		

X indicates that the control is applicable

Table 3: (Priority 2 Controls continued)

Priority 2 Controls	FACILITIES			
	A	B	C	D
Planning, Contingency Planning, Incident Response				
IR1	X	X	X	X
Maintenance				
MA3	X	X		
Security Assessment and Authorization; Program Management				
PM1	X	X	X	X
PM4	X	X	X	X
PM5	X	X	X	X
Personnel Security				
PS1	X			
PS2	X	X	X	X
PS4	X	X	X	X

X indicates that the control is applicable

Table 3: (Priority 2 Controls continued)

Priority 2 Controls	FACILITIES			
	A	B	C	D
Risk Assessment				
RA2	X	X		
System and Service Acquisition				
SA1	X	X	X	X
SA2	X	X	X	X
SA3	X	X	X	X
SA5	X	X	X	X
System and Communications Protection				
SC13	X	X		
SC7	X	X		
SC9	X	X	X	X

X indicates that the control is applicable

THE DECISION-MAKING FRAMEWORK

Municipal water utilities in the State operate under a governance framework consisting of an elected body that delegates the executive functions necessary to the provision of water service to an appointed individual – a city or town manager or a department head. This leadership team has the ultimate responsibility for articulating risks that can affect the key missions and business functions of the organization. The effective management of risk depends on an understanding of the likelihood and impact of adverse events. Decisions involving the acceptable level of risk, and the management of risk, can only be taken at this organizational level.

Security objectives for information systems generally focus on:

- Confidentiality: preserving authorized restrictions on information access and disclosure, including means of protecting personal privacy and proprietary information.
- Integrity: Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity.
- Availability: Ensuring timely and reliable access to, and use of, information.

Attacks on the organization's SCADA system, either directly or though connections with an enterprise network, can impair its functionality. Understanding the potential impacts of impairments (low, serious, catastrophic) can help guide the types of security policies, and administrative and technological controls, that the organization chooses to deploy.

The NIST Framework

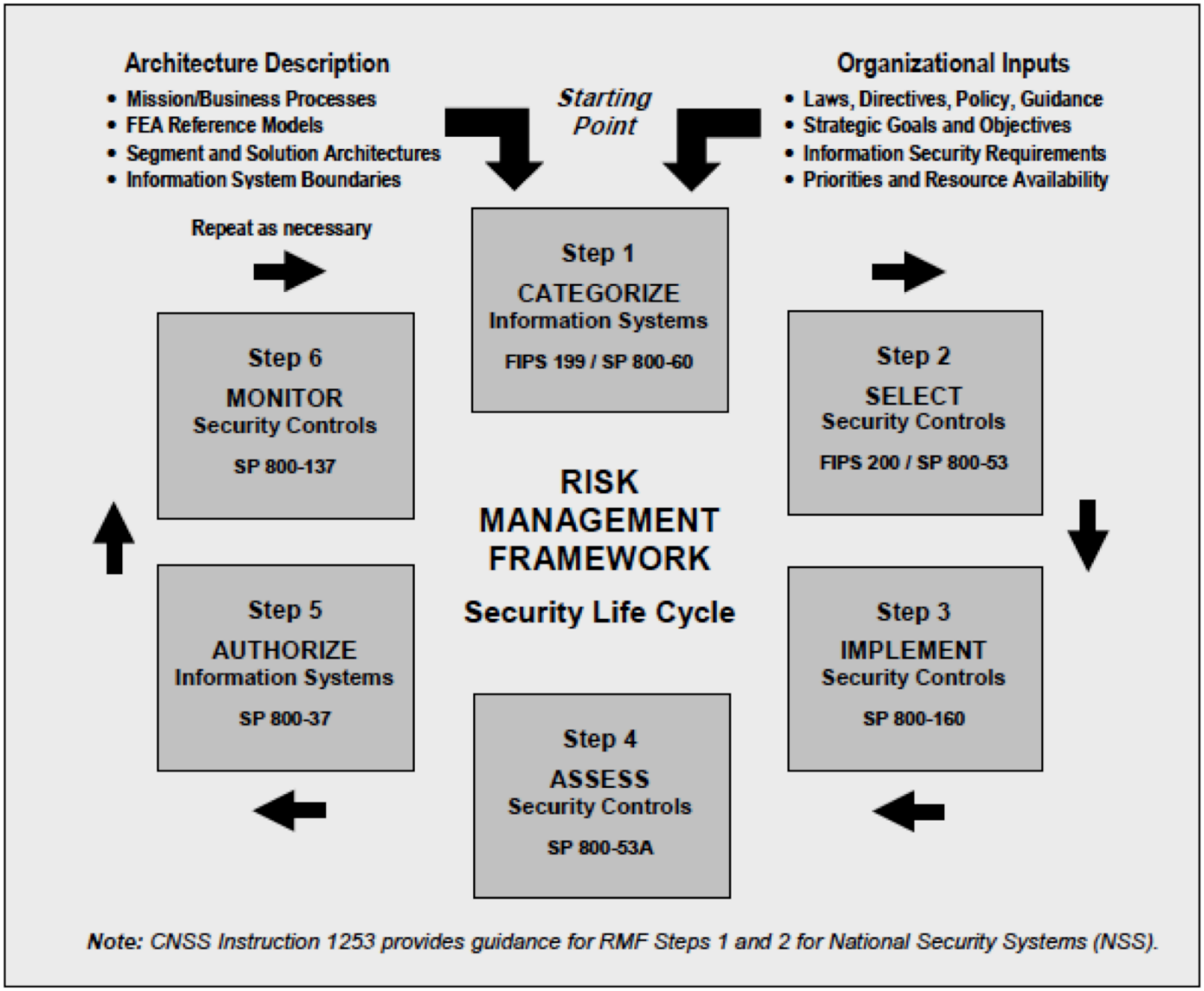
The NIST, and others, have developed a comprehensive set of security controls that can be tailored to the security policies of an organization. *Non-technical* controls address matters such as policies and procedures at the management and operational levels, including emergency response and recovery; *technical* controls address the architecture and the specific security functions embedded in hardware, software and firmware (i.e.; computing hardware containing built-in software that cannot be modified).

This Cybersecurity Framework is a voluntary mechanism that encourages organizations to understand their current security posture, develop a desired target state based on internal risk assessments, engage in a process for improvements and communicate to internal and external stakeholders about cybersecurity risk. The Framework recognizes that organizations fall into implementation "Tiers" based on how they view cybersecurity risk and the processes currently in place to manage risk. [6] The 6-step sequence recommended by NIST (the Risk Management Framework) involves:

[6] Cybersecurity Framework Section 2.2, "Framework Implementation Tiers"

- Categorization of the information system(s)
- Selection of Security Controls
- Implementation of Security Controls
- Assessment of Security Controls
- Authorization of Security Controls
- Monitoring of Security Controls

NIST's risk management framework is depicted in the figure below.



The NIST source document provides detail on the six-step approach and is recommended reading by systems seeking to get a better understanding of the general approach to cybersecurity implementations for any enterprise. [7] The Framework identifies four "Implementation Tiers" - Partial, Risk Informed, Repeatable and Adaptive. The tier that best characterizes a particular organization is a function of its choices with regard to its risk appetite and the management of risk. The Framework presumes that the organization has the capacity to institute a process to properly frame these choices and implement appropriate controls commensurately.

The AWWA Approach

As discussed earlier in this document, the AWWA has crafted a set of recommendations tailored to water utilities, organized under four discrete levels of control. These levels of control are more directly prescriptive in comparison with the implementation tiers of the NIST Framework. The AWWA Guide and Tool were developed through consultations with water industry experts and provide a way to more directly generate the security controls in step 2 of the NIST risk framework. It should be noted that the AWWA approach heavily references the extensive body of cyber security work developed by the DHS and NIST. The Priority 1 Controls identified for the utilities surveyed for this study are detailed in Appendix A. Implementation of the AWWA recommendations requires understanding and interpretation of the referenced source documents.

[7] NIST Special Publication 800-53, Rev. 4; Security and Privacy Controls for Federal Information Systems and Organizations

GUIDANCE FOR NON-TECHNICAL DECISION MAKERS

"HALT! WHO GOES THERE!"

The medieval castle is a useful analogy to illustrate the obligations and concerns of municipal managers with regard to cybersecurity. A castle is a complex of sturdy structures with one or more defensive features. Its function is three-fold:

- House the lord and lady of the "realm" (the agricultural and forest lands under their control)
- Provide defense against military attacks and serve as the base for projecting military power
- Serve as the administrative center

The construction and maintenance of a castle represents significant expense requiring careful thought regarding the design of the structures, the policies, practices and resources devoted to defense against subversion and attack, and the day-to-day management and control of the interactions with the surrounding countryside. Implicit in these decisions is the involvement of the lord and his advisers as they weigh the potential expense against the perceived risks that must be protected against. Furthermore, the defenses provided solely by architectural means must be supported by procedural defenses to assure that the transactions of people and goods that are necessary to the functioning of the castle do not allow hostile elements to infiltrate. These procedural defenses may include a layered approach requiring special permissions and escorts to certain sensitive areas of the castle and internal eyes and ears ("spies") to track and report on anomalous activity.

Your water utility represents a critical component of the municipal functions that you provide. The SCADA system embedded in your utility enables the continuous tracking of parameters[8] that define the performance of the utility function. It may also provide the capability to operate system components either automatically or under operator control from a central site, remote from the components being controlled. [9] At its most basic level, a SCADA system consists of a central computer and a desktop graphic display for the operator, which continuously displays the status and performance of the system components and (depending on the design) allow for individual devices to be remotely controlled. [10]

---

[8] For example, pumping flow rates, tank levels, chlorine levels

[9] For example, chemical dosing rates, turning pumps on and off, flow pacing in response to system demand.

[10] The display panel is variously known as a Human Machine Interface (HMI), a Graphical User Interface (GUI) and other such labels.

Operating components of the utility are connected to the central computer through other special purpose computers called programmable logic controllers (PLC). A PLC typically connects to a group of related water system components[11] and can both report back on the status of these components and execute a local control program particular to the components/devices to which it is connected.

THE LEADERSHIP CHALLENGE – AN OVERVIEW

As the leader or key manager of the enterprise, you preside over the people, structures, and operating and control equipment that make up your utility. Analogous to the lord of the castle, you have the obligation to make and implement decisions regarding the protection of the utility against both physical and cyber attacks. In consultation with your internal (key staff) and external (SCADA vendor, engineer) advisers you will need to:

- Carefully consider your risk posture, through a formal assessment of the likelihood and consequences of an attack
- Identify the resources you are willing to allocate to mitigating risk
- Define the SCADA architecture commensurate with these resources and your risk tolerance
- Identify the pool of people who are allowed access to the SCADA system and the methods you will use to mimic the "guardhouse" and "spy" functions
- Develop mechanisms for response to, and recovery from, attacks

In broad terms, the actions you will need to consider fall under two categories:[12]

- **Governance**: embodying the policies and practices you instill within the organization controlling access to and use of the system by your staff, vendors and other authorized users;
- **System design**: enabling the basic operational monitoring and control functions of the utility, the enforcement of the policies and practices above and resiliency to recover from a disabling incident.

Access control, a central focus of both of these categories, takes many forms.

[11] For example, a storage tank and associated pumps and monitoring instruments.
[12] The section that follows draws from the suite of Priority 1 Controls recommendations of the AWWA cybersecurity tool; See Appendix A.

- Begin with instilling security consciousness within the organization and making clear the behaviors that are expected from staff as they perform their daily functions.
- A formal system must be established for assigning unique user IDs and strong passwords to every authorized user; a formal mechanism for reuse and disabling of identifiers must be in place. The organization develops policies and procedures concerning the generation and use of passwords; rules of complexity are commensurate with the criticality of the systems being accessed.
- User access privileges may be limited depending on operational need, with wide-ranging administrative privileges being limited to a select few; the SCADA system is configured to enforce limits on access to information and system resources consistent with the adopted access policies;
- The system uniquely identifies and authenticates users and processes acting on behalf of users; the system must provide for user authentication and support management oversight through reporting on system use;
- Remote users are subject to strong authentication procedures and access only though a secure firewall; the organization establishes and documents usage restrictions, configuration and connection requirements and implementation guidance for each type of remote access allowed; remote access is authorized prior to allowing connections to be made.
- Physical access to the SCADA system is also controlled through access authorization systems (e.g.; key cards), guard security, visitor escort;
- Security is provided for keys, key cards and combinations and a periodic inventory is conducted of all access devices.
- The organization restricts connections of mobile devices to the SCADA system and monitors for unauthorized connections.[13]
- The configuration settings for each component of the SCADA system are consistent with the adopted security posture; deviations are identified documented and approved based on defined operational requirements.

System design must provide for system security and resiliency:

- Software installed on the system must be subject to rigorous review and approval.
- Monitoring and control components include management of inbound and outbound communications through each telecommunications channel.
- System architecture includes multiple layers, with different, overlapping security requirements.
- The SCADA system must be correlated with the critical business/mission processes provided by the utility and the consequences of disruption must be characterized; use the outcome of this assessment to develop contingency plans

[13] Mobile devices include portable computers, PDAs, USB sticks, portable hard drives

including need for back-up and redundancy. (While targeted to the more complex SCADA systems, this recommendation may be a useful exercise for small systems to consider as well).

- Cryptographic keys, if used, must be coupled with a manual or automated process to manage keys.
- The SCADA system must be logically separated from the corporate network; eliminate direct communication pathways between the corporate and SCADA networks by placing common accessible components in a separate zone (a DMZ) [14] protected by a firewall.
- Intrusion detection and prevention tools, scanning tools, protection against malware, network monitoring software, audit record monitoring software are deployed; the system monitors events external to the SCADA system (perimeter defense). (This recommendation is also targeted to the more complex SCADA systems, but is useful to consider for small systems as well).
- Control systems are divided into functional zones and the organization deploys defensive practices appropriate to each zone and across zones;
- The Industrial Automation Open Networking template is used when adopting practices regarding firewalls.
- The system generates time-stamps mapped to a reference using internal clocks for audit purposes (usually set to GMT)

Contingency and recovery planning is a critical element of the SCADA deployment and management process:

- The organization must have a response team and proven incident response plans in place to recover control system operational status after a disruption.
- The plans must be based on understanding and preparing for attacks from likely sources and must prioritize its response actions based on business impact, information security and recoverability.
- The ability to maintain essential utility functions in the event of the failure of a primary telecommunications service may require the establishment of an alternative service arrangement.

"EASY FOR YOU TO SAY!" – SIMPLIFYING THE DIALOGUE

Utilities seeking to improve their security posture using the AWWA tool are confronted with the challenge of understanding and interpreting the contents of the reference documents associated with each control recommendation. While large utilities may be able to bring in the necessary expertise to help them craft a successful program, they, along with their smaller counterparts, may well find the task to be daunting.

[14] Demilitarized Zone

In recognition of this potential roadblock, and as a further supplement to the broad guidelines offered in the previous section, this report includes a list of actions (Appendix B: "Cyber Security Policy Document for Managers") to facilitate the decision-making dialogue. The document in Appendix B was developed in collaboration with a SCADA integrator. [15] The simplified approach offered here may help ease the learning curve for decision makers by improving awareness of the cyber security challenge and the actions needed to mitigate risks.

[15] Allied Control Services, Inc., West Point PA

APPENDIX A: AWWA PRIORITY 1 CONTROLS

26 AWWA-recommended cybersecurity controls are generally applicable to all Delaware water utilities. They are described below.[16] These controls represent the minimum acceptable level of security for SCADA systems. They are organized under 9 major categories (Audit and Accountability, Configuration Management, etc.). Each major category has several sub-categories. Only selected elements for each category are applicable to the Priority 1 control level. For example, in the Audit and Accountability category, the elements applicable to Priority 1 are AU-2 and AU-3; elements AU-1, AU-4 and AU-5 will come into play when the utility elects to advance to Priority 2.

Audit and Accountability

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.

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 areas of responsibility.

Configuration Management

CM-7: Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.

Access Control; Identification and Authentication

IA-1: Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication and management oversight.

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.

IA-5: Access control for diagnostic tools and resources, and configuration ports.

IA-9: Multifactor authentication system established for critical areas.

[16] A total of 82 controls make up the full suite of controls in the 2014 AWWA Cybersecurity Guide. The control descriptions are from Table 3-2 of the Guide.

IA-10: Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.

IA-12: Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.

Planning; Contingency Planning; Incident Response

IR-2: A security program established 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.

Physical and Environmental Protection

PE-1: Security perimeters, card controlled gates, manned booths and procedures for entry control

PE-2: Secure areas protected by entry controls and procedures to ensure only authorized personnel have access.

PE-8: Physical/logical protection against power failure of equipment (UPS)

Security Assessment and Authorization; Program Management

PM-3: Centralized logging system including policies and procedures to collect, analyze and report to management.

System and Services Acquisition

SA-4: Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication problems.

System and Communications Protection

SC-1: Policies and Procedures governing cryptography and cryptographic protocols including key/certificate management established to maximize protection of systems information

SC-2: Centralized authentication system or single sign-on established to authorize access from a central system

SC-3: Policies and procedures established for network segmentation including implementation of DMZ's based on type and sensitivity of equipment, user roles and types of systems established

SC-4: Intrusion detection, prevention and recovery systems including approved policies and procedures established to protect against cyber attacks. System includes repository of fault logging, analysis and appropriate actions taken.

SC-6: Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.

SC-8: Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.

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).

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.

System and Information Integrity

SI-3: Interactive system for managing passwords implemented to ensure password strength

SI-4: Organization-wide clock synchronization system in place

SI-5: Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as audit tools that can modify or delete audit data

SOURCE DOCUMENTS AND CROSS REFERENCING:

Implementation of the recommended controls requires detailed review of the source documents on which they are based. Table A-1 identifies the source document sections applicable to the control elements specified above.

LIST OF SOURCE DOCUMENTS

AWWA G430	Security Practices for Operation and Management, AWWA 2014
DHS CAT	Catalog of Control systems Security: Recommendations for Standards Developers; Department of Homeland Security, 2011
DHS DID	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies; Department of Homeland Security, 2009
NIST 800-34	Contingency Planning Guide for Federal Information Systems; NIST 2010, Rev. 1
NIST 800-53	Security and Privacy Controls for Federal Information Systems and Organizations; NIST, 2013, Rev. 4
NIST 800-61	Computer Security Incident Handling Guide; NIST, 2012, Rev. 2
NIST 800-82	Guide to Industrial Control Systems (ICS) Security; NIST, 2013, Rev. 1

TABLE A-1: Cross-reference to Sources

CONTROLS	AWWA Cross reference	Sub reference
Audit and Accountability AU2 AU3	DHS CAT 2.1 Security Policy NIST 800-53 Appendix J: AR-1 governance and Privacy Program	NIST 800-53r3: AC-1, SC-14, PM-1
Configuration Management CM7	NIST 800-53 Appendix F-CM; CM-11 User Installed Software	
Access Control; Identification and Authentication IA1 IA10 IA12 IA2 IA5 IA9	NIST 800-82 6.16 Access Control DHS CAT: 12.15.11 Permitted Actions without ID or Authentication NIST 800-53: Appendix F-SC: SC-7 Boundary Protection; NIST 800-82: 5.4 Recommended Defense-in-Depth Architecture NIST 800-53: Appendix F-IA; IA-4 Identifier Management NIST 800-53: Appendix F-AC; AC-3 Access enforcement NIST 800-34: 3.2 Conduct the Business impact Analysis NIST 800-82: 5.8 Specific ICS firewall Issues	2.15.11: NIST 800-53r3, AC-14

CONTROLS	AWWA Cross reference	Sub reference
Planning, Contingency Planning, Incident Response IR2	AWWA G430: 4.4 Up-to-date Assessment of Risk DHS CAT: 2.12 Incident Response NIST 800-61R2: Whole document	
Physical/Environmental Protection PE1 PE2 PE8	NIST 800-53: Appendix F-PE; PE-3 Physical Access Control NIST 800-53 Appendix F-PE: PE-5 Access Control for Physical Devices NIST 800-53 Appendix F-CP; CP-8 Telecommunications Services	
Security Assessment and Authorization **Program Management** PM3	NIST 800-53: Appendix F-AU; AU-6 Audit Review, Analysis and Reporting	
System and Service Acquisition SA4	DHS CAT: 2.15.25 Access Control for Mobile Devices NIST 800-34: Executive Summary	

CONTROLS	AWWA Cross reference	Sub reference
System and Communications Protection SC1 SC10 SC12 SC2 SC3 SC4 SC6 SC8	DHS CAT: 2.8.11 Cryptographic Key Establishment and Management NIST 800-82: Specific ICS Firewall Issues NIST800-34: 3.2 Conduct the Business Impact Analysis NIST 800-53: Appendix F-CM; CM-6 Configuration Settings NIST 800-53: Appendix F-AC; AC-17 Remote Access DHS CAT: 2.1`5.16 Passwords NIST 800-82: 5.3.4 Firewall with DMZ between Corporate Network and Control Network NIST 800-53: Appendix F-SI; SI-4 Information system Monitoring NIST 800-82: 5.6 Recommended Firewall Rules for Specific Services DHS DID: 3.1.1 Architectural zones NIST 800-82: 5.2 Logically Separated Control Network	Section 5.8
System and Information Integrity SI3 SI4 SI5	NIST 800-53: Appendix F-IA: IA-5 Authenticator Management NIST 800-53: Appendix F-AU: AU-8 Time Stamps DHS DID: 3.5.1 Log and Event Management NIST 800-53: Appendix F-IA; IA-2 Identification and Authentication	

APPENDIX B: CYBER SECURITY POLICY DOCUMENT FOR MANAGERS

Version 1.0

This is a living document that helps you define how your organization will put in place, periodically review and update your policies and procedures related to cyber security. This policy defines how you intend to protect your organizations personnel and assets, the staff and outside contractors and vendors that are covered by the policy, and the processes you will use to assure compliance and meet your regulatory commitments.

This document was created in consultation with a SCADA system integrator with the express purpose of communicating cyber security needs and processes to decision makers and managers with non-informational technology backgrounds.

Disclaimer

This document is not intended as the sole guide for the implementation of cyber security for utility SCADA systems. Its purpose is to help facilitate the dialogue between utility managers and Information Technology and SCADA integration professionals so that utilities can arrive at the right suite of policies, procedures and technology appropriate to the local circumstance.

COMMENTS

Please provide critique and suggestions to help improve this document.

kash@ksgroupllc.com

TABLE OF CONTENTS

1. GOVERNING BODY

Designate the person or team with responsibility for establishing and overseeing compliance with the security policy. The team would typically consist of person in charge of the utility function, an information technology person and a risk manager to help define the cyber security rules applicable to the use of the system and the system configuration specific to cyber security risk mitigation.

2. CONFIGURATION MANAGEMENT

Limit functionality to reduce vulnerability

The configuration of the SCADA system and components should be based on the principle of "least functionality." Ensure that the SCADA team has conducted a criticality assessment of system components (servers, workstations, network components, application software). Critical components should, in general, have their functionality limited to the monitoring and control functions they are required to perform. Hardware and software elements should be carefully evaluated for need and only allowed to remain when the need is clearly established. These components should also be configured to provide for maximum security without impeding the functionality of the control network.

Disable all ports that are not needed for use by the system to prevent the unauthorized attachment and loading of programs through portable devices such as flash drives.

Control the software installation process

Installation, modification and upgrades of software programs must be restricted to, or supervised by, authorized users typically possessing "Administrator" privileges. All applications to be installed must be pre-approved and the installation process must conducted by an authorized person whose identity is verified through a multi-factor authentication process (see Access Control)

3. ACCESS CONTROL

Identification And Authentication

Each user must be uniquely and positively identified before gaining access.

Prohibit sharing of passwords.

Password administration should require the use of strong passwords. This is an evolving area and the organization must periodically assess its definition of "strong" to stay current with best practice.

Assign a trusted individual (Administrator) as the keeper of passwords. Provide for the ability to reset passwords (either forgotten or expired).

Passwords should be changed frequently. Passwords must not be reused.

Include a challenge/response system to verify user authenticity.

Consider using a multi-factor authentication system – password and a physical token (such as a card) or a biometric system (e.g.; fingerprint reader) for access to sensitive control areas.

Principle Of Least Privilege

Limit users to only those functions they need to execute on the system to meet their assigned tasks. The user sign-on establishes the extent of access allowed.

System design should ensure that ports, protocols and operating system services are also limited in their functionality based on "least privilege." If the system cannot achieve this goal by design, then other appropriate compensating controls must be provided. The local user should not have administrative privileges for the operating system of the workstation that accesses the SCADA control system.

Other

Disconnect the user after a certain idle period and require re-login. This prevents a workstation from remaining unattended. Disable Internet access from the SCADA workstation(s).

4. INTRUSION DETECTION AND INCIDENT REPONSE

An active incident response program must be in place in order to effectively monitor and respond to incidents, discover and handle security alerts and technical vulnerabilities, and collect and analyze security data. Monitoring could be some form of a physical system and/or a software program designed for this purpose.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

Physical Access

Define areas that are openly accessible and areas that are restricted.

Make the area containing the SCADA system a restricted area. Limit access to this area(s) to authorized personnel.

Visitors to the SCADA area should be escorted and monitored.

Access to the area(s) is through an access device such as a key, a combination lock or key card system. On a periodic basis (established in your policy), change combinations and keys/cards.

Maintain logs of every entry to the restricted area(s).

Utility Power

Provide backup electric power to all SCADA components – Servers, Workstations, Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Network Switches – with appropriate Uninterruptible Power Supplies (UPS).

UPS units must receive the proper scheduled maintenance.

The utility should assess the probability and duration of power outages and select the backup-power systems accordingly.

6. ORGANIZATIONAL SECURITY AND INTEGRITY

Audit records are typically maintained by the SCADA system - tracking all actions taken, by whom and when. These records are available for review and must be reviewed on a periodic basis. Track all persons entering and leaving a secure area. The findings and anomalies encountered by the audit should be reported to the governing body.

The unauthorized re-setting of passwords and modification of system audit records can introduce vulnerabilities into the system and must be prevented. The system must be capable of restricting users from installing rogue software programs that can reset passwords and make other unauthorized changes.

7. MOBILE DEVICES

Mobile devices (laptops, tablets, smartphones, removable media (a.k.a. flash drives, thumb drives) and other such devices) represent a significant pathway for introducing unauthorized programs into the SCADA system.

Restrict connections to only those devices controlled by the organization. Enforce these restrictions.

Have a monitoring system in place that reports unauthorized connections. (See "Incident Response" section).

Prevent the automatic execution of code on removable media without direction from an authorized user.

Travel by individuals with an organization-issued mobile device represents a significant risk; issue specially configured devices if such travel is a necessity. Establish and apply measures to mobile devices returning from risky locations to assure that unwanted code is not introduced into the SCADA system.

8. ADDITIONAL SYSTEM AND COMMUNICATIONS PROTECTIONS

Firewalls

The simplest SCADA arrangement is a closed system limited to Human-Machine Interface (HMI) devices and the PLC network. Unfortunately, it is frequently desirable to include the capability to access the system from outside this basic closed loop; users such as maintenance, and management staff may need information generated by the SCADA system for legitimate business purposes. System vendors also often need access to provide support to the system in the form of software upgrades. To facilitate these uses, a special purpose device [17] known as a firewall must be placed within the network to manage access from outside the basic SCADA loop. Firewalls should be properly configured to provide for maximum security without impeding the functionality of the control network.

[17] While usually a discrete piece of computer hardware, a firewall can also be implemented through software directly on a server.

Prevent unauthorized actions

A user has the ability to change set-points within automatic control loops and start and stop equipment remotely. These actions involve communication steps within the SCADA network. Discuss with your integrator/IT professional the methods they will use to manage this communication using IT methods such as "cryptography" and "key/certificate management." The outcome of these discussions should be captured in writing and used as Standard Operating Procedures as the SCADA system evolves.

Track remote access

If your system will need to support access from remote (outside the control room) locations (e.g.; telecommuting staff, off-hours response), ensure that acceptable methods of connecting to the SCADA system have been carefully considered before implementation. View-only access is the preferred method; additional protections must be in place if additional functionality is desirable. All remote access should be subject to monitoring and audit.

9. RESILIENCY

Resiliency is the ability to quickly recover operational control of a water system after a disabling event. Operations staff must possess the ability to take over manual control of the various components of a water system until normal operating modes are restored. A drawback of having a SCADA system in place is that the operations function has a "video-game" feel; hands-on operational skills could atrophy over time or be only minimally present in a new hire.

From a cyber security perspective, back-up devices and protocols must be in place to quickly restore SCADA system components and software. The SCADA integrator must be actively engaged in the process of developing these response protocols.