Manatee County
SCADA Master Plan for the WRFs, Biosolids Dryer, and MRS

SCADA Master Plan

FINAL | May 2020

Manatee County
FLORIDA

Manatee County
SCADA Master Plan for the WRFs, Biosolids Dryer, and MRS

SCADA Master Plan

FINAL | May 2020

Digitally signed by Norman Anderson
Contact Info: Carollo Engineers, Inc.
Date: 2020.05.19 15:40:00-04'00'

NORMAN E. ANDERSON
LICENSE
No 71642
★ ★
★
STATE OF
FLORIDA
PROFESSIONAL ENGINEER

Norman E. Anderson
FL PE 71642

Carollo Engineers, Inc.
CA 8571
301 N. Cattlemen Rd. Suite 302
Sarasota, FL 34232
P: 941-371-9832

Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies.

Contents

Appendices

Tables

Figures

Chapter 1

INITIAL SYSTEM VISIONING

1.1 Introduction

This SCADA Master Plan Report first presents an assessment of Manatee County's existing Supervisory Control and Data Acquisition (SCADA) system for their Water Reclamation Facilities (WRFs), Biosolids Dryer and Master Reuse System (MRS). Secondly, it presents a framework outlining recommended SCADA system upgrades which are developed into specific projects, based upon end user needs, hardware and software functional requirements, and current system deficiencies.

Initial visioning held with the County regarding the general anticipated desired state of the SCADA system along with a high-level SWOT to generate some initial thoughts about the current state of the SCADA system and opportunities for improvement. These initial discussions focused on understanding the goals to allow for optimized and efficient control through the use of the SCADA system, and to empower staff with data. Carollo Engineers obtained input from key staff in each department of the Utility to assess their needs, hardware and software functional requirements, and deficiencies found in the existing SCADA system.

To further determine the County's operational and data access needs, secondary workshops were held where all of the key stakeholder groups involved with plant operations, maintenance, communications & information technology support, and utility management were involved. The goal of these workshops was to gain a thorough understanding of the current day-to-day operations, usage, and accessibility of the existing SCADA system and document the users' future needs.

1.2 Organization Values

The following is a summary of the values the organization that were used as driving factors for decision making as solutions are developed:

- Safety and efficiency.
- Best in Class.
- Stay current and be on the leading edge.
- Provide useful data.
- Be secure.
- Develop a maintainable system.
- Reliability - the system must operate.

Based on these organizational values, the following key themes and concepts were used in determining recommendations and developing projects.

1.2.1 Key Development Themes

Solutions for the SCADA system will look at being efficient and adding value. This means the development of cost-effective solutions that meet the need of utility and not necessarily the best solution at all costs. Additionally, solutions should have an added benefit and not be driven only because it is a want or just because it is standard practice. In this case, recommendations will be made that reduce costs, optimize treatment, are at the technical forefront, increase safety and security, and are highly reliable. Items this will impact will be recommendations related to governance, software and hardware selection, upgrades to systems, and degree of automation.

Additionally, solutions should be clean and consistent and look high end and well thought out. This means that Manatee County equipment and software should be identifiable due to a high level of standardization that provides a consistent look and feel across all hardware and software systems. Items this will impact will include standards, requirements for system replacements and upgrades, and how system data can be used to provide a positive impact for internal users.

Manatee County wants a best in class system that will be highly reliable. Having a modern and current system is a high priority. This will drive the use of newer technologies and tools to enable operations and others to be empowered by the data generated in the SCADA system. System reliability is a key as the system must be operational. This will drive key decisions in system hardware, communications, and system architecture. This also means using proven solutions that are known to work. By following these values, Manatee County can ensure that their vision is met.

1.3 Focus on Standards Development

A critical part of this master planning effort and Manatee County's overall goals is the development of standards to ensure consistency not only in project delivery but in operator experience and operational control methods. The following current obstacles affecting standardization were identified:

- No written standards currently in place.
- Full standards not developed due to different equipment at different sites.
- SCADA Assets are not currently in the Lucity Computerized Maintenance Management System (CMMS).

Despite these obstacles, Manatee County has good consistency of hardware across the utility and continues trying to maintain standards within their system despite not having these documented. Most of their PLCs are the same platform and all their plant systems and related remote systems share are on a CitectSCADA HMI system. Some of the main reasons Manatee County has been able to maintain a reasonable level of standardization are the following:

- Manatee County staff know their preferences and standards and try to ensure these are incorporated into their replacement program.
- The utility does have a documented naming and tagging standard for their new CMMS system.

As standards continue to be developed and documented, the following outlines some of the goals that are hoped to be achieved:

- More control over the SCADA system and better access to its data.
- Additional transparency into system operations and maintenance.
- Consistent operation.
- Consistent calibrations and tracking records.
- Change Management for applications, configurations, and programs.

- Addition of SCADA assets to the CMMS including:
  - Asset hierarchy of PLCs.
  - Incorporation of Battery replacement schedules and other preventive maintenance activities.

1.4 Organization

Within the organization, the Senior Industrial Electrician currently manages the wastewater SCADA system and has staff to help maintain system hardware and software. Currently only specialty projects, large projects that are generally bid to a general contractor, and specific support for the CitectSCADA system and Allen-Bradley PLCs are outsourced. BCI Technologies is currently the preferred vendor and McKim and Creed has provided programming services on numerous projects as well. This is currently working for the County and staff feel as if they are able to complete their necessary work and do not feel overwhelmed or underutilized. The group is staffed sufficiently to handle work in after hours and emergency situations as well.

Currently, there is less control of the work and equipment selections on capital improvement projects (CIP), than there is on rehabilitation and replacement (R&R) projects due to the procurement and review processes. In these cases, generally the consulting engineer and the open procurement process dictate how SCADA system upgrades and additions will be implemented and the types of equipment selected due to the low and open bid nature of the work. County staff are involved in the projects and project planning so their input as well as the IT department's input is considered which does provide a higher level of meeting County requirements and providing more consistent systems.

1.5 SWOT Analysis

An initial Strengths, Weakness, Opportunities, and Threats analysis was performed on the SCADA System. The following outlines the major items in each category:

1.5.1 Strengths

- The system is functional.
- Process are controllable and controlled properly.
- Data is logged and accessible in the system.

1.5.2 Weaknesses

- Reporting and Trending.
- Aging equipment.
- High amount of maintenance.
- Slow to move into smart equipment.

1.5.3 Opportunities

- Ability to incorporate work into other projects.
- Coordination with Electrical Master Plans.
- R&R projects.
- Hach WIMS, new system which does not have a legacy to be maintained.

1.5.4 Threats

- Cybersecurity:
  - Addition of remote access.
  - No USB security.
  - No Anti-virus.
  - No automatic logouts.
  - No use of Active Directory.
- Physical Security:
  - Easy physical access to buildings and critical equipment.
  - Gate issues.
  - Funding issues.
  - No electronic security and limited cameras in place.
- Limited documented policies and procedures.

Performing the SWOT analysis, it is clear that Manatee County's SCADA system is functional and provides the means for monitoring and control that staff need. However, there are major risks to the operation of this system due to not having strong cyber and physical security measures in place as well as documented procedures. In analyzing the different areas of the County's SCADA system, these key areas will be evaluated in order to minimize risk to the SCADA system and utility as a whole.

1.6 Enterprise Software Systems

The following is a summary of other enterprise and business level software systems employed by the County and their use. This section also notes areas where enterprise data exchange could add additional value to the utility.

Table 1.1 Other Systems Used by the County

System	Platform	Use	SCADA Integration
GIS	ESRI Arc GIS	Mapping and documenting linear and reclaim assets	None
CMMS	Lucity	Asset management and work orders	None
LIMS	Hach WIMS	Used to generate DMR Report	Planned integration
Warehouse	ONESolution	Warehousing of parts	None
CIS	Banner	Customer information and billing	None
EO&Ms	SharePoint	SharePoint serves as the repository for Digital EOMs	None
Document Management	OnBase	Management of plans	None

Some of the issues or frustrations with the systems above include the following:

- CMMS not fully implemented so limited assets and reporting functionality.
- OnBase is difficult to use to find plans and paper documents are still used and not organized.
- SharePoint seems to have some good capabilities since EOMs can be accessed anywhere but what happens if a specific location loses communication and cannot access SharePoint.

- No change management or document solution currently in place to backup documents or programs. Still stored on a network drive or laptop.

1.6.1 Data Integration

Currently the County has limited integration with the data in its SCADA system, but would like to leverage this data to a higher degree such as CMMS integration and the development of KPIs. The following ideas were expressed regarding data integration between the SCADA and the CMMS system as a starting point:

- Integrate Runtimes and possibly auto generate work orders.
- Pump changeouts in CMMS drive a reset to runtime counter in SCADA.
- RTDs and Vibration alarms tied to CMMS work orders.

Another major element is the addition of KPIs for higher level management understanding of the efficient operation of the utility. Not only can automating KPIs reduce the effort of manually creating this information but can also provide a more real-time understanding to enable changes to be made to optimize the system. Depending on the KPI functionality, these could be developed in numerous locations or an additional visualization solution may be required. Some of the KPIs of interest were the following:

- Cost related KPIs such as treatment, electrical, and chemical costs.
- Comparison of plants to see demand changes and differences.
- Ability to see best location to store water.
- Network quality information (bandwidth) and communication status.
- Oxygen use and demand and comparison with energy usage and DO.
- Sludge monitoring to determine if over digesting.

In addition, the idea of digitizing and provide more solutions for more information and interaction with operations and maintenance is seen as a necessary path. Adding features to the organization such as a digital logbook and mobile viewing of system status and alarm management are all seen as features that would aid in operations making the organization run better and making operations more effective and reducing employee frustration and fatigue.

1.7 Summary

Manatee County's vision for their SCADA system is to utilize technology to enhance operations and decision making. Manatee County sees a high value in the data produced by the SCADA system and would like to take better advantage of the investment they have made. Some of the keys and core principles in meeting this vision include:

- Implementing best in class systems.
- Standardized solutions and implementations.
- Increased system security.
- Access to data.

Chapter 2
ORGANIZATIONAL AND GOVERNANCE ASSESSMENT

2.1 Introduction

This chapter presents the resources available for providing sustainable, reliable SCADA system support to the Manatee County wastewater system as well as the overall SCADA systems governance strategy. The goals of this chapter are to assess SCADA system governance and associated support personnel and maintenance practices. Main areas of focus for governance include change management, policies, planning, disaster recovery and document management. In addition, this chapter discusses the best ways to match resource requirements with the level of automation required for their facilities and to determine the ongoing support needed to maintain and enhance each system. This chapter also includes specifics on the equipment, systems, and outcomes of the control system and how to best support these control system elements.

Recommendations presented are based on findings from workshops, peer comparisons, County staff interviews, current and planned information technology system infrastructure analysis, Carollo's experience, and industry best practices.

2.2 The SCADA System Organization

Presently, Manatee County has staff dedicated solely to the management and maintenance of the SCADA systems. This group was led by the Senior Industrial Electrician and has been converted to the Utilities Maintenance Supervisor and there are five supporting SCADA-Instrumentation Technicians. The County currently has a very stable group in regards to turnover. Three years ago, staff turnover was much more common. Specifically, the electricians had significantly more turnover 4-5 years ago, which was attributed to having a low wage for this position, but turnover has since been reduced after electrician salaries have been increased. Instrumentation and SCADA position salaries have not increased in recent years but the same levels of turnover have not been seen. The SCADA positions have only existed for about 5-6 years. Generally, electrical staff who have gained SCADA knowledge and training transition into the SCADA-Instrumentation position. Job descriptions related to the SCADA-Instrumentation positions include the following:

- Industrial Control Technician.
- Industrial Electrician.
- SCADA-Instrumentation Technician.
- Utilities Maintenance Supervisor.

Job descriptions for these positions can be found in Appendix A. Currently, the Utilities Maintenance Supervisor position job description does not include any SCADA specific duties or knowledge. The only job descriptions that include SCADA specific knowledge include the Instrument Technician and SCADA-Instrumentation Technician positions. Job descriptions for specific levels within these classifications do not currently exist. It is recommended that the group leader over the SCADA-Instrument Technicians would have the following main duties at a minimum:

- Provides guidance, development and management of the Utility's SCADA systems and staff.
- Manages SCADA system projects and CIP/R&R planning.
- Develops and manages hardware system standards and PLC/HMI programming standards.
- Manages control system cybersecurity and OT/IT coordination.
- Coordinates and provides input during project design and implementation.
- Governs data exchange and system access for process and system data dashboards to the enterprise.
- Manages SCADA system documentation and change management.
- Provides input and feedback to the enterprise applications where required.

The County is working to enhance their personnel management regarding succession planning and career paths and have already taken steps to work with local vocational schools and groups to get more young hires and promote internal staff. Technicians, in general, currently have 4 levels of advancement up to a supervisory position. Electrical and SCADA-Instrumentation personnel have not had formal career levels established as of yet. A draft electrical career path has been established and can be found in Appendix B, a SCADA career path has not yet been established. Human Resources (HR) has the final approval on advancement and career paths but does not develop the initial recommendation. Recommended career paths and their requirements are first developed by individual group leaders and presented to HR for approval. Decisions on placement in the career program are controlled by the County based upon the criteria established in each group's career path. Performance evaluations are conducted annually and are tied to advancement and pay increases.

The current draft Electrical career path top levels are highly tied to obtaining SCADA knowledge and training. This could pose a couple of difficulties for the organization:

1. Difficulties in generating a SCADA career path that looks different than the electrical career path.
2. Difficulty in showing SCADA staff are different than electrical staff.

It is recommended to review these career paths and the Utilities Maintenance Supervisor position title and job description and consider the following modifications:

- Create an electrical career path tied directly to electrical knowledge, experience, licensure, training, certifications, and ability to manage and supervise.
- Create a SCADA career path tied directly to SCADA knowledge, programming ability, design capabilities, network administration, experience, licensure, certifications, and ability to manage and supervise.

- Have a career path migration built into both career paths to allow for transfer of staff at either levels 2 or 3 from electrical to SCADA or vice-versa based on an employee's aptitude, training, and desire to change career paths.

The specific career path requirements and updated job descriptions of the staff in these groups will need to be further defined, but by performing the above tasks they will eliminate the overlap between the different groups in the utility, and better define responsibilities.

Responsibilities of the SCADA-Instrumentation group can then be more tied and coordinated with operations and IT to provide seamless support for all of the technical elements included in the SCADA and Enterprise data information systems. IT will act as the communications and Enterprise system administrator and the SCADA-Instrumentation group, would provide operational application management. Additionally, other organizational changes may be required in order to better delineate these operational groups, the County's current Wastewater Organizational Chart can be found in Appendix C and below are specific organizational subgroups highlighted for further discussion.

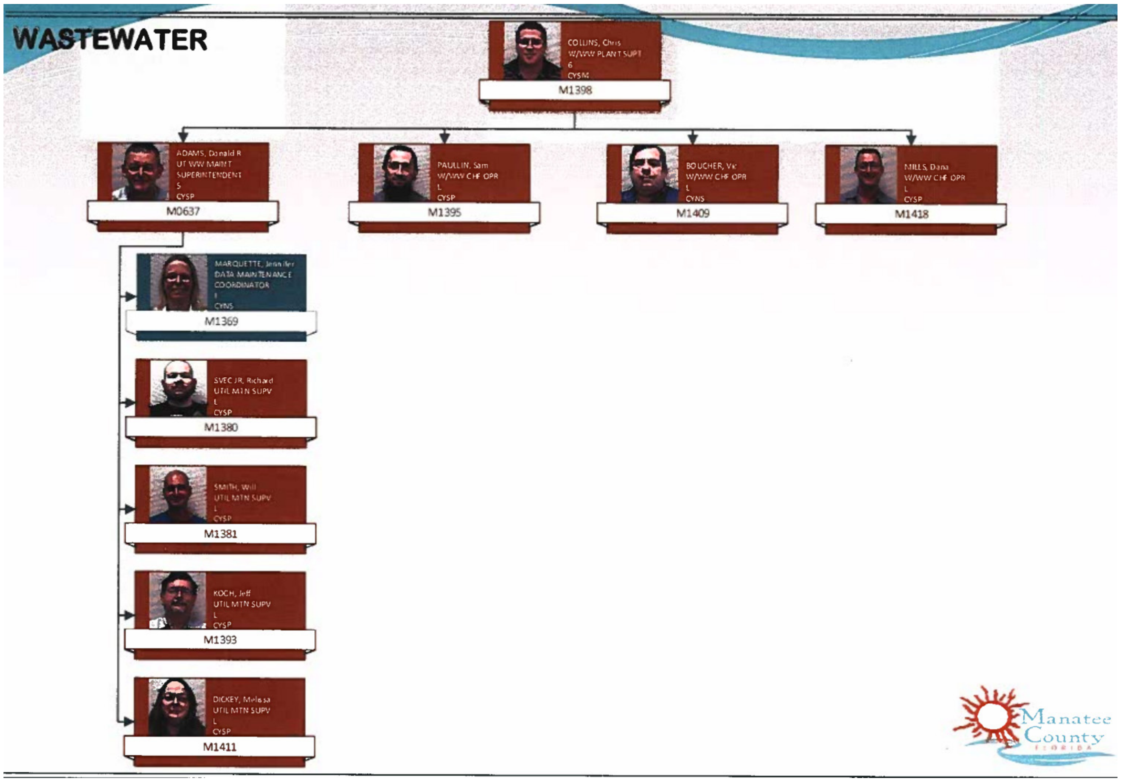


Figure 2.1 Wastewater Organization Chart - Wastewater Plant SCADA

This chart shows the organization of the SCADA group under the Water/Wastewater Plant Superintendent. Additionally, Industrial Electricians also reside under the Utilities Plant Maintenance Supervisors. SCADA staff are also found within the Utilities Superintendent group as shown below.

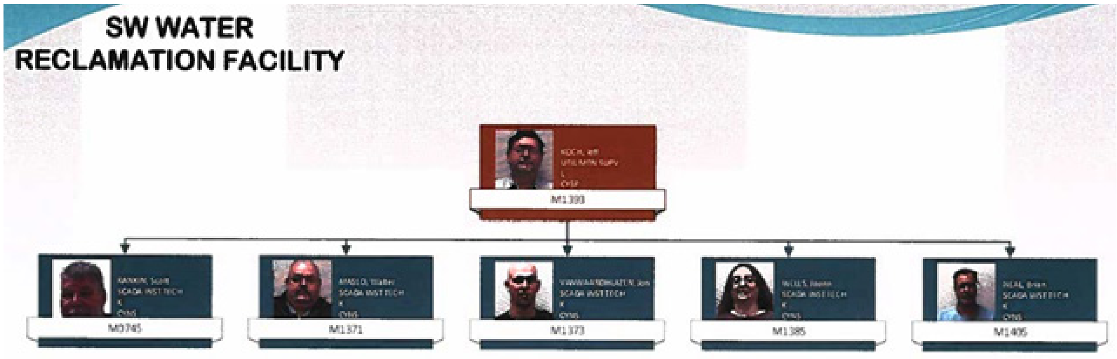


Figure 2.2 Title Group Organization under the Utilities Maintenance Supervisor

Looking at the group organization under the Utilities Superintendent, there are also three SCADA-Instrument Technicians working under a Utilities Maintenance Supervisor. Since SCADA systems generally carry a high cost for software, hardware, and programming, a high degree of savings is generally seen by standardizing these systems to reduce licensing and associated programming software and training costs. Having two separate groups containing SCADA staff could pose the following risks:

1. Duplication of services and systems.
2. Inconsistencies in how SCADA services are provided between groups.
3. Lack of standardization across County utility services.
4. Increased costs.

The best practice would be for SCADA services to be provided from a single coordinated group within a division. In some cases where utility divisions such as water and wastewater services act as completely separate entities there can be difficulties in coordination but for services provided for a single division, it is best if these services can be provided from a single group. The following are the recommendations to coordinate these staff:

- Coordinate all SCADA-Instrumentation staff under the Utilities Maintenance Supervisor position.
- If staff are in SCADA-Instrumentation positions due to advancement and not job duty, then the new Electrical career path should be implemented, and staff assigned to the appropriate higher level Industrial Electrician Position.
- If staff are truly performing SCADA-Instrumentation duties, then they should be re-assigned under the Utilities Maintenance Supervisor.

Having a coordinated group will ensure SCADA system work is performed consistently and reduce the risk of systems potentially interfering with each other. Similarly to how IT departments provide services for multiple other departments under one group in order to leverage staff and equipment across an enterprise, the SCADA system is no different in order to minimize costs and maintain a high degree of reliability. This should also help in clearly defining work responsibilities and identifying qualified personnel for each task. The County has already noted that they have had calibration issues resulting from a technician working on the piece of equipment and not being qualified for that work. By clearly defining group and individual job responsibilities more clearly these types of situations would be minimized or eliminated.

To support this single coordinated group, increased SCADA system governance in the form of increased standardization, standard work order procedures and policies, and standardized equipment across all utility divisions including water, wastewater, and lift stations would be beneficial. This overall increase in standardization would reduce spare part requirements, training needs, and software licensing creating an overall simpler and lower cost system. As the system becomes more and more standardized and maintenance more coordinated, the consistency and quality of maintenance will increase as well.

A big success of the SCADA group is that staff have the adequate tools and responsibility to perform their work and have the funding they need to get the necessary equipment to perform their jobs. This in turn has led to a high degree of job satisfaction and reduced employee stress. This is likely a factor in staff retainage even during times of minimal pay increase. Additionally, the staffing levels within the group appear to be adequate. Staff do not feel overwhelmed with tasks that must be completed immediately, but have a sufficient backlog of work that can be completed progressively. Besides an update to staff job descriptions and potential organizational changes, the SCADA-Instrumentation group has adequate staffing and tools to support the utility as required to maintain required level of operations.

2.3 SCADA System Governance

SCADA System governance encompasses management and operation of the entire SCADA system and generally encompasses the following key areas:

- SCADA Organization.
- Policy and Procedure Management.
- Document Control Policies.
- Change Management Procedures.
- Work Order Policies.

The establishment of a Governance policy will set the rules for both internal staff and outside vendors and contractors to ensure consistency even when staffing is variable. The objectives of having a governance policy are the following:

- Availability – Staff and procedures in place to ensure systems are operational.
- Accountability – Justification of actions and decisions.
- Compliance – Changes and modifications are reviewed, tested, and documented.
- Standardization – All work and systems executed similarly.

The starting point in obtaining system governance is to create a SCADA/ICS governance committee. The SCADA/ICS governance committee is responsible for developing, reviewing, and approving new Utility Technical Services group policies as well as updating the general governance policy. Members of this team should be stakeholders of the SCADA system such as those who use and maintain the system as well as management staff capable of enacting policies and driving change. For Manatee County, this committee will include a representative from each of the following departments:

1. Wastewater Management Representative.
2. Water Management Representative.
3. Wastewater Operations Representative.
4. Water Operations Representative.

5. Utility Business Group Management Representative.
6. IT Representative.
7. Utilities Maintenance Supervisor.

Additionally, key members with the Utility operations and maintenance group along with management that is able to drive policy and decision making are key to ensure all utility stakeholders are represented and have the authority to make changes to the organization. An additional function of the SCADA governance committee is to recommend and prioritize SCADA system projects and initiatives and to ensure that all SCADA related efforts are properly coordinated with other utility projects. This group will also work to remove obstacles between the SCADA-Instrumentation group and county wide departments and address staffing issues. It is recommended that the governance committee meets on a quarterly basis in order to discuss the current status of policies, staffing, and projects.

The County has not yet established SCADA governance policies or a specific disaster recovery plan. The County does have an existing emergency response plan but it does not sufficiently cover emergency response related to control system or cybersecurity issues of the utility. The County has fortunately had few emergency issues due to the robustness and redundancy in their water and wastewater systems, however, the utility should ensure they remain prepared. Additionally, the new America's Water Infrastructure Act (AWIA) lays out new requirements for addressing all hazards of water and wastewater utilities including those affecting SCADA operations, cybersecurity, and physical security. The AWIA requirement is comprised of two parts:

- All Hazards Risk and Vulnerability Assessment.
- Emergency Response Plan (mitigation report).

The current guidance to meet these requirements consists of compliance with the AWWA G430, J100, and G300 standards along with the NIST Cybersecurity Framework for the risk and vulnerability assessment portion and AWWA G440 for Emergency Preparedness. The linkage of these guiding documents is shown in the following figure:

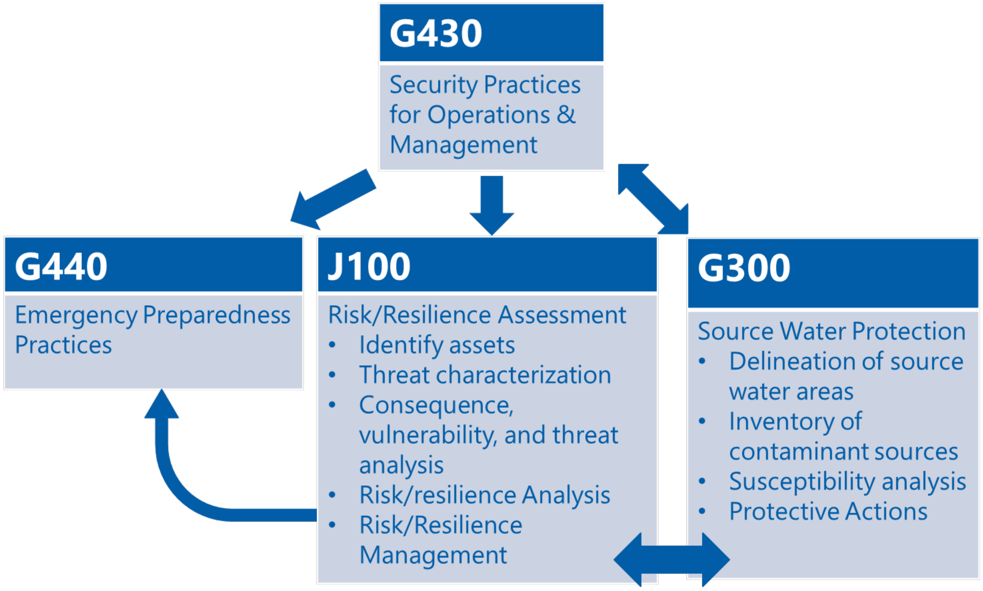

G430
Security Practices for Operations & Management
G440
Emergency Preparedness Practices
J100
Risk/Resilience Assessment
• Identify assets
• Threat characterization
• Consequence, vulnerability, and threat analysis
• Risk/resilience Analysis
• Risk/Resilience Management
G300
Source Water Protection
• Delineation of source water areas
• Inventory of contaminant sources
• Susceptibility analysis
• Protective Actions

Figure 2.3 Linkage of Guiding Documents

The requirements for completing this work are outlined in the following table:

Table 2.1 Requirements for Completing Work

Utility Size	Risk and Resilience Assessment	Emergency Response Plan
>100K	March 31, 2020	September 30, 2020
50k to 100k	December 31, 2020	June 30, 2021
3.3k to 50k	June 30, 2021	December 30, 2021

2.3.1 SCADA Organization

Manatee County currently has a SCADA organization that is suitable to meet the needs of its operation. While this group cannot handle 100 percent of the work internally, the balance can be handled by outside contractors and the County's risk of having no support in times of emergency need are mitigated. As noted previously, the job duties and career path of SCADA-Instrumentation technicians and Industrial Electricians along with duplication of SCADA-Instrumentation staff within the organization provide duplication of services and an unclear delineation of responsibility. The County is in the process of correcting these items with the development of the Utilities Maintenance Supervisor role in the organization and modifications to the organizational structure and responsibilities of staff.

Key areas of organizational governance that will need to be addressed for a successful SCADA-Instrumentation group implementation include the following:

- Implementation of a career path to assist in continued staff retention
  - Currently the SCADA/Electrical staff do not have a ladder program where other staff do.
- Development of a training program and budget.
- Development of staff performance metrics.
- Development of staff retention statistics and other suitable staff and group KPIs.

Due to having dedicated resources for SCADA implementation the following outlines the current status of completing SCADA related work:

- All work is being completed to keep the SCADA system operational even though maintenance requirements are high.
- System is functional, online, and meets permit requirements.
- Upgrades are being completed using both internal and external support.
- The SCADA system and related process operation is not being expanded upon to enhance treatment quality or efficiency.

The County is finding that having dedicated internal staff with a vested interest in the operation of the SCADA system, they are able to have the support they need to effectively maintain their existing control system.

2.3.2 Policy and Procedure Management

SCADA policies and procedures should be managed and maintained by the SCADA-Instrumentation group supervisor and reviewed periodically by the SCADA governance committee generally on an annual basis. Policies should be created by SCADA governance committee members and approved by the committee. Procedures can be developed by a SCADA-Instrumentation group member and approved by the SCADA-Instrumentation supervisor. Procedures should also be reviewed annually by the SCADA-Instrumentation supervisor to verify they are still applicable and remain updated with current practices and technology.

Currently, there are no formal SCADA policies or procedures. Some work in asset management and standard operating procedure development is starting as part of the Lucity computerized maintenance management system (CMMS) implementation project. The addition of standards, specifications, and contractor work requirements would greatly increase the consistency of project delivery and provide the County with a method to enforce quality among contractors and ensure consistency of delivery across the organization. The county has recently submitted a RFP to standardize on support and implementation providers. Standards should continue to be expanded and developed so that as the County undergoes upgrades to its PLC and HMI system and enters into the execution of the phase of the SCADA Master Plan then these standards can be used to ensure consistency across all facilities. These standards should be continually reviewed and expanded to account for updated system components and model numbers, updated software versions, and to include programming and graphical standards as these systems are developed and expanded.

Forms and checklists for various staff activities exist and are located on a network drive. The drive does have an organization and forms stay in a logical order in this location. While the system is working and is organized, it does not provide a method of version logging of forms or tracking changes to documents to ensure validation of data and management of document changes. It is recommended to migrate these forms and checklists into a system that can provide document management such as the CMMS system depending on how the forms and checklists are used. The CMMS system is widely accessible and already used by staff for other purposes and would be the logical place for these forms and checklists to reside. In some cases, forms and checklists may be associated with other SOPs and Work Orders within the CMMS system which would further aid in staff use. A set file naming structure must be identified and documented within document management policies to ensure naming is consistent to help readily identify, find, and search documentation.

Policies do exist for defining and executing purchases of all amounts but not necessarily for defining what constitutes a project. Public administrative codes define purchasing types mostly based on cost and this information is documented within the County BoCC Administrative Standards and Procedures Manual under Procedure number 501.00 for the Manatee County Purchasing Division. Within this structure there are five categories of purchases based on cost. Categories start at $5,000 and below and go up until category 5 which is purchase of over $1M. Purchasing has the ability to authorize purchases of up to $250,000 depending on internal policies and requirements and purchase over $250,000 require a bid process. Due to the bid process threshold of $250,000 this is generally viewed as the threshold for project definition. After the project threshold is reached, it follows the following process:

- County develops a scope.
- Scope is provided to the County's Engineer of Record (EOR) for design, construction, and internal staff resource estimating.
- Project is then categorized as CIP or R&R.
- CIP projects are then submitted as part of the budget for approval. R&R projects may have less restrictions due to need for keeping existing systems operational.

- Once approved, project goes to BoCC for adoption.
- Project can then be executed as scheduled and funded.

The County's IT department has a formalized TAG process for projects, but there is a need for improved coordination between utilities and IT as IT is often unaware of projects on the water/wastewater side until late in the project execution process. While efforts have been made to include IT to a higher degree, work is still being done that impacts IT without their knowledge. Some of these issues could be resolved through formal governance committee meetings to review all utility projects on a quarterly basis. In addition, the Utility business group serves as the liaison with IT. In any respect, projects, especially those containing SCADA and communications upgrades, should be submitted to the IT TAG process early in the planning phases to ensure the IT department is brought in as stakeholders and are prepared to support projects.

2.3.3 Document Control Policies

No formal document control policy is in place. Staff mostly retain documents individually based upon their own methods regardless of document type or format with the exception of EOMs and forms and checklists. The main documents which require formal documentation control policies are the following:

- Drawings and O&M.
- Application Programs.
- Policies and Procedures.
- Communication Network Drawings.
- Forms and Checklists.
- Financial Documents.
- Training.

For the most part, it seems that most of the forms and checklists are stored and organized in a County network drive directory. Drawings and O&Ms are mainly digital documents as the County has developed most electronic O&M manuals (EOMs) and have these stored on their SharePoint site. While this documentation is stored well and accessible, there are concerns over its availability if there were a network or internet outage. Additionally, there are no formal procedures for updating EOM information such as drawing redlines. For control systems, this often means that changes to control panels are either not documented or redlines are only contained within the drawings inside of the enclosure door.

Currently Application Programs are stored by each individual who performs a change and they are responsible for where to store a backup copy outside of the copy stored on the associated controller or server. Currently, there are no formal procedures in place and mistakes have been made where modified applications were overwritten by others making subsequent changes on an older version of the application. A formalized change management procedure is necessary for these types of changes in the system and this can be aided by software solutions.

This is very similar for communication network drawings. These drawings are critical for troubleshooting and understanding critical communication pathways and are necessary for implementing disaster recovery procedures. The County had network drawings produced as a part of Phase 1 of the master planning process. Since this time, the County has continued to make changes to their network architecture and have not always kept up with the revisions to these drawings as a standard method for versioning revisions, storing documents, and validating the accuracy of these drawings does not exist. As work is completed and items are revised, the associated documentation also needs to be revised. Creating procedures and including these on forms and checklists within the CMMS to update drawings on modifications and then having these changes reviewed and approved by supervisor should be added to the standard workflow. Having the appropriate EOM information tied to assets within the CMMS system would aid in streamlining this process.

Other documents such as training information, and training records are also limited due to not having a formal documentation procedure. As groups continue to add career paths, this documentation will be increasingly important to verify promotions and level advancement within the organization. Developing a common and consistent set of document management procedures is critical to ensure that all organizational data is stored correctly and is able to be accessed for all aspects of the SCADA-Instrumentation group.

2.3.4 Change Management Procedures and Work Order System

Task assignment and system changes are currently tracked through Work Orders. Work order policies and the existing maintenance approaches are working well but have room for improvement. Presently, operators put in requests for changes using the work order process. Requests currently go through senior level personnel for approval and assignment. The County noted possible improvements with regards to change management and identifying the appropriate people to make hardware and software changes. Additionally, some changes are small but still require high level approval which can delay the time it takes to implement these requests and can lead to inefficiencies. A positive aspect of the system is that changes are tracked through the CMMS system so that reports can be generated to see the work completed on the SCADA system. However, additional change management procedures or revision tracking is needed for programming changes, especially for changes made in one plant that could benefit other plants. This could also be aided by the use of global functions, standard Citect objects known as genies, and documented programming standards and procedures that would assist in changes that are common among system to be globally changed instead of locally changed.

After hours or in an emergency, any required changes are made and documented. Work Orders from operations personnel must be approved by a supervisor, but it is difficult to track past Work Orders. The County is aware of this difficulty and taking steps to address it.

Currently the County does not have change management procedures in place for any of the following:

- Drawings.
- Application Programs.
- Assets not in the asset management system.

For assets that are in the asset management system, change management is administered through the Lucity work order system but this system currently has limited assets in its current deployment. This system is currently being developed utilizing a standard tag naming scheme and standard templates which should be coordinated with the equipment model within the CitectSCADA system. The following is the general workflow for work orders within this system:

- A request is issued.
- Request is sent to supervisor.
- A work order is generated.

- Work order is assigned to staff.
- Staff completes work.
- Supervisor checks work and closes out work order.

Limited SCADA assets are in the work order system leading to minimal change management and tracking of changes within this system. Additionally, application programs are not versioned or commented appropriately by integrators to note changes made in some instances. This has led to staff overwriting changes using an older version of an application of which they have modified causing unintended system operation that operations staff has had to troubleshoot.

SCADA system integrators are also not tracked in the work order system. A history of the work that integrators have completed and changes they have made is then not available for review. This can make future troubleshooting difficult and also limits visibility into the work that integrators have completed and in determining continual issues within the SCADA system that may require upgrades or replacements rather than continuing maintenance corrections. To start, integrators performing maintenance functions should follow the same work order process as County staff so that the work they do can be similarly assigned by Supervisors, checked and tested, and work order closed out and logged. This will also provide the County more insight into the requirements and level of effort of work required to be completed by future internal staff.

2.4 Common Themes and Gaps

Resource planning requires an understanding of the level of automation required, end-user requirements, gaps, common themes, risks, and relationships with other essential support areas such as Information Technology (IT) teams.

For this Master Plan, strategic visioning and governance workshops were held to review management, supervisors, and key support staff expectations and requirements for control systems. Workshop objectives included determining the facility level of automation and evaluating the risk and vulnerability of the existing SCADA systems, current planned expansions and expectations, common themes, and a generalized gap analysis.

Discussions focused on the organization, general system governance and policies, and project planning. Through the workshop and assessment process, gaps were found in the governance policies and procedures. The workshop outcomes identified common themes and gaps.

For this review, the SCADA system was defined to include the following related components:

- The Process Control System (PCS) and Computer Control System (CCS) associated with the wastewater treatment system along with related control system software.
- Individual PLC-based controllers that report to the SCADA system.
- In-plant control system local area network (LAN).
- Inter-facility communications networks.
- Wireless communication system to remote stations.

2.4.1 Level of Automation

The present level of automation (LOA) for the wastewater treatment system was discussed in the workshops. Understanding the control system expectations was necessary to complete an assessment and provide recommendations.

Staff indicated that the present control system LOA at the plants and remote sites was mostly "Automated Control with Alarm Response". Going forward, the treatment facilities are striving to implement "process response" for key process areas such as digestion or aeration control in order to optimize process operations. Management strives for better Key Performance Indicators (KPIs) and "business system links" but recognizes this lofty goal is years away. There is also an understanding that the data the SCADA system produces can be empowering and that more people in the utility need access to the information.

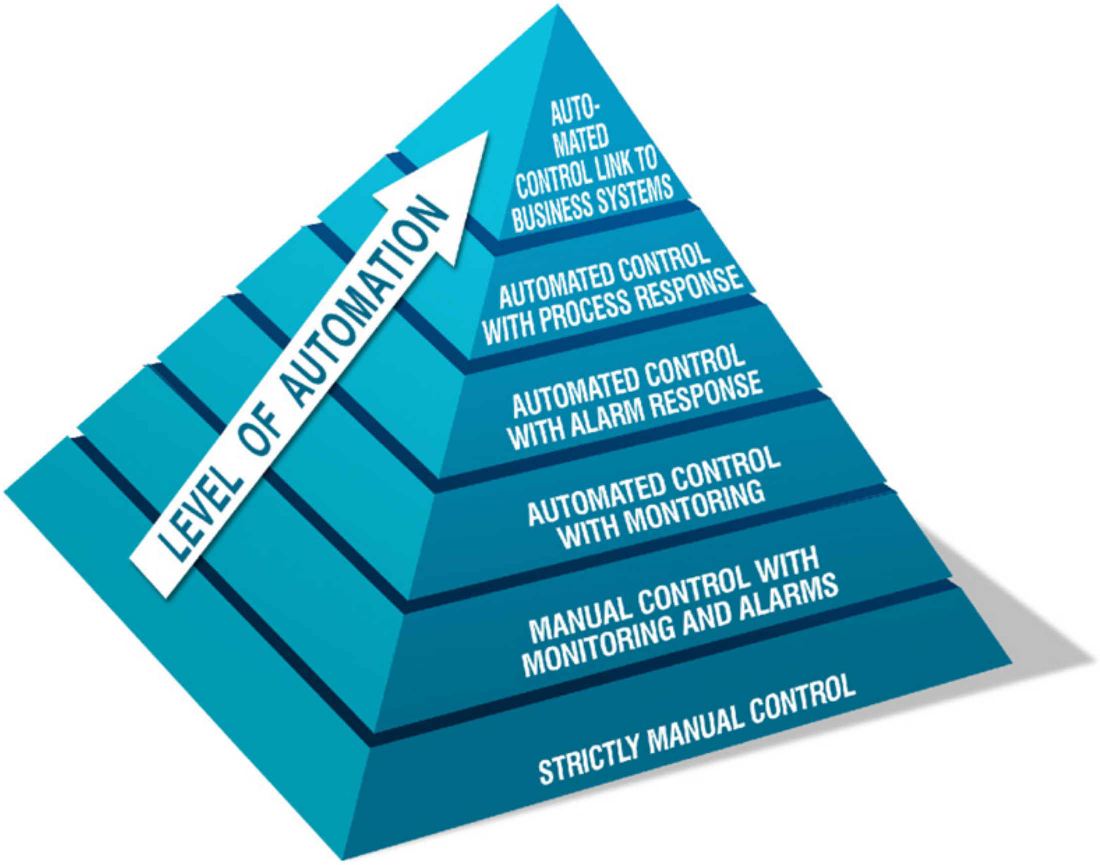


Figure 2.4 Level of Automation

2.4.2 Common Themes: Workshops, Meetings, and Interviews

Common themes were developed from survey, workshops, meetings, and interviews and include the following:

- Internal staff can sufficiently support the system and have the resources they need.
- Documentation of system standards and procedures has not been developed, but the value of this documentation is understood.
- IT is engaged and supports backhaul communication networks and security.
- Control system and network objectives include a secure, streamlined, and efficient SCADA system applied consistently across the County's facilities.
- Additional network security is needed.
- Additional physical security is needed.
- PLC systems need to be updated.

2.4.3 Resource Planning Gaps

Gaps were identified for resource planning which include the following:

- SCADA support staff career paths and training need to be established. Additionally, clearly defined job duties need to be established.
- Increased cooperation and defined responsibilities needs to be established with the IT department to ensure Operational Technology (OT) systems are reliable and secure. If IT cannot dedicate the necessary resources, then service level agreements (SLAs) may be required.
- An approach to standardizing components commensurate with procurement rules in order to minimize maintenance and learning/training requirements is critical.
- Information on system needs and requirements must be included in the specs and drawings. This will result in a final product that meets OT, Maintenance, and IT expectations.
- More needs to be done with system data. Data needs to be made more accessible, decisions need to be made on what data is necessary for key decisions, and key performance indicators need to be developed.
- Maintenance functions are made more difficult due to lack of quality documentation and procedures.

2.4.4 Identified Risks

Staff identified vulnerability issues and risks, which were included when assessing the network topology, sustainability, reliability, performance, and security. The risks were identified during the internal standards philosophy review and implementation. Approaches to minimizing these risks include:

- Provide procedures to manage the system long-term.
- Provide an approach for change management.
- Increase system security through protection from natural disasters, outside threats, and cybersecurity threats.
- Consider the vulnerability of existing SCADA system sustainability during design for any current planned improvements, replacements, and/or expansions.
- Increase reliability of in-plant communication system through redundant and updated fiber optic cabling.

2.5 Summary of Current Performance

- Sufficient staff and funding to maintain SCADA system operations.
- No formal governance program.
- No formal written standard, specifications, or operating procedures.
- No formal change management for application programs.
- Work order system in place.
- SCADA-Instrumentation Technicians not all part of the same group.

2.6 Best Practices

- Formal and comprehensive governance policies and procedures.
- Job descriptions exactly matching job functions.
- Change management systems in place.
- All documentation stored and easy to find and revise.
- SCADA staff managed as a cohesive unit.
- Staff levels adequate and funded appropriately.

2.7 Initial Recommendations for Assessment

Based upon the information obtained, the following is a listing of initial system recommendations:

- Create SCADA and Electrical career ladders and update job descriptions to match ladder positions and job duties.
- Re-organize SCADA-Instrumentation staff within the organization and determine overlap with water.
- Implement a governance program.
- Develop a governance team of stakeholders.
- Mitigate governance gaps through procedures and technology where appropriate.

Chapter 3
PLC AND HARDWARE ASSESSMENT

3.1 Introduction

This chapter includes information on the County's existing PLC and Hardware systems used for automation within the wastewater treatment systems. As part of the work for this section, equipment inventories developed in a previous planning phase were reviewed and an assessment completed on the County's existing SCADA hardware. Information on the previous assessment are included in the Appendix.

Recommendations presented are based on findings from workshops, peer comparisons, County staff interviews, current and planned information technology system infrastructure analysis, Carollo's experience, and industry best practices. The following sections provide background information of the present state of the County's SCADA PLC and Hardware systems along with recommendations for improvements to meet industry best practices.

3.1.1 Organization Values

The following is a summary of the values the organization would like to be considered as solutions are developed:

- Redundancy and Reliability.
- Cost.
- Ease of Maintenance.
- Development of Standards.

3.2 Existing Equipment

Existing equipment was inventoried during phase 1A of the master plan project. The existing instrumentation, SCADA hardware, control panel components, and physical security components were evaluated to identify specific areas of improvement and input from the County's operational and management staff were obtained in a targeted stakeholder workshop. In general, most systems are performing adequately to maintain reliable automated system operation. A common theme throughout the assessment was the desire to standardize on instrument manufacturers to reduce maintenance efforts and to reduce the time spent training new employees, as well as the number of different types of spare components in storage.

Hardware is evaluated against the manufacturer's current end of life cycle and current product models and revisions in order to determine if hardware is still supported, has an available and suitable replacement, or requires a migration to new hardware at this time based upon manufacturer's product support. Hardware is additionally evaluated based on evidence of corrosion, poor installation, and suitability to perform required functions. In some cases, new hardware may be proposed based upon new features that would solve current issues that the County is having or provide additional functionality or standardization desired by the County.

A typical product lifecycle status is shown below and used in the following sections to evaluate hardware lifecycle status.

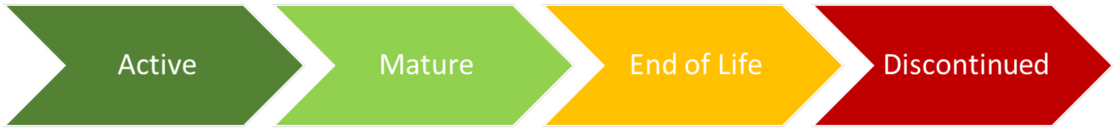


Figure 3.1 Lifecycle Status

- Active: Current offering with full support and replacement availability.
- Mature: Product still fully supported but new product exists. Consider migrating if installed product fails or is in need of replacement.
- End of Life: Discontinued date announced and may no longer be available. Plan for migration to new product.
- Discontinued: Product no longer manufactured and limited support.

Currently, no written standards or specifications exist for any SCADA system components, but staff have their preferences that are known. The County is satisfied with the performance of the existing Allen-Bradley PLCs and have started moving towards the newer CompactLogix line as the existing SLC Series PLCs are past their end-of-life date and no longer supported by the manufacturer. There was overall agreement that physical security systems were lacking and needed to be addressed. In general, significant progress can be made with regards to standardization and redundancy of all hardware systems.

3.3 Existing Instrumentation

Manatee County's existing instrumentation standards are presently not documented. Existing instrumentation was provided through multiple construction projects leading to a variety of manufacturers and varying measurement technologies depending on the application and facility. The County typically uses ABB or Endress & Hauser magnetic flow meters across the plant. Operations personnel are familiar with the maintenance and troubleshooting required for these flow meters. Pressure transmitters are fairly standardized on Rosemount at most facilities, and the County also prefers Endress & Hauser. The County has an idea of the instrument manufacturers on which they would like to standardize and a strong desire to move towards standardized instrumentation across the plants to ease maintenance and reduce the additional training required when technicians rotate. The County has a clear desire to move toward a specific manufacturer and technology for each type of instrument, and they have already begun to standardize with regards to pressure and flow transmitters. The following table outlines some of the initial instrument types and proposed standard manufacturers where they are known.

Table 3.1 Initial Instrument Types and Proposed Standard Manufacturers

Field Instrument	Application	Manufacturers
Ultrasonic Level Transmitter	Liquid Level. Non-contacting	Endress and Hauser Siemens/Milltronics
Hydrostatic Pressure Level Transmitter	Liquid Level. Submerged.	Endress and Hauser
Radar Level Transmitter	Liquid Level. Non-contacting	
Chlorine Analyzer	Total or Residual Chlorine	Severn Trent CL500
Turbidity Analyzer	Online low range turbidity analysis. Offline sample stream.	Hach 1720E, sc200 SWAN Analytical
pH Analyzer	Liquid pH	Hach
ORP Analyzer	Oxidation Reduction Potential	Honeywell
Thermal Mass Flow Meter	Gas Flow Measurement	Kurz FCI
Flow Switch	Pump flow and no-flow status indication. Uses thermal mass flow technology at fixed setpoint.	
Temperature Transmitter	Temperature measurement of liquid or gas in process.	
Ammonia Analyzer	Free Ammonia	
Phosphate Analyzer		
Nitrate Analyzer		
Float Switches	Discrete HIGH and HIGH Level Alarm. Counterweighted non-Mercury type.	Anchor Scientific
Pressure Transmitter	Liquid and Gas Pressure Measurement	Rosemount Endress and Hauser
Piston/ Diaphragm-Activated Pressure Switches	Liquid and Gas Pressure Alarm. Use in lieu of Bourdon-tube and bellows-type switches.	Ashcroft
Pressure Gauges	Liquid and Gas Pressure Indication. Glycerin filled for corrosion protection and limited surge protection. Use Bourdon-tube elements. Diaphragm or bellows elements may be required for low ranges.	Ashcroft
Electromagnetic Flow Meters	Liquid Flow Measurement. Use pulsed DC excitation. Liners: Polyurethane or Epoxy.	Endress and Hauser ABB
Pump Check Valve Limit Switch	Pump Flow and No-Flow Status Indication. Use switches securely mounted on valve bodies to provide reliable, low-maintenance operation.	Provided by valve manufacturer

3.3.1 Instrumentation and Maintenance Challenges

The majority of instrumentation operates well and are well maintained. The County calibrates their analytical compliance instruments and analyzers on a monthly basis and flow meters on a yearly basis. The County has had issues with calibrations and accuracy on their existing chlorine analyzers and dissolved oxygen analyzers. Input from staff identified that maintenance of some of the existing analyzers can seem unreliable because of analyzer drift and inaccuracies when compared to measurements taken from samples. Part of this issue is due to not having a standard calibration method that all staff use as well as the number of different analyzers having different calibration methods. Additionally, the training provided by Contractors in the past was too rapid and not adequate to fully train all staff on how instruments operate and are calibrated.

As noted in Chapter 2, the addition of stronger governance policies and procedures regarding instrument calibration would be beneficial to ensure a standard calibration method and repeatable calibration results. The County currently has a calibration program in place, and this would just be an addition to that program. Additionally, training on specific instruments should be provided to staff and the training logged in employee records to verify staff have received the necessary training on each instrument in the system.

3.4 Existing SCADA Hardware, UPS, Control Panel Components

Carollo completed a hardware analysis of the existing PLCs, UPS, Ethernet switches, and miscellaneous communications components in the County's SCADA system. Detailed component information from the previous analysis can be found in the appendix. As seen in the table below, approximately half of the County's currently installed PLCs are the Allen-Bradley SLC platform with the majority of the remaining being either the Allen-Bradley MicroLogix or CompactLogix platforms. Allen-Bradley has recently announced that their SLC platform has been discontinued and is no longer in production or sale. This puts the County at risk of not being able to find spare parts in the case of failures. The majority of MicroLogix PLCs installed are the series 1000 or 1100 which are currently mature products and reaching the end of their lifecycle status. The County does have a few 1400 series controllers that are still in the Active status. The CompactLogix platforms are still fully supported and continue to be upgraded with new features and functionality. Allen-Bradley does recommend migration from the SLC platform to the CompactLogix 5370 or 5380 series controllers which is what the County has currently standardized on. Based on the current install base, over 80% of the currently installed PLCs are at the mature or end of life status.

Table 3.2 Existing PLC Platforms

Controller	QTY	Lifecycle Status	Percentage
SLC	39	End of Life	50.6%
CompactLogix	7	Active	9.1%
MicroLogix (1000/1100)	28	Mature	36.4%
Other	3		3.9%
Total	**77**		

Ethernet switches at the County facilities are a mixture of managed and unmanaged switches. The majority of switches in service are manufactured by Phoenix Contact. The best practice would be for all switches to be of similar model, have layer 2 management features, and have compatibility for in-plant fiber optic ring topologies. Many switches in the system have also been in service for many years and in need of replacement to prevent failures and to leverage features of modern equipment. The following table summarizes the major switch types discovered during the Phase 1 Master Plan evaluation. The majority of existing switches are Phoenix Contact managed and unmanaged versions along with a variety of other manufacturers such as 3COM, Netgear, Allen-Bradley, and N-Tron among others.

Table 3.3 Major Ethernet Switch Types

Manufacturer	QTY	Percentage
Phoenix Contact	27	69%
Other	12	31%
Total	**39**	

Currently, many of the Ethernet switches are unmanaged. These are plug-and-play devices that do not provide any control of where the information is being sent. Therefore, they can greatly slow down the speed of the data being sent and possibly create broadcast storms that negatively impact the response of the network. It is recommended to replace all unmanaged switches with managed Rockwell Stratix switches. Utilizing managed switches allows for IGMP Snooping to be enabled which allows data to be sent only to the intended destination therefore optimizing the network bandwidth. Managed switches also optimize the performance of full-duplex mode which allows for messages to be both sent and received concurrently. The Plant Floor Switches should be replaced with the Rockwell Stratix 5700 series. These switches support the spanning tree protocol that provides the County desired resiliency and these switches are industrial rated and suitable for control panel mounting. Stratix switches also have higher level integration with CompactLogix controllers providing direct monitoring of the switches through pre-built add on instructions. Additionally, as Rockwell continues to embed security into their hardware, these devices will allow for direct implementation of these security features.

The County utilizes 120Vac UPS for their control panels and computer components. UPS are generally installed inside of each major control panel and equipment rack or cabinet. In general, the UPS are well maintained, and batteries are replaced based on a schedule. About half of all the currently installed UPS systems are manufactured by APC of Schneider-Electric and this is the County's standard UPS manufacturer.

Table 3.4 Uninterruptible Power Supply Inventory

Manufacturer	QTY	Percentage
Eaton	9	16%
APC	29	51%
Tripp-Lite	8	14%
Other	11	19%
Total	**57**	

Having a mixture of UPS creates some maintenance inefficiencies and the plants would benefit from standardization. The suggested equipment to standardize on is the Schneider Electric APC platform without maintenance bypass switches. These UPS provided with monitoring cards allow for monitoring of useful information in order to predict maintenance and operating status. It is recommended to provide UPS with Ethernet capable monitoring cards and integrate into the control system for notification of UPS errors and general monitoring. The APC platform UPS allow for monitoring of battery failure notification which provides early-warning fault analysis enabling timely preventive maintenance. They can also operate in an ECO mode that by-passes unused electrical components in good power condition to achieve high operating efficiency without sacrificing protection. These UPS also have LCD graphics display in which text and graphical display modes of operation, system parameters and alarms are easy to view. These UPS are also easily convertible between rack and towers mounting which allows for simple migration for installation condition and further standardization of components. Additional benefits to the County would be automatic self-test: Periodic battery self-test ensures early detection of a battery that needs to be replaced. Predictive failure notification: provides early-warning fault analysis ensuring proactive component replacement. User-replaceable batteries: Increases availability by allowing a trained user to perform upgrades and replacements of the batteries reducing Mean Time to Repair (MTTR). Disconnected battery notification: Warns when a battery is not available to provide backup power. Audible alarms: Provides notification of changing utility power and UPS power conditions. Scalable runtime: Allows additional run time to be quickly added as needed

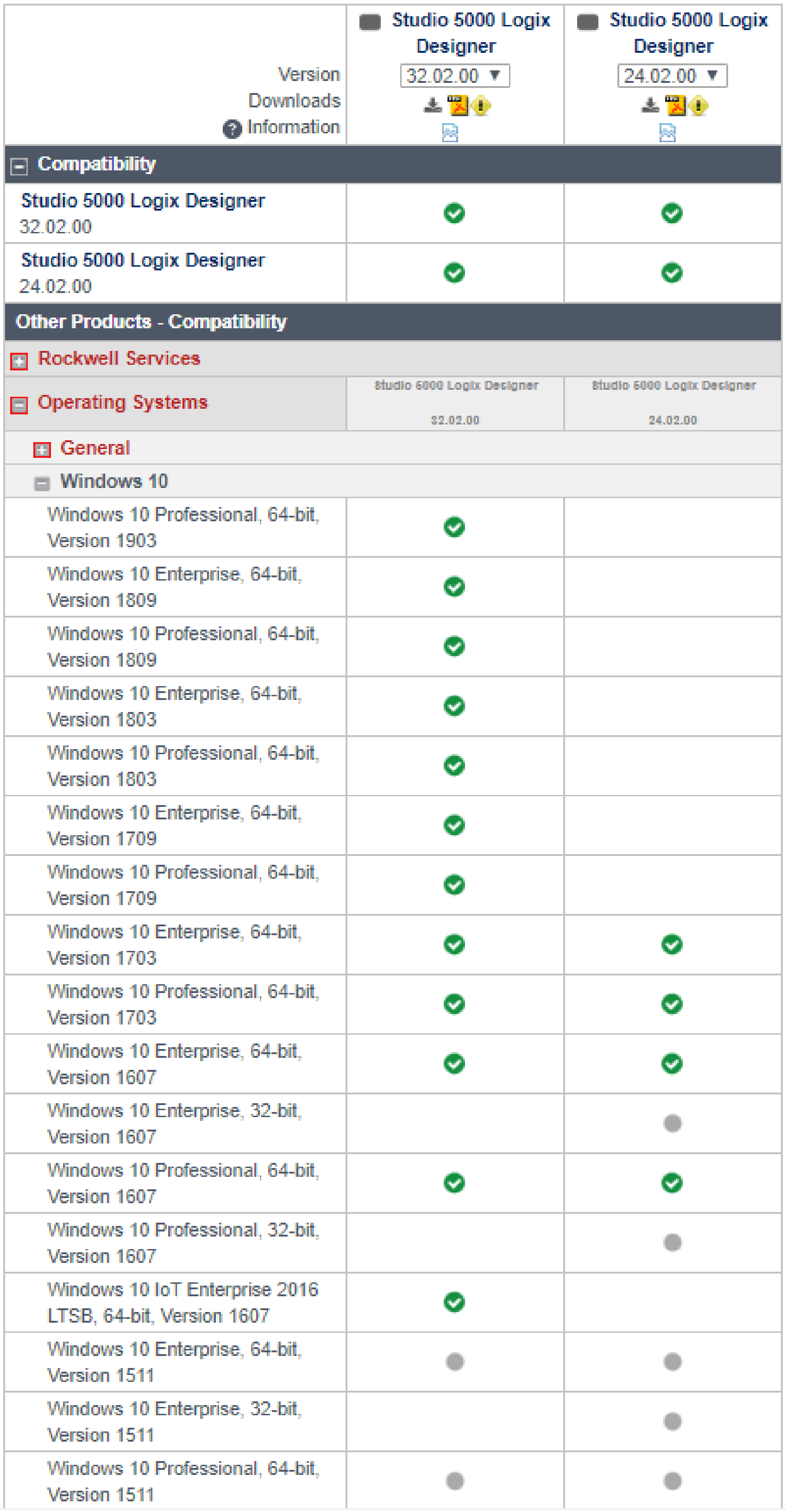
The County also utilizes GE MDS iNET 900 Ethernet radios, Engenius Ethernet bridges, and Digi One serial to IP converters for communication and communication protocol conversion. These devices are current and functioning properly. Continued maintenance is required for device replacement and upgrade as equipment ages. One item to note is the current fluctuation of use within the 900MHz spectrum. The licensed 900MHz spectrum is currently frozen by the FCC due to re-allocation of this band for the use of 5G technology. The impact of 5G technology in the unlicensed 900MHz spectrum is currently unknown but increased noise may be seen in this spectrum as well.

Control panel components such as power supplies, relays, breakers, and terminal blocks vary in each control panel cabinet depending on the design engineer and integrator performing the work. The best practice would be to standardize on a select few similar types of components to make replacement and troubleshooting easier and to minimize the spare parts inventory requirement. Additionally, panel mounted components include industrial touchscreens used for local access to the SCADA HMI screens. These devices will be evaluated in conjunction with network modifications and mobile solutions to determine possible future modifications to how remote clients are distributed.

3.4.1 Programmable Logic Controllers (PLCs)

As seen in the previous section, the existing PLCs are primarily Rockwell Automation’s Allen-Bradley SLC and MicroLogix platforms. The existing SLC PLCs have reached end-of-life and are slowly being replaced, but there is no defined replacement plan or hierarchy. The 1000 and 1100 series MicroLogix PLCs are also at the mature phase of the product lifecycle. The manufacturer’s suggested replacement for these PLCs is the Micro870 controller. The County is in the process of upgrading to their new standard which is the Rockwell Automation Allen-Bradley CompactLogix L18 or L33 Series. Some of the SLC PLCs have already been replaced and any new PLC is planned to be a CompactLogix platform. The exact CPU and I/O modules should be defined in order to maintain consistency and standardization. PLC upgrades require both the controller to be replaced as well as for I/O to be re-terminated. Specialized connectors for adapting SLC terminations to CompactLogix terminations are available to assist in faster cutovers. Testing procedures for checkout after replacement should be developed in order to verify all I/O has been correctly terminated and addressed in the new PLC programming.

PLC logic will also need to be migrated as part of the upgrade process. The SLC family of PLCs utilize RSLogix 500 and have limited Ethernet I/O scanning capabilities. The CompactLogix PLCs operate on the RSLogix 5000/Studio 5000 software platform requiring existing control logic to be migrated to this platform. The County noted that the migration tool only works for approximately 80 percent of the existing program, and the other 20 percent typically has to be reprogrammed. Additionally, during programming, desired logic changes should also be implemented as well as the use of standard programming blocks and ladder logic. In some cases, it may be more beneficial to re-program PLCs rather than convert logic so that a new tagging system can be used that is consistent with the County's standard and can be directly referenced by the HMI software. The enhanced Ethernet I/O capabilities of the CompactLogix PLCs should also be utilized for systems such as motor control, power monitoring, and some instrumentation. This functionality can minimize wiring, increase visibility, and increase system standardization. The County's use of Rockwell Motor control and Endress-Hauser instrumentation provides a direct integration with the Allen-Bradley CompactLogix PLCs. The County has also currently standardized on firmware Version 24. This is a key component to the standardization process along with standardizing software versions being used to make programming changes. Support for application management and change management will be a critical component to maintaining long term standardization. It should be noted version 24 of Rockwell software Studio 5000 has some support issues running on specific version of Windows 10. Version 24 was originally launched under Windows 7. In January 2020, Windows 7 which is no longer supported by Microsoft. therefore, it is suggested Manatee County upgrades the revision level of Studio 5000.



Version Downloads Information	Studio 5000 Logix Designer 32.02.00 ▼	Studio 5000 Logix Designer 24.02.00 ▼
⊟ Compatibility		
Studio 5000 Logix Designer 32.02.00	✓	✓
Studio 5000 Logix Designer 24.02.00	✓	✓
Other Products - Compatibility		
⊞ Rockwell Services		
⊟ Operating Systems	Studio 5000 Logix Designer 32.02.00	Studio 5000 Logix Designer 24.02.00
⊞ General		
⊟ Windows 10		
Windows 10 Professional, 64-bit, Version 1903	✓	
Windows 10 Enterprise, 64-bit, Version 1809	✓	
Windows 10 Professional, 64-bit, Version 1809	✓	
Windows 10 Enterprise, 64-bit, Version 1803	✓	
Windows 10 Professional, 64-bit, Version 1803	✓	
Windows 10 Enterprise, 64-bit, Version 1709	✓	
Windows 10 Professional, 64-bit, Version 1709	✓	
Windows 10 Enterprise, 64-bit, Version 1703	✓	✓
Windows 10 Professional, 64-bit, Version 1703	✓	✓
Windows 10 Enterprise, 64-bit, Version 1607	✓	✓
Windows 10 Enterprise, 32-bit, Version 1607		●
Windows 10 Professional, 64-bit, Version 1607	✓	✓
Windows 10 Professional, 32-bit, Version 1607		●
Windows 10 IoT Enterprise 2016 LTSB, 64-bit, Version 1607	✓	
Windows 10 Enterprise, 64-bit, Version 1511	●	●
Windows 10 Enterprise, 32-bit, Version 1511		●
Windows 10 Professional, 64-bit, Version 1511	●	●

Figure 3.2 Studio 5000 Version Comparison

In addition to PLC migration due to legacy equipment, PLC standardization to reduce the number of overall processors and types being used in the control system is a driving factor for PLC system upgrades. Any component, including processors, are a point of failure in the control system. Being able to reduce the quantity of components can then reduce the number of failures and having the same type of components reducing the requirements for different spare parts and training requirements. Generally, there are two methods for providing a reliable PLC control system. One is to have redundant processors for critical control applications and utilize distributed remote I/O. This reduces the number of processors in the system and provides processor redundancy, but communication between facilities becomes highly important since remote I/O does not have control intelligence and must have communication to the PLC processor in order to function properly. The other method is to provide distributed control where there separate processors are used for each process. This reduces dependence on communication between systems and prevents full system outages unless a single critical process is adversely affected. Each of these types of systems are described in more detail in the following sections along with a comparison and recommended path for PLC migration.

Central Redundant PLC System

A Central Redundant PLC system consists of two redundant controllers located centrally in each plant with remote I/O located near different processes. Central Redundant PLCs would decrease the amount of controllers necessary. For the controller, Allen Bradley ControlLogix 5580 controllers would be utilized with remote I/O modules located around the plant. All existing I/O cards would need to be replaced in order to support the ControlLogix controllers. Converting the system to a central redundant system would require more programming which would increase the cost as well as extra training for plant staff.

Using redundant process controllers does not necessarily increase the redundancy in the control system overall and can be costly for such a small return. To best utilize central redundant controllers, the processes need to also be redundant. This would require equally separating I/O between redundant processes as much as possible. For example, if there are 5 pumps in a system, three pumps would go to one set of remote I/O while two would go to the other remote I/O unit.

Central Redundant PLCs generally have a lower number of failures compared to a distributed system due to the limited number of controllers. Unlike the distributed PLC system, complete system failures could occur causing the entire plant to be down for maintenance as opposed to a single process.

Distributed PLC System

Distributed PLC systems are made up of several cabinets with process controllers spread out around the plant. These systems typically have a controller per process. The current Manatee County PLC system is a distributed PLC system. Due to this, it would make upgrading to Allen Bradley CompactLogix 5380 controllers from the existing SLC 5/05s throughout the plant easier. An additional option to simplify an upgrade in a distributed system would be that the SLC 5/05 I/O cards can continue to be used with CompactLogix controllers. This could allow for a more gradual system change over time. Therefore, the plant could upgrade their system in stages which will reduce downtime.

Distributed PLCs will require more maintenance due to the larger number of controllers. The benefit to a Distributed PLC system is that local failures occur which allows only one process or a few processes to be down at a time. This allows maintenance to occur on a small portion of the plant and the rest to continue running.

Redundant vs. Distributed PLC Comparison

Both of these options were considered as potential methods to upgrade the PLC system. In considering the use of redundant PLCs with remote I/O to upgrade existing wastewater control systems the following outlines the major benefits and potential drawbacks or issues with this option:

Table 3.5 Redundant PLC Option Benefits vs. Drawbacks

Benefits	Drawbacks
Single PLC Program	Only supported by ControlLogix Platform
Reduction in number of PLC CPUs	Requires a new system architecture
Redundant Processors	Requires highly reliable in-plant communication
	More difficult to phase migration
	Programming changes affect the entire plant and are not generally done at the process location

In considering upgrades using distributed PLCs, the following outlines the major benefits and potential drawbacks or issues with this option:

Table 3.6 Distributed PLC Option Benefits vs. Drawbacks

Benefits	Drawbacks
Current architecture can be maintained	No processor redundancy
PLCs can be replaced sequentially, and programming updated on a per processor/process basis	PLC CPUs on the process floor
Lower dependence on in-plant communication	More PLC CPUs to maintain
Lower Cost CompactLogix PLCs can be used	

Rockwell Automation was also consulted to solicit their opinion on the best option for PLC migration. Information on the current architecture of the County's system along with the current list of installed equipment was provided to Rockwell Automation in order to provide an opinion on simplest migration path along with associated costs for replacement hardware. Working with Rockwell Automation, Carollo assisted in developing the following table that directly compares the major hardware features of both solutions along with major implementation considerations:

Table 3.7 Distributed vs. Redundant PLC Comparison

Configuration Features	Distributed PLCs (CompactLogix)	Central Redundant PLCs (ControlLogix)
Supports Ethernet Scanning of Equipment	X	X
Supported Ethernet Speed	10/100/1000 Mbps	10/100/1000 Mbps
Number of Nodes Supported	Up to 180	Up to 300
Able to use PAX add ons	X	X
Able to make programming changes without a reboot	X	X
Application memory size	0.6MB to 10MB	3MB to 40MB
Able to use non-volatile memory	X	X
Able to eliminate batteries	X	X
Amount of I/O supported	Up to 31 Modules	128,000
Main Security Features	• Digitally signed and encrypted • Logs all changes • Role based access control • Ability to disable ports	• Digitally signed and encrypted • Logs all changes • Role based access control • Ability to disable ports
Localized failures	X	
Total system failures		X
Single application	X	X
Ability to remove and insert under power		X
Reuse SLC 5/05 I/O Cards	X	
Able to use Ethernet/IP	X	X
Lower training cost	X	
Less Programming Involved	X	
Ability to use migration tool for programming	X	X

Based on the feature comparison in the table above, the distributed PLC system replacement option has more benefits than the redundant PLC replacement option. This is in line with the benefit and downside comparison that Carollo developed independently. In addition to this feature comparison, the associated hardware cost of the distributed PLC solution is more than half the cost of the redundant PLC solution.

Due to the ease of converting the current system during an upgrade, comparison of features, and associated equipment costs, Carollo Engineers, Inc. recommends upgrading the system to a distributed system using Allen-Bradley CompactLogix PLCs. With this solution, almost all of the existing I/O cards can continue to be used which eliminates the need of re-terminating every point. Additionally, migrating I/O can be simplified by using specialized connectors to prevent re-termination of I/O wiring. Rockwell's recommended migration procedure from SLC PLCs to CompactLogix PLC is provided in the Appendix. One of the main reasons that this migration path is preferred is that the plants are already set up in this manner which makes it an easier transition on the staff and for the integrator. At the option of the County, Rockwell's conversion tool can be used in the upgrade to decrease the amount of programming necessary. However, Carollo recommends full reprogramming of these PLCs in order to take advantage of Rockwell add on instructions (AOIs) and to redevelop programming so that it is properly commented and uses conventions that the County understands and approves. This will also help in developing reusable code that can be linked to standard Citect graphical objects and templates. Downtime will also be reduced in the transition due to the ability to remove one PLC at a time and keep all others running.

3.4.1.2 PLC Control Logic

Because of the disparate and varied models of PLCs within Manatee County's control system, multiple programming software systems are necessary to support the varied hardware. The recommended solution is to move to a single programming software platform. Therefore, it is recommended to migrate from the SLCs and Micrologix PLCs which utilize the RSLogix 500 programming software to the CompactLogix PLCs which utilize the RSLogix5000/Studio 5000 platform to simplify training, software licensing, and software deployment. Implementing this recommendation will result in a single PLC programming software, Studio 5000, throughout the entire control system.

The judicious design and implementation of control and network products will minimize the number of different hardware systems as well reduce the number of different software systems that Manatee County staff need to be trained on and support. Due to the large number of PLCs at the facilities, the overall migration to the Rockwell CompactLogix platform and Studio 5000 software across all facilities will be an involved and lengthy project. As noted in this plan, the existing PLCs are varied in platform, model, family, and programming software. Full implementation of a single control system hardware and software solution is estimated to require three to five years. The migration to a single software platform and standardization of hardware will provide the following long-term benefits:

1. Better ability to leverage staff.
2. Reduced spare components.
3. Increased programming efficiency.
4. Increased communication efficiency.
5. Increased ability to access and utilize data for improved production and maintenance efficiency.
6. Enhanced ability to make widespread changes.

3.4.2 Operator Interfaces

The existing operator interfaces are split between CitectSCADA touchscreen interface terminals and PanelView/PanelViewPlus touchscreens. These operator interfaces are used by field operations to monitor systems and to make changes in the field. In some cases, these field interfaces only provide monitoring and control of specific processes. In these cases, PanelView and PanelViewPlus operator interfaces are utilized which were generally configured by the associated process package system supplier. In some cases, these local operator interfaces have additional information and functionality that has not been provided at the overall CitectSCADA system.

Twenty (20) of the total thirty-two (32) operator interfaces are CitectSCADA based with the remaining being Allen-Bradley PanelView (9), Maple Systems (1), and QuickPanel (2). The CitectSCADA operator interfaces are generally installed on either Pro-face or Xycom industrial touchscreen computers running Windows 7 operating systems. Xycom became part of Pro-face in 2007 and has since fully adopted the Pro-face branding. Pro-face has also now become part of Schneider-Electric. These touchscreen systems are in good shape, provide for consistency with the plant SCADA systems, and allow for replacement by numerous other industrial touchscreen computer manufacturers.

Allen-Bradley PanelView and PanelView plus systems installed include the PanelView 600 and 1000 series along with the PanelViewPlus 400 and 1250 series. These systems are programmed using either PanelBuilder 32 or FactoryTalkME, however the current software and version used to develop each application is not known. The PanelView series has been discontinued by Allen-Bradley. Allen-Bradley does provide guidance on migration to the new PanelViewPlus series in their 2711-AP002B-EN-P publication along with their product lifecycle status website which can be found at https://www.rockwellautomation.com/global/support/product-compatibility-migration/lifecycle-status/overview.page . All new PanelViewPlus series operator interfaces are programmed using the Factory Talk View Studio ME software which includes an application conversion wizard for legacy PanelView Standard and PanelBuilder32 applications. The PanelViewPlus hardware is current and supported.

The Maple Systems touchscreen, HMI5070TH, is a currently an available and supported product.

The QuickPanels that are deployed are no longer directly supported by the original vendors. QuickPanels have always been manufactured by Pro-face but white labeled by other vendors. Pro-face continues to support QuickPanels and does have a Product Lifecycle and Migration Guide. For the currently installed QuickPanel QPKSTDN000-A, the recommended replacement is the AGP-3300T. While this is a similar and equivalent hardware unit, due to the changes made in hardware and software for this product line, existing applications cannot be converted. Since re-development would be required, it is recommended to re-develop applications on a County standard operator interface.

In order to reduce maintenance and standardize on a single platform, it is recommended to utilize thin clients with the CitectSCADA system similar to the County's already deployed Pro-face/Xycom solutions. This will allow for reduced maintenance and training through the use of a single HMI platform. Additionally, it is recommended to transition from the Pro-face/Xycom panel mounted PCs to ThinManager ready thin client terminals. Thin clients as manufactured by Arista, OnLogic, and Dynics are Rockwell Automation partners that come pre-configured to work with the ThinManager system to provide a more seamless integration. With this system, remote clients do not need to be configured and replacement is simplified. Additionally, security is increased by the fact that these remote terminals do not store data or have control system information. All information is being stored and maintained by the main SCADA servers and content delivered by the ThinManager server.

3.4.3 Network Hardware

The existing network hardware on the process floor consists mostly of unmanaged Phoenix Contact switches and fiber optic communication throughout the plants. The County would prefer a self-healing fiber optic ring topology at each facility and has implemented some ring and pseudo-ring topologies within their facilities. In some cases, existing star networks were converted to logical but not physical rings. As network upgrades are made, a move towards more of a ring or multi-path technology should be continued.

Within the control network, managed Ethernet switches should be utilized. Managed switches minimize the potential for broadcast storms, provide visibility into the network, and allow for traffic management. The County should standardize on the use of managed switches within their networks. The County would also benefit from the following additional functionality to better manage and troubleshoot networks: port security, port control, Rapid Spanning Tree Protocol (RSTP), and overall traffic monitoring. The County has two main levels of control system switches, the plant floor switches, and the control room switches. Plant floor switches are generally industrial type switches while control room switches are generally rackmount commercial workgroup type switches. The weakest point in the system right now are the aging 3Com workgroup switches that are in need of replacement and located in plant control rooms providing the critical connection between control system components and operator graphic screens.

The following are the main requirements for plant floor switches:

- Industrial grade suitable for control panel mounting.
- Layer 2 management capability.
- Ability to integrate with the PLC/HMI system or network management system.
- Ability for SCADA staff to maintain.
- Product that IT staff is familiar with and can assist in supporting.

Based on the requirements for these types of switches, the Rockwell Automation Stratix series of switches would be recommended for the plant floor. These switches meet all of the above requirements along with the following additional benefits:

- Switches utilize the Cisco IOS software with a Rockwell GUI and add-on feature and can be configured through CLI with standard Cisco commands for IT familiarity.
- Common platform to the County's chosen PLC platform offering direct integration and added features.
- Common platform to the County's preferred motor control platform offering enhanced features.
- Directly compatible with Rockwell Automation's Asset Center for integrated management and added security features.
- Support of Rockwell Device Level Ring topology.

- Support Rockwell Common Industrial Protocol (CIP) Ethernet security utilizing Transport Layer Security (TLS) configured through Rockwell's FactoryTalk Linx communication platform.

Exact models of these Ethernet switches need to be determined based on exact implementation features and required number of ports.

Requirements for enterprise and workgroup level switches need to be more fully developed. Plant control system rackmounted switches should be Rockwell Stratix platform for direct integration with the plant floor switches. Higher level switches that integrate with SCADA servers and other higher level connectivity should be Cisco switches with features meeting the necessary requirements for routing and switching. These requirements include items such as VLAN segmentation, routing requirements, interfaces with IT equipment, number and type of ports, availability and redundancy, and security features. The solution at this level should be redundant such as the use of a stacked set of switches at critical core network locations to ensure a failure of one device will not interrupt the entire network. Where motor controllers and instrumentation are connected via Ethernet, multiple switches should be used to segment Ethernet I/O.

Additionally, the configuration of these switches may be more complex and require support and maintenance by the IT department. Coordination and potentially a service level agreement (SLA) may be required between the County SCADA support staff and the IT department in order to properly manage and maintain equipment.

3.4.4 Uninterruptible Power Supplies

The County has all of their control and computing equipment on UPS backup power. Existing UPS are 120Vac versions and are generally distributed at the point of use. Two of the plants have a large-scale UPS for backup power to control rooms and IT server and network equipment. These systems are well maintained and components replaced when they fail and batteries are replaced on a regular maintenance interval. In general, the County has standardized on the Schneider-Electric APC uninterruptible power supply platform for control panels. The County does not utilize or desire to have a maintenance bypass switch. Currently, UPS system are not monitored via hardwired or network connections. It would be beneficial to monitor UPS status over Ethernet to determine when UPS or batteries need to be replaced before failures occur and to receive notification of when power is lost and the system is on UPS supply. Monitoring can be done via hardwired signals or through Ethernet monitoring.

3.4.5 Control Panels

The County does not presently have a standard control cabinet layout or specifications regarding individual control panel components. Operations staff noted that standards for panel circuit breakers, pilot devices, surge suppressors, and terminal blocks would be useful. Existing I/O is a mixture of 24 VDC and 120 VAC, and operations staff noted that a standard of 24 VDC would be safer. SCADA touchscreens are distributed on control panels to provide operators with local SCADA access. The majority of control panels are well maintained and in good condition. Some control panels were found to have condensation build-up on the interior or in conduits entering from the top of the panels. Control panels should be inspected to ensure all conduits entering the enclosure are sealed with duct seal or an equivalent to prevent the intrusion of water and gases. Additionally, some enclosures may require additional thermal management to mitigate condensate.

The County does not presently have a standard drawing or schematic format. The style of schematics varies panel-to-panel and can add difficulty when troubleshooting or performing maintenance as maintenance technicians must be familiar with a variety of standards. The County desires a standard for schematics to ease troubleshooting and maintenance. Additionally, there are no formal change management procedures for control panel changes. Not all modifications are in the local panel drawings or on a central set of plans.

3.5 Power Monitoring

The South West Water Reclamation Facility (SW WRF) is currently the only facility to have power monitoring devices installed that are connected to the SCADA system. This facility has Square D PM 800 power monitors with DeviceNet communications. Other facilities appear to have power monitors on the electrical gear but they are not SCADA connected. The County is interested in system optimization and effective power management will be a key component in reducing power usage and cost.

3.6 Existing Site Security

The existing physical security systems at the water reclamation facilities do not meet current industry standards. The County does not presently have a formal security program in place for tracking keys and credentials and for implementation of security prevention system. A security risk and vulnerability assessment was performed in the past but not implemented. The County also mentioned that occasional acts of vandalism and the theft of maintenance equipment have occurred in the past. Areas of security improvement include the following:

- Add locks to outdoor control panels.
- Add intrusion switches to control panels.
- Correct operation of the plant gate and control access to the site.
- Keep facility doors locked.
- Develop security policies and tracking procedures to ensure items such as keys, keycodes, and other access and authentication credentials are accounted for and tracked.

There are security cameras only in one area, and the County is in the process of adding process cameras to the various sludge processes, septic receiving and truck loading. Cameras that are recorded are required to follow the state requirements for video retention and are managed by IT. Live viewing only cameras are not subject to these requirements. Currently, there is no formal video management policy for security and process video feeds or what should be monitored.

A security plan and upgrades are necessary to ensure potential future threats can be mitigated. Security planning will need to be coordinated with IT and other public works departments to ensure continuity across the County and to leverage investments properly.

3.7 Summary of Current Performance

- No formal written standard, specifications, or operating procedures.
- No formal change management for application programs and control panel drawings.
- Discontinued PLCs in the treatment process.

- Unmanaged and aging communication network components.
- Power management system not fully developed.
- No physical security plan and limited security implementation.

3.8 Best Practices

- Formal and comprehensive standards and SOPs.
- Common PLC hardware and software platforms.
- Change management and backup procedures for application programs.
- Updated documentation on all system components.
- Typical control panel layouts and standard hardware.
- Backup power for all components.
- Spare parts for all components.
- Common network hardware and use of managed layer 2 components.
- Current and supported hardware systems installed.
- Utilization of networked components for optimization and maintenance.
- Security plan and procedures in place.
- Security mitigation and detection components installed and monitored.

3.9 Initial Recommendations for Assessment

Based upon the information obtained, the following is a listing of initial system recommendations:

- Standardize on PLC platform and specific associated modules.
- PLC migration plan for end-of-life SLC PLCs.
- Development of PLC, Instrumentation, and Control Panel standards.
- Control Logic requirements and use of standard objects.
- Standard network switch selections.
- Diagnostic tools for managing network components and connected devices.
- Specification for construction guidelines and standard components.
- Panel inspection checklist for evaluating and testing control panels.
- Addition of access control system that allows tracking of entry and key management.
- Development of a security plan.
- Addition of IP video cameras for security and process control with centralized video management.

Chapter 4

SCADA SOFTWARE ASSESSMENT

4.1 Introduction

This chapter presents an analysis of Manatee County's existing SCADA HMI system software as well as supporting software systems used in the SCADA system. The goals of this chapter are to review the County's existing SCADA HMI system against County requirements and operational needs and current industry standards and competitor offerings to determine the suitability of the existing solution.

In addition, this chapter discusses existing HMI graphics, existing system architecture, and related SCADA software packages to assess the County's existing system. Information from a high level survey is also used to generate some initial thoughts about the current state of the SCADA system and opportunities for improvement. This chapter summarizes the major outcomes of the SCADA software assessment.

Recommendations presented are based on findings from workshops, peer comparisons, County staff interviews, current and planned information technology system infrastructure analysis, Carollo's experience, and industry best practices.

4.2 Existing SCADA System

The results of the staff survey were discussed to clarify the responses received prior to the workshop. Answers varied based on the operational role of the employee. The County currently uses Citect SCADA 2016 across each plant, except for in Biosolids. There is a plan to migrate to the newer Citect SCADA 2018 in the year 2019, and upgrades have gone smoothly in the past. In general, staff feel that the SCADA software platform meets their operational needs and is user friendly. For the most part, SCADA support staff feel that the system is easy to maintain and edit. Major components of the existing SCADA software system include the following:

- Citect SCADA – installed at numerous facilities.
- Citect Historian.
- Hach WIMS.

Table 4.1 County's Citect Licensing by Facility Summary

Facility	Key Serial Number	Part Number	Description	QTY
North WRF	47895877			
		CT101114	CitectSCADA, Full, 5000 Points	1
		CT102288	CitectSCADA, Redundant Web Display Client	3
	47895878			
		CT101114	CitectSCADA, Full, 5000 points	1
		CT102214	CitectSCADA, Web Display Client, 5000 points	1
		CT102214	CitectSCADA, Web Display Client, 5000 points	2
	48052166			
		CT103099	CScada-View Only Client	1
SE WRF				
	47933833			
		CT101114	CitectSCADA, Full, 5000 Points	1
	47933835			
		CT101114	CitectSCADA, Full, 5000 Points	1
	48062116			
		CT102099	CScada-Control Client-Unl pt	1
	48062117			
		CT102099	CScada-Control Client-Unl pt	1
	48067480			
		CT102014	CScada-Control Client-5000 pt	1
SW WRF	47933834			
		CT101114	CitectSCADA, Full, 5000 points	1
		CT102214	CitectSCADA, Web Display Client, 5000 points	1
		CT102214	CitectSCADA, Web Display Client, 5,000 points	2
		CT103099	CScada-View Only Client	1
		CT103099	CitectSCADA, Manager Client	1
	47933836			
		CT101114	CitectSCADA, Full, 5000 points	1
		CT102288	CitectSCADA, Redundant Web Display Client	3
		CT103088	CitectSCADA, Redundant Manager Client	1
	48052167			
		CT103099	CScada-View Only Client	1
	48078975			
		CT102014	CScada-Control Client-5000 pt	1
	48078976			
		CT102014	CScada-Control Client-5000 pt	1
	48088256			
		CT102014	CScada-Control Client-5000 pt	1
Biosolids				
	47944723			
		CT101114	CitectSCADA, Full, 5,000 points	1
	47944725			
		CT102014	CitectSCADA, Display Client, 5,000 points	1
	47944726			
		CT102014	CitectSCADA, Display Client, 5,000 points	1
	48052165			
		CT101114	CitectSCADA, Full, 5,000 points	1
		CT102214	CScada-Web Control Client-5000 pt	3
MCMRS				
	48099370			
		CT101112	CitectSCADA, Full, 500 points	1
	48099371			
		CT101112	CitectSCADA, Full, 500 points	1
	48099372			
		CT101112	CitectSCADA, Full, 500 points	1
IT Datacenter				
	A-CDC2-CPG8-KNFX			
		VJHNS212400	Historian CAL-User/Device	1
	A-FDDR-C4YG-AYZV			
		VJHNS212400	Historian CAL-User/Device	1

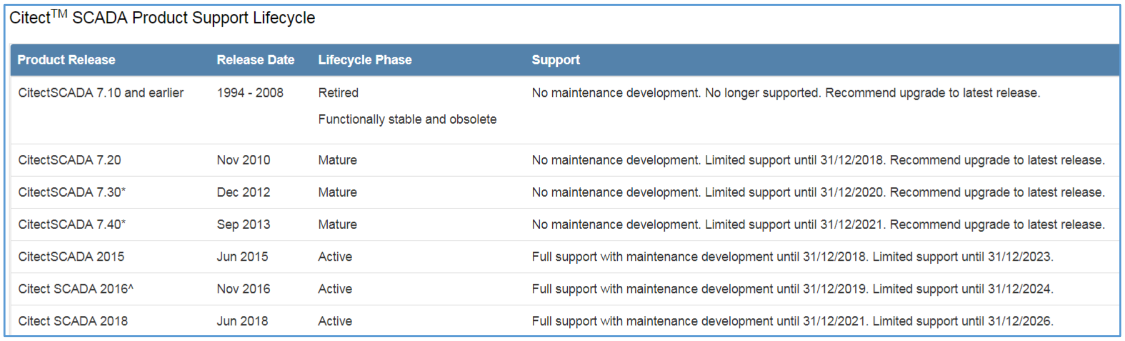
Table 4.1 County's Citect Licensing by Facility Summary (Continued)

Facility	Key Serial Number	Part Number	Description	QTY
To Be Removed				
	48077766			
		VJHNS211013	VJ Historian-1500 Pt	1
	A-FSS4-C2RJ-UV6L			
		VJHNS211013	VJ Historian-1500 Pt	1
Unknown				
	48099368			
		CT101114	CitectSCADA, Full, 5,000 points	1
		CT103099	CScada-View Only Client	1
	48099369			
		CT101114	CitectSCADA, Full, 5,000 points	1
		CT103088	CScada-Redundant View only Client	1
	48108564			
		CT305511	Citect Anywhere 5 User	1
	A-F39D-CUPM-8CB2			
		CT305511	Citect Anywhere 5 User	1

4.3 SCADA HMI Software

The County has Citect SCADA HMI software installed at the North WRF, South East WRF, South West WRF, Biosolids Facility, and at the Mars Booster Station. Each location has redundant servers plus numerous display clients. A Citect Historian server is centrally located in the IT datacenter with two server CALs and client licenses for user access. The Historian licenses are planned to be upgraded to a Wonderware Historian license having two client licenses. Appendix A provides a general overall layout of the County's SCADA Architecture. In general, the SCADA system architecture follows a hierarchy where clients are located at the facility level obtaining information from the redundant servers at each main facility. These servers then report data back to the centralized SCADA system Historian. Each SCADA server has two network cards for dual homing between the local control system network and the County wide network. Additionally, web clients exist in the SCADA system which would allow remote user access to the SCADA HMI at each of these facilities. However, each facility is basically its own island having its own application and authentication policies. A caveat to this is that the applications at the Dryer facility and MCMRS are the same but still hosted and maintained separately.

Currently, all SCADA installations are Citect SCADA 2016. This version is Active and fully supported until 12/31/2019 with limited support until 12/31/2024 as shown in the table below. Citect SCADA was recently migrated to the AVEVA brand after the merger between AVEVA and Schneider-Electric was completed. Citect SCADA continues to be a supported and continually developed SCADA software platform. Distribution of Citect SCADA also changed after the migration, and Citect SCADA is no longer distributed by BCI Technologies but is now exclusively distributed by InSource Solutions. This migration does not have major changes on the software itself or purchasing but does have some impact on application level maintenance and support since the software is no longer distributed through a control system integrator.



Citect^{TM} SCADA Product Support Lifecycle

Product Release	Release Date	Lifecycle Phase	Support
CitectSCADA 7.10 and earlier	1994 - 2008	Retired Functionally stable and obsolete	No maintenance development. No longer supported. Recommend upgrade to latest release.
CitectSCADA 7.20	Nov 2010	Mature	No maintenance development. Limited support until 31/12/2018. Recommend upgrade to latest release.
CitectSCADA 7.30*	Dec 2012	Mature	No maintenance development. Limited support until 31/12/2020. Recommend upgrade to latest release.
CitectSCADA 7.40*	Sep 2013	Mature	No maintenance development. Limited support until 31/12/2021. Recommend upgrade to latest release.
CitectSCADA 2015	Jun 2015	Active	Full support with maintenance development until 31/12/2018. Limited support until 31/12/2023.
Citect SCADA 2016^	Nov 2016	Active	Full support with maintenance development until 31/12/2019. Limited support until 31/12/2024.
Citect SCADA 2018	Jun 2018	Active	Full support with maintenance development until 31/12/2021. Limited support until 31/12/2026.

Figure 4.1 Citect^{TM} SCADA Procut Support Lifecycle

Additionally, AVEVA is about to release CitectSCADA 2020 which is being re-branded as Plant SCADA.

The SCADA server architecture at each facility is consistent. All three WRFs along with the Biosolids (Dryer) facility have redundant SCADA servers with 5,000 tag count licenses. Each of the remote MCMRS (MARS) booster pump stations have single SCADA servers with 500 tag count licenses. This topology provides redundancy at critical sites and is easily scalable. Additional system flexibility in regards to redundancy and enhanced visualization could be gained through the use of Clustering within the Citect SCADA system. Clustering allows for grouping independent Citect server objects within a single project which allows for multiple systems to be monitored and controlled simultaneously but managed separately. In this way, advanced functionality such as servers at different facilities could operate as Primary and Standby to each other while remaining Primary to the facility they are installed providing the opportunity to maintain redundancy while reducing licensing.

The following rules apply when Clustering Citect Servers:

- Each cluster must have a unique name such as Cluster A and Cluster B or Cluster North WRF and Cluster SW WRF.
- Each server process needs to have a unique name. Server processes include I/O server, Trend server, Report Server, Alarm Server, etc.
- Each server process needs to belong to one cluster. For example, separate I/O servers need to be created for Clusters A and Cluster B; a single I/O server cannot be assigned to both clusters.
- Each cluster can only contain one redundant pair of the following servers:
  - Alarm Servers.
  - Report Servers.
  - Trend Servers.
- Each cluster can contain an unlimited number of I/O Servers.

The following is an example system from the Citect SCADA website showing two clusters split across three machines:

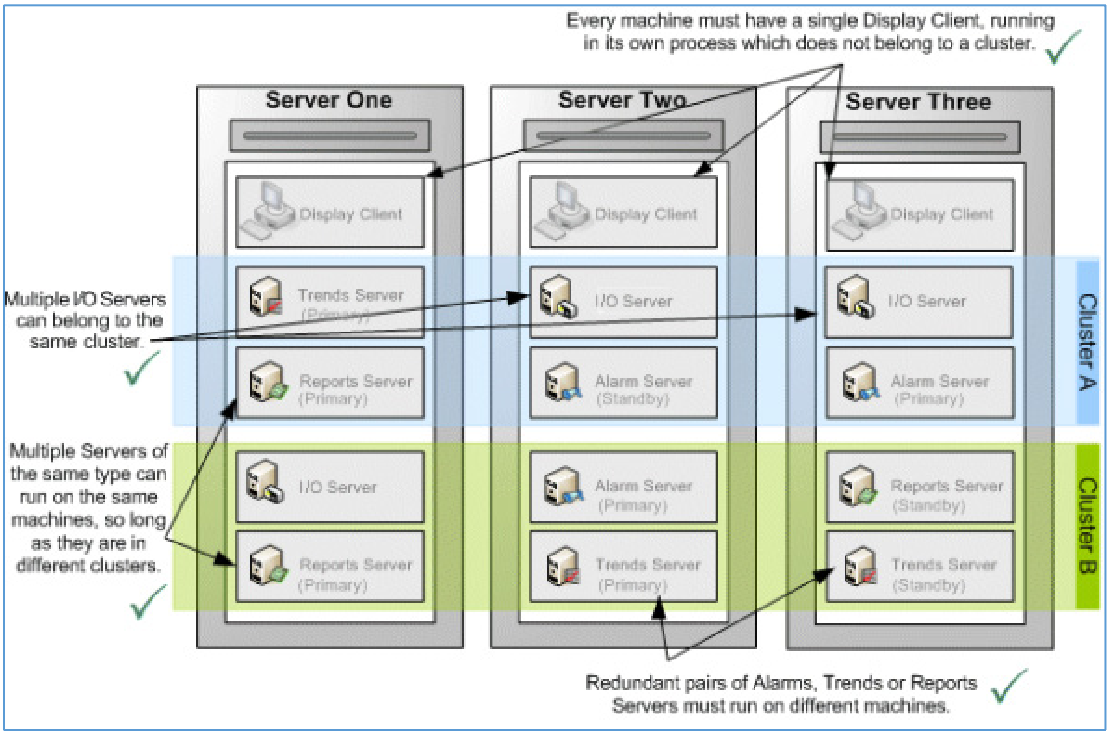

Every machine must have a single Display Client, running in its own process which does not belong to a cluster. ✓
Server One
Server Two
Server Three
Display Client
Display Client
Display Client
Trends Server (Primary)
I/O Server
I/O Server
Reports Server (Primary)
Alarm Server (Standby)
Alarm Server (Primary)
I/O Server
Alarm Server (Primary)
Reports Server (Standby)
Reports Server (Primary)
Trends Server (Primary)
Trends Server (Standby)
Cluster A
Cluster B
Multiple I/O Servers can belong to the same cluster. ✓
Multiple Servers of the same type can run on the same machines, so long as they are in different clusters. ✓
Redundant pairs of Alarms, Trends or Reports Servers must run on different machines. ✓

Figure 4.2 Two Clusters Split across Three Machines

In addition, there are multiple types of clustering techniques that are supported including:

- Standalone – No clustering is used and every server component runs on a single computer.
- Distributed I/O – Separate standalone servers are installed at each site. A single cluster can then be used to create a centrally managed application while maintaining the distributed components.
- Redundant Server – Redundant standalone servers are installed at a site. A single cluster can be used to manage the application.
- Client Server System – Server processes can be distributed across multiple servers and locations on the network and each server act as a display client for the single clustered application.
- Redundant and Distributed Control – Similar to redundant server but standby server is in a remote location.
- Cluster Controlled – Each site can be a separate cluster but all separate clusters can be viewed as if a single application.
- Load Sharing System – Allows separate servers to balance system components across the network. For example in a two cluster system, server 1 can be primary for Cluster A processes and backup for Cluster B processes while server 2 can be primary for Cluster B processes and backup for Cluster A processes.

In order to utilize clustering to best meet the County's requirements, the answers to the following criteria are important:

1. Is there a need for onsite redundancy?
2. Can SCADA server functions be hosted centrally or paired with a neighboring facility having good communication to each site?
3. Who needs to see facility information and where do they need to see it from?
4. Is there a desire to have central control room functionality?
5. Is a remote application needed having access to all facilities?

Utilizing this information, a best practice can be established in order to develop clustering parameters to meet the County's needs. Initially, two types of topologies seem to best fit the County's needs:

1. Maintain the existing topology and migrate the application to a Globally managed application with facility applications and communications in subgroups.
2. Eliminate the secondary servers at each location and deploy a central server to serve as the backup for all locations and to be a central deployment site.

The first topology maintains the existing County setup and offers the highest level of onsite reliability. In this scenario, servers would maintain their current functionality but the Citect application should still be migrated into a global application for a higher level of management and standardization. One of the servers in the County would be selected as the deployment server and be used to make application changes and would also be used for change management and revision history. This will provide a higher level of application management, standardization, and system security. No licensing changes would occur in this topology.

The second topology would modify the existing structure by removing the secondary servers. The associated equipment and licensing could also be removed. In this scenario, a centralized backup server would be located in the IT datacenter and configured to communicate with all other SCADA servers in the County. This server would then backup all other servers in the County, allowing for a decrease in licensing. This server would be configured as the deployment server for the system and provide a central location for deploying and managing applications. This would provide the advantage of having an offsite backup for every location in the system. A disadvantage to this topology is that if both a Primary server and the communication to a specific location were lost then this location's SCADA interface would be down and data lost. While not a single point of failure, this is a failure scenario that does not exist in the current topology.

The County's SCADA HMI system also has varying levels of access for different users, but no central password management. Passwords are local to each machine for both workstation and application authentication. In most cases, workstations utilize a common authentication login and password. The present architecture also means that each plant is its own island up to the SCADA servers.

4.4 SCADA HMI Graphics

The majority of the County's custom HMI graphics have been developed within the County's Citect SCADA system at each of the County's main wastewater facilities. Additional graphics exist on local touchscreens such as PanelView terminals, however, the majority of these are standard package system vendor applications. The following summarizes some of the main configuration items for the existing Citect SCADA HMI graphics:

- Resolution: 4 x 3 aspect ratio, stretched to accommodate widescreen monitors.
- Authentication: Local:
  - Citect credentials and user groups managed through each Citect application at each facility.
  - Workstation credentials managed at the workstation level (no workgroup) generally using a shared login.
- Graphic Display Layout:
  - Navigation:
    - Page Menu.
    - Forward and Back buttons.
    - Screen Targets.
  - Standard page top and bottom banners.
  - Alarm banner on each page.
  - Operator Name.
  - Date/Time.
  - Facility name and location.
  - Trending Tools.
  - Report Tools.
  - Alarm Tools.
  - Display area.

Process graphics are built in a hierarchical format having an overall facility layout and drill down graphics into each major process with additional popups for specific equipment. The general graphic development is physical. A physical facility layout shows the locations of processes based upon a site layout. Processes are shown in a typical P&ID schematic layout. Colors are used to indicate operational states and are also used for general coloring of non-indicating graphics such as ponds/lakes, piping, instruments, and equipment as well as for backgrounds. Limited text is used to indicate operational states or alarms. Most text is static and used for equipment identification.

Table 4.2 Graphic Colors and Text

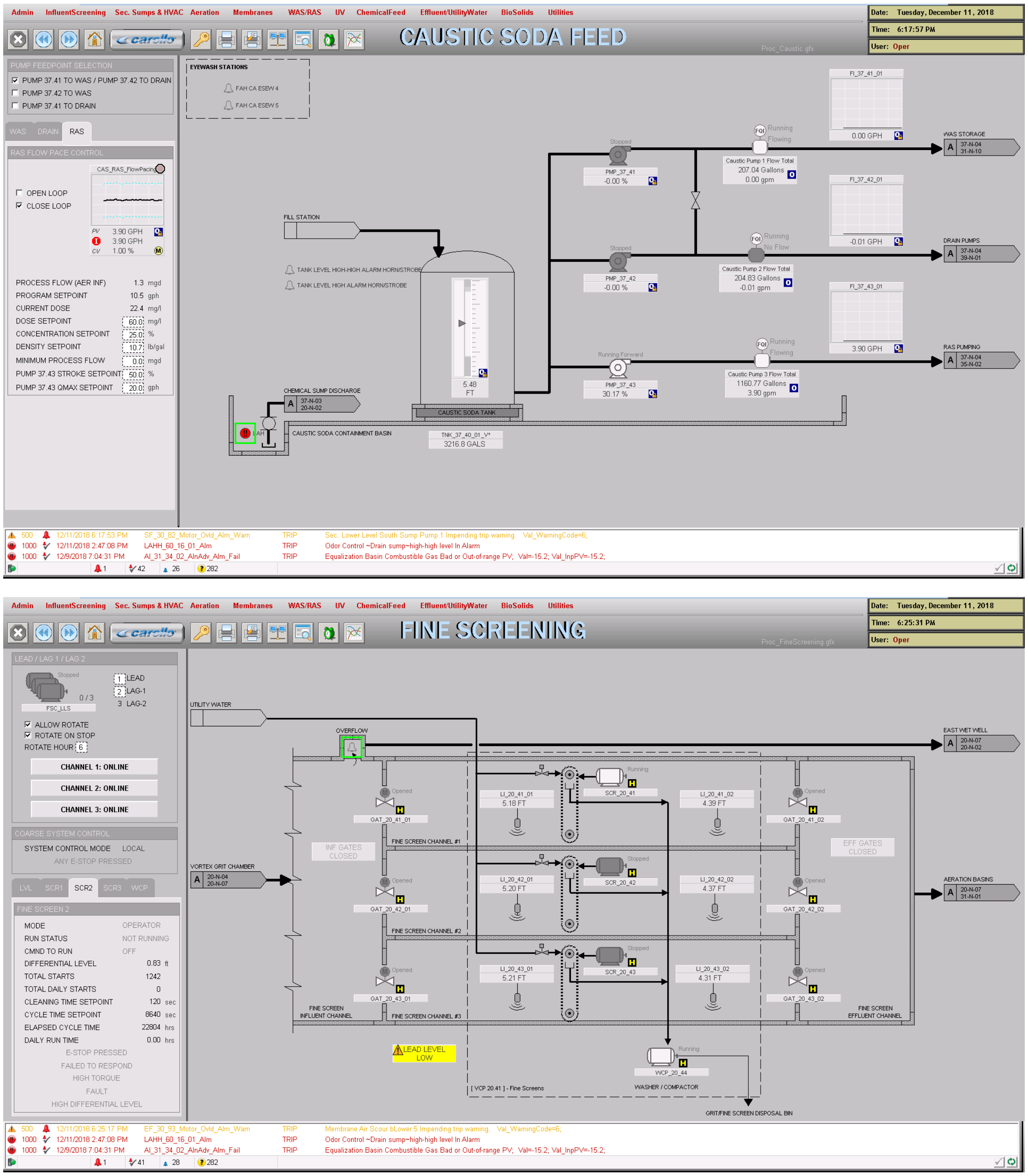
Equipment State	Color	Text
Running / Running Low Speed	Red	Black
Running High Speed	Orange	Black
Off	Green	Black
Open	Red	Black for position
Closed	Green	Black for position
Travelling / Midspan	?	
Failed / Trouble	Yellow	None
Alarm	Orange	None

All process values are indicated on the corresponding process displays and shown next to the physical location of the indicating instrument. The majority of these indicators are shown in boxes with black text with white background. In some instances, they are shown with black text directly on the page background. No indication is provided to aid operations in determining if the values are within operating ranges, however, some process graphics do contain embedded trends for critical process variables, but acceptable ranges are not shown. Not showing acceptable ranges requires operations to rely on their knowledge of acceptable and normal process values and can slow down reaction to abnormal conditions by experience process operators and can create a steep learning curve for inexperienced operations staff.

In general, the SCADA HMI graphics are fairly well standardized and consistent across County facilities which aids in operator performance and consistency of operation. The existing graphics layout is also well understood so current operators are able to perform all of their required tasks, however, some areas of improvement are noted below:

- Graphics standards are not documented.
- Graphics do vary some from plant to plant, but functionality is similar enough that operations can perform their duties despite some of the graphic variations.
- Increase clarity of icons and buttons and be very clear in their meaning.
- Existing graphics are busy making it hard to process critical information.
- Increase consistency of graphics.
- Add information such as motor current, totalized runtime, and other motor data as available to assist maintenance.
- Resolution does not match up with modern wide screen displays.

Staff at the County did indicate that they are open to and interested high-performance type graphics. These types of graphics are based on upon the ANSI/ISA-101, Human-Machine Interfaces standard. This standard outline recommended practices for industrial control graphics systems including layouts, graphical hierarchy, indicators, colors, and work process.



Date: Tuesday, December 11, 2018
Time: 6:17:57 PM
User: Oper

PUMP FEEDPOINT SELECTION

☑ PUMP 37.41 TO WAS / PUMP 37.42 TO DRAIN
☐ PUMP 37.42 TO WAS
☐ PUMP 37.41 TO DRAIN

WAS DRAIN RAS

RAS FLOW PACE CONTROL

☐ OPEN LOOP
☑ CLOSE LOOP

CAS_RAS_FlowPacing
PV 3.90 GPH
3.90 GPH
CV 1.00 %

PROCESS FLOW (AER INF)	1.3	mgd
PROGRAM SETPOINT	10.5	gph
CURRENT DOSE	22.4	mg/l
DOSE SETPOINT	60.0	mg/l
CONCENTRATION SETPOINT	25.0	%
DENSITY SETPOINT	10.7	lb/gal
MINIMUM PROCESS FLOW	0.0	mgd
PUMP 37.43 STROKE SETPOINT	50.0	%
PUMP 37.43 QMAX SETPOINT	20.0	gph

```
500   12/11/2018 6:17:53 PM   SF_30_82_Motor_Ovld_Alm_Warn   TRIP   Sec. Lower Level South Sump Pump 1 Impending trip warning.   Val_WarningCode=6;
1000  12/11/2018 2:47:08 PM   LAHH_60_16_01_Alm              TRIP   Odor Control ~Drain sump~high-high level In Alarm
1000  12/9/2018 7:04:31 PM    AI_31_34_02_AlnAdv_Alm_Fail    TRIP   Equalization Basin Combustible Gas Bad or Out-of-range PV;  Val=-15.2; Val_InpPV=-15.2;
      1    42    26    282
```

Date: Tuesday, December 11, 2018
Time: 6:25:31 PM
User: Oper

LEAD / LAG 1 / LAG 2

Stopped
0 / 3
FSC_LLS
1 LEAD
2 LAG-1
3 LAG-2

☑ ALLOW ROTATE
☑ ROTATE ON STOP
ROTATE HOUR 6

CHANNEL 1: ONLINE
CHANNEL 2: ONLINE
CHANNEL 3: ONLINE

COARSE SYSTEM CONTROL

SYSTEM CONTROL MODE LOCAL
ANY E-STOP PRESSED

LVL SCR1 SCR2 SCR3 WCP

FINE SCREEN 2

MODE	OPERATOR	
RUN STATUS	NOT RUNNING	
CMND TO RUN	OFF	
DIFFERENTIAL LEVEL	0.83	ft
TOTAL STARTS	1242	
TOTAL DAILY STARTS	0	
CLEANING TIME SETPOINT	120	sec
CYCLE TIME SETPOINT	8640	sec
ELAPSED CYCLE TIME	22804	hrs
DAILY RUN TIME	0.00	hrs

E-STOP PRESSED
FAILED TO RESPOND
HIGH TORQUE
FAULT
HIGH DIFFERENTIAL LEVEL

```
500   12/11/2018 6:25:17 PM   EF_30_93_Motor_Ovld_Alm_Warn   TRIP   Membrane Air Scour bLower 5 Impending trip warning.   Val_WarningCode=6;
1000  12/11/2018 2:47:08 PM   LAHH_60_16_01_Alm              TRIP   Odor Control ~Drain sump~high-high level In Alarm
1000  12/9/2018 7:04:31 PM    AI_31_34_02_AlnAdv_Alm_Fail    TRIP   Equalization Basin Combustible Gas Bad or Out-of-range PV;  Val=-15.2; Val_InpPV=-15.2;
      1    41    28    282
```

Figure 4.3 Example, SCADA High Performance HMI Graphic

The latest version of Citect SCADA 2018 supports this style of HMI design with what they refer to as Context Aware graphics. Citect SCADA 2018 now has the following features to support generation of a high-performance graphic environment including:

- Context-Aware Workspace:
  - Templates for 1080p and 4K screen resolutions.

  - Built-in context system that updates faceplates and information for selected equipment.
  - Enhanced navigation features.
  - Multi-monitor support.
- Comprehensive Graphics Library:
  - Pre-built symbols that follow industry best practices for situational awareness.
  - Configurable, out of the box.
  - Sample Library Graphics.

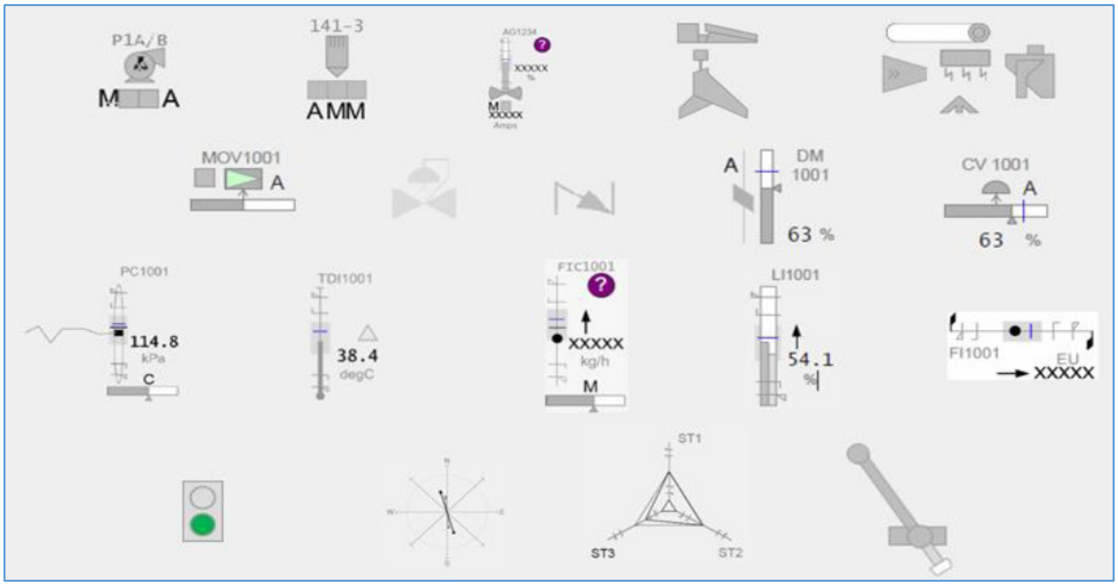
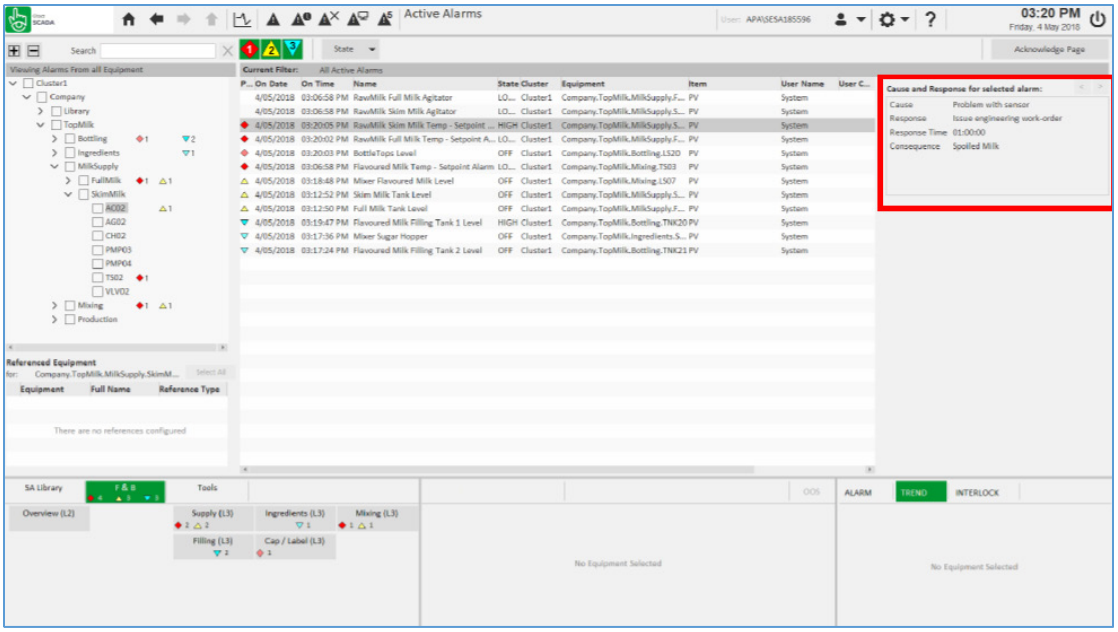


Figure 4.4 Example, Comprehensive Graphics Library

- Alarm Management:
  - Native alarm indicators following industry best practices.
  - Ability to shelve alarms.
  - Define cause / response for any alarm.



Current Filter: All Active Alarms

P...	On Date	On Time	Name	State	Cluster	Equipment	Item	User Name	User C...
	4/05/2018	03:06:58 PM	RawMilk Full Milk Agitator	LO...	Cluster1	Company.TopMilk.MilkSupply.F...	PV	System	
	4/05/2018	03:06:58 PM	RawMilk Skim Milk Agitator	LO...	Cluster1	Company.TopMilk.MilkSupply.S...	PV	System	
◆	4/05/2018	03:20:05 PM	RawMilk Skim Milk Temp - Setpoint ...	HIGH	Cluster1	Company.TopMilk.MilkSupply.S...	PV	System	
◆	4/05/2018	03:20:02 PM	RawMilk Full Milk Temp - Setpoint A...	LO...	Cluster1	Company.TopMilk.MilkSupply.F...	PV	System	
◆	4/05/2018	03:20:03 PM	BottleTops Level	OFF	Cluster1	Company.TopMilk.Bottling.LS20	PV	System	
◆	4/05/2018	03:06:58 PM	Flavoured Milk Temp - Setpoint Alarm	LO...	Cluster1	Company.TopMilk.Mixing.TS03	PV	System	
△	4/05/2018	03:18:48 PM	Mixer Flavoured Milk Level	OFF	Cluster1	Company.TopMilk.Mixing.LS07	PV	System	
△	4/05/2018	03:12:52 PM	Skim Milk Tank Level	OFF	Cluster1	Company.TopMilk.MilkSupply.S...	PV	System	
△	4/05/2018	03:12:50 PM	Full Milk Tank Level	OFF	Cluster1	Company.TopMilk.MilkSupply.F...	PV	System	
▽	4/05/2018	03:19:47 PM	Flavoured Milk Filling Tank 1 Level	HIGH	Cluster1	Company.TopMilk.Bottling.TNK20	PV	System	
▽	4/05/2018	03:17:36 PM	Mixer Sugar Hopper	OFF	Cluster1	Company.TopMilk.Ingredients.S...	PV	System	
▽	4/05/2018	03:17:24 PM	Flavoured Milk Filling Tank 2 Level	OFF	Cluster1	Company.TopMilk.Bottling.TNK21	PV	System	

Cause and Response for selected alarm:

Cause	Problem with sensor
Response	Issue engineering work-order
Response Time	01:00:00
Consequence	Spoiled Milk

Figure 4.5 Example, Alarm Management Page

Migration to the most current version of the Citect SCADA 2018 along with re-development of graphics would provide the following benefits:

- Modernize resolution to widescreen HD or 4K resolutions.
- Standardize graphics and reduce clutter.
- Implement high performance style "context aware" graphics.

The migration of graphics can be done sequentially in order to minimize operator confusion over large scale changes, maintain consistency throughout the County, and leverage the tools within Citect. The following would be the recommended graphics migration path:

1. Develop a global Citect Application:
   a. Develop global include library for genies and objects.
   b. Develop global template.
2. Develop subdirectories for each site which would contain:
   a. Local comms including those for PLCs.
   b. Special local objects.
   c. Local application.
3. Migrate each facilities pages into the local application structure of the global application:
   a. Select template Citect 2016 or 2018.
   b. Import graphic into the template and make any minor changes needed for appearance.
   c. All graphics should be migrated, or they will be lost in navigation. A temporary navigation page can be created to assist with the migration process to ensure that screens are not lost during the process.
4. Develop global genies and objects for use in graphics conversion.

5. Develop an equipment structure within Citect to group tags associated with a particular asset:
   a. Asset tag should match Asset tag from CMMS system for consistency.
6. Re-develop Screens using the following guidelines:
   a. 16:9 aspect ratio.
   b. Utilize Citect toolkit to extent possible and match equipment to standard genies and templates.
   c. Re-layout graphic screens using the Citect Operational Awareness guidelines.

This migration will first allow the use of Citect standard tools for navigation, alarming, and trending and then provide additional features for graphical viewing and alarm management. This work can also be paired with PLC upgrades and application clustering in order to coordinate upgrades and minimize efforts.

4.5 SCADA Access

County Staff interviewed and surveyed all noted having access to the SCADA system in order to perform tasks required of the job positions, however, there is still a desire to have a higher level of SCADA access most notably in having more reliable remote access and additional access throughout the plant. Additionally, most staff feel that they have adequate access to historical data and trending abilities, but do not feel they have adequate access to Operations and Maintenance material. Almost all staff noted that having remote access to the SCADA system and access via a mobile device such as a tablet would be very beneficial to their job functions.

Currently, the SCADA system is accessed through the SCADA workstations at each facility and the Citect SCADA client operator interface terminals located throughout the facilities. When operators do not have access to either of these types of SCADA HMI interfaces, they cannot see what is happening in the facility. This can reduce operator efficiency at times such as when alarms occur while operations staff is working around the facility or making rounds and operators must go and find the nearest client machine in order to identify and correct the alarm condition. These types of SCADA clients also require dedicated infrastructure, communications, and licensing so adding additional client machines to locations can become costly. Mobile clients would offer solutions to some of these issues but the following items would also need to be addressed:

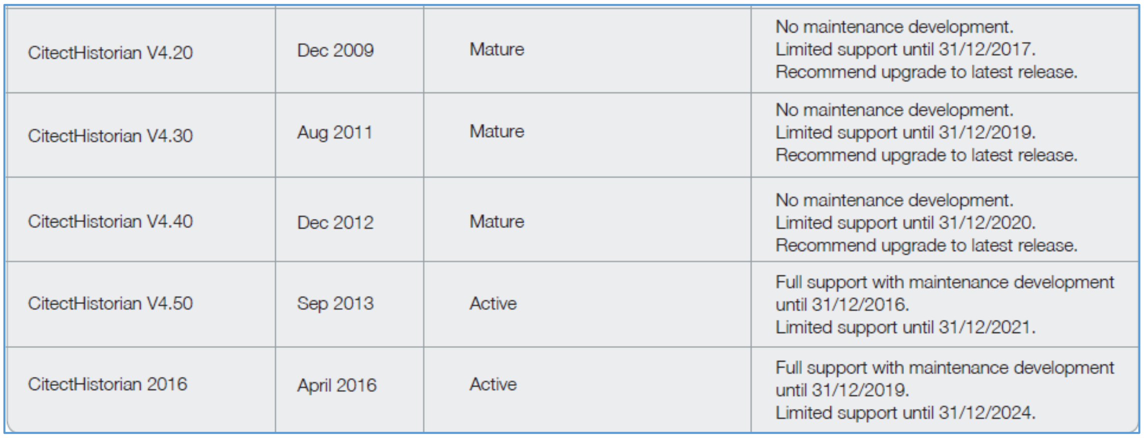
- Reliable communications both inside and outside of facility buildings for client operation.
- Mobile device security coordinated with IT.
- Consistent SCADA client application delivery for common access environment.
- Enhanced SCADA client authentication and security groups for application security.
- General management of mobile devices.

In addition to SCADA client access, a centralized management system is needed for Operations and Maintenance data including drawings, application backups, and other digital files. SharePoint is currently used to manage some of this information but access to this system has been slow likely because of offsite hosting. County IT is planning to migrate to an onsite solution that should increase speed.

4.6 Historian

One central Citect historian collects data from the SCADA servers at each facility. The historian is hosted in a virtualized cluster in the County IT datacenter. Facility SCADA servers can access data from the Historian using the Process Analyst inside the Citect SCADA environment providing operators the ability to trend all necessary information. The existing historian has issues with data gaps, where a zero is inserted for data gaps that has to be manually edited. Shutting down the server or processor also causes a data gap. The exact cause of the data gaps is unknown but could be due to communication issues or improper configuration of buffering from the Citect I/O servers. When the Citect SCADA system is upgraded, the configuration of the Citect SCADA servers and associated Historians should be reviewed and modified as necessary to ensure minimize the possibility of gaps in date.

The Citect SCADA Historian appears to be on a phase out path. Since the transition of CitectHistorian from Schneider-Electric to AVEVA, no new versions of the CitectHistorian have been planned and CitectHistorian is not a listed Historian option from AVEVA. Currently, full support for the CitectHistorian will end at the end of 2019 and the product will continue limited support until 2024 as noted in the figure below.



CitectHistorian V4.20	Dec 2009	Mature	No maintenance development. Limited support until 31/12/2017. Recommend upgrade to latest release.
CitectHistorian V4.30	Aug 2011	Mature	No maintenance development. Limited support until 31/12/2019. Recommend upgrade to latest release.
CitectHistorian V4.40	Dec 2012	Mature	No maintenance development. Limited support until 31/12/2020. Recommend upgrade to latest release.
CitectHistorian V4.50	Sep 2013	Active	Full support with maintenance development until 31/12/2016. Limited support until 31/12/2021.
CitectHistorian 2016	April 2016	Active	Full support with maintenance development until 31/12/2019. Limited support until 31/12/2024.

Figure 4.6 CitectHistorian Support Projections

AVEVA's current Historian options are the Wonderware Historian which operates very similarly to the CitectHistorian and the eDNA Enterprise Historian which appears to be the migration of the Telvent OASyS system DNA Historian which would be more commonly used in a DCS system environment. Additionally, InSource is offering special pricing on a Wonderware Historian migration package. While not directly related, the Manatee County Lake Manatee WTP is also being upgraded from its existing HSQ system to a new control system based on CitectSCADA and the Wonderware Historian. Based on the current status of the AVEVA offering, maintaining system consistency across the County, the recommended approach to continue with CitectSCADA, and the currently reduced pricing it would be recommended to work with the Wonderware Historian distributor, InSource Solutions, on a migration to the Wonderware Historian platform. The following key requirements should be addressed as a part of the historian migration from CitectHistorian to Wonderware Historian. If these requirements cannot be met, then alternate solutions should be evaluated:

- Migration of existing CitectHistorian Data into the new Historian system:
  - This appears to be possible using a custom Citect CiCode script written by Aveva.
- Continued ability to access historical data through the CitectSCADA Process Analyst or Trends server:
  - Citect Trends Server will remain active within Citect.
  - Process Analyst will not connect to Wonderware Historian.
  - Process Analyst connection should be pointed to the Citect Trend Server.
  - Wonderware Insight can be added to connect to Wonderware Historian providing a simple user interface for all users.
  - Wonderware Historian Client could be used to connect to Wonderware Historian as a standalone application or as an ActiveX component to display trend data on a CitectSCADA display.
- Link from new Historian Platform to Hach WIMS system:
  - Hach WIMS has a standard driver for Wonderware Historian.
- Ability to Tier historians if necessary:
  - Wonderware Historian can be tiered and does have backfill function with Citect Trend Server.
  - Wonderware Historian also has cloud services for enhanced visualization and analytics.

As a part of the Historian migration, data that is being historized should be analyzed to ensure that all necessary variables are being included in the historical data and that the associated Historian tag count license is appropriately matched to the data needs. Currently not every value is historized due to storage limitations. As the cost of storage has gone down additional points that may provide insight into optimization or enhanced maintenance strategies should be considered to be added to the new Historian. Also, any points required for integration with the CMMS deployment should be added to the Historian as well. If a direct connection to the CMMS system is desired, the Avantis Condition Manager can be used which already has built-in connectors between Citect and popular CMMS systems. The compatibility with the Lucity system the County uses will be investigated if this is a desired functionality of the SCADA system.

In addition to Historian platform migration, the following organizational items also need to be addressed:

- Additional operator training on Historian operation.
- Development of a standard procedure or instructions on how to query and export raw historical data.
- Update Historian permissions and security authentication through Active Directory.
- Develop standard operating procedures:
  - Report Generation.
  - Trend Development.
  - How to verify Historian if functioning.
  - Data Validation.

4.7 Alarms

Alarms are currently displayed within the CitectSCADA environment. The majority of alarms are displayed with the same priority and color scheme which can make it difficult at times for operators to quickly differentiate between critical and non-critical alarms. In general, the necessary alarms for operators to effectively perform their duties are in place. Operations could be further optimized by rationalizing alarms into different categories to assist in determining the criticality and type of each alarm. The latest version of CitectSCADA 2018 has enhanced tools for effective alarm management. Some of these tools include the ability to shelve alarms, define the cause and action for alarms, and the use of indicators and flags to enhance operator identification of alarms. Alarms should be rationalized following the ISA 18.2 Alarm Management Standard. The ISA 18.2 alarm management cycle is summarized in the following figure:

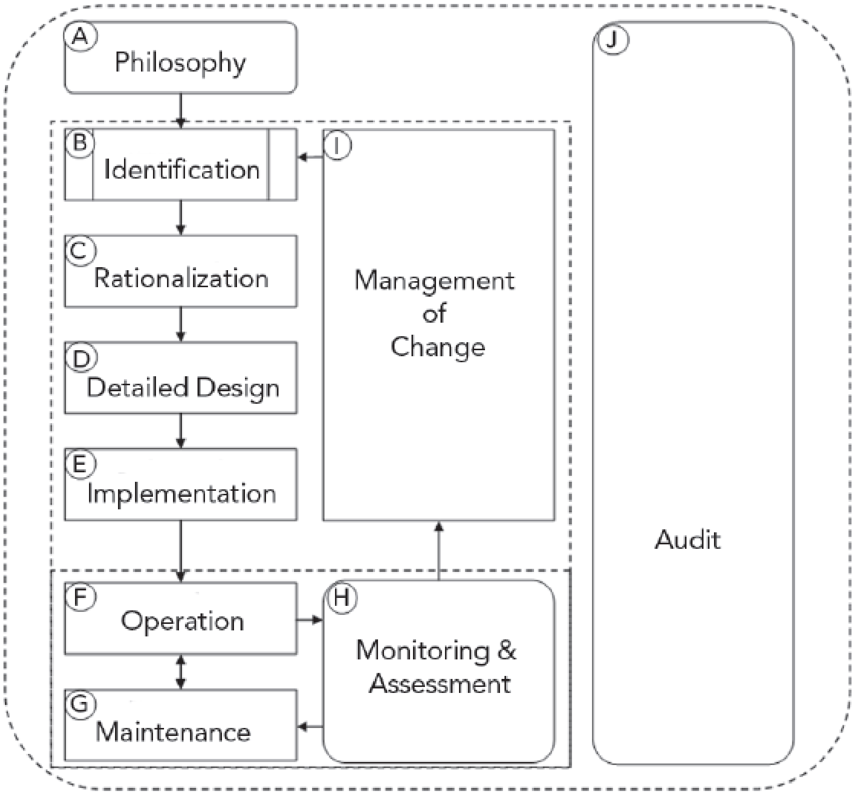


Figure 4.7 The Alarm Management Life Cycle

In addition to general alarm management and rationalization, operations also have specific issues with nuisance alarms that are generated on power outages such as during generator transfers. Alarm rationalization should help with this issue, but nuisance alarm suppression should be implemented in the PLC logic in order to suppress alarms that are related to other large or more widespread failures such as power failures. In order to provide this type of suppression, loss of power indication may need to be added to specific control panels for indication of power fail and suppression of alarms subsequently created by this condition. Similar nuisance alarms occur at booster stations and other remote sites. Similar nuisance alarm suppression should be added at these locations as well.

Developing reports to display alarm statistics would also assist in the identification of nuisance alarms as well as indication of alarms indicating equipment failure or faulty alarm conditions. Examples of statistics to generate and review include the following:

- Highest count of specific alarms.
- Highest count of similar alarms (such as high level, high pressure, etc.).
- Time of occurrence of alarm floods.
- Alarm level distribution (Critical, high, warning, event, etc.).

Reports can be generated monthly noting statistics such as alarm most often triggered each day, week, and month in specific categories along with days and times of alarm floods and the alarm level distribution for the end of the month. Alarms can then be modified as necessary to minimize excessive alarms and equipment investigated to determine if there are faulty conditions or incorrect settings. The latest version of CitectSCADA 2018 has tools to help with alarming issues such as those noted above. Migration of graphics to this version and the utilization of the equipment structure within Citect should be developed in order to assist operators with alarm management.

In addition to system alarming, remote alarm capabilities could also provide a benefit such as when operations staff are making facility rounds. During these periods, operators are notified of alarms through local alarm horn and light notification systems. In order to determine the alarm cause and criticality, the operator must return to the control room to investigate the alarm. Using remote alarm notification systems, the operator would receive the alarm on a device such as a cellphone and be able to determine how to address the alarm on the spot and acknowledge as appropriate. This would also provide the capability of notifying staff not at the facility of the alarm condition through either active or passive notifications depending on the response required. The following are examples of systems compatible with CitectSCADA that could provide SMS, Email, and other types of notification solutions:

- WIN-911.
- SMS Server.
- SCADAPhone.

WIN-911 is the current market leader in the remote notification alarm software market sector and offers multiple levels of solutions including a mobile application for alarm management. One of the drawbacks of this platform is the difficulty in developing a redundant solution. SCADAPhone has many similarities to WIN-911 and does offer built-in support for redundancy. SMS Server is another option which was developed specifically for use with CitectSCADA, however, is not as feature rich as the other two options. All three options do have trial versions that can be tested before purchase. It is recommended that if a remote notification solution is planned to be implemented that it is run in trial version to verify features meet operational needs before purchasing.

4.8 Automation, Monitoring, and Reporting

Automation improvements such as trim control and automatic response for chemical processes and aeration basins would help improve process efficiency and performance. The current report generation software is Hach WIMS, and the County desires the ability to transfer data into the Hach WIMS system. The County is satisfied with the Hach WIMS trending and reporting functionality, and wishes to maintain this going forward. The County would benefit from additional data monitoring and reporting on motor amps and torque, energy management, running averages of SRTs, and dissolved oxygen. Additional data could be tracked to optimize various processes: Mixed liquor, bionutrients, chemical systems, and more. Energy management is a long-term goal, and the County desires power / energy monitoring to identify peak demand for each plant, kilowatts, harmonics, motor efficiencies, and any additional information available to view at the SCADA level. In addition to the Hach WIMS system, the Wonderware Insight client can also be used to developed management level dashboards in order to visualize data to a higher degree to provide a simpler view of information needed to optimize system operation and can be used to display KPIs to gauge the systems performance.

4.9 Recommendations

Carollo will provide recommendations on an Access Management System (AMS) to interface with SCADA, as well as a mobile-to-mobile network and remote alarm notification system. During the site visits, a wireless mesh network or plant-wide wireless network was discussed. Various existing structures may present a challenge for wireless access.

Carollo will provide recommendations on power monitoring systems to provide the County with additional data monitoring ability for motors and energy management metrics. Carollo will also provide recommendations on the historian and assist with standard operating procedures relating to report generation.

Carollo will provide recommendations on network diagnostic tools, network architecture, and workflow improvements. Refer to TM-3 for SCADA access and network architecture recommendations.

4.10 Summary of Current Performance

- No formal written standard, specifications, or operating procedures.
- No formal change management for application programs.
- HMI standards are not documented.
- Supported version of SCADA HMI system in place but not the latest.
- SCADA HMI graphics are not utilizing the current software tools.
- Historian in place and migrating to the latest version.
- Not all data needed for optimization being trended.

4.11 Best Practices

- Formal and comprehensive standards and SOPs.
- Centrally managed and standardized HMI system with revision management.
- Redundancy and backup systems in place for reliability.
- Supported software in use.
- SCADA clients available to operations staff.
- Software tools used to aid operator visualization, alarm management, and data access.
- Data available to staff and systems.
- Application security in place.

4.12 Initial Recommendations for Assessment

Based upon the information obtained, the following is a listing of initial system recommendations:

- Upgrade to latest version of CitectSCADA 2018.
- Migrate graphics into a global application and upgrade to use latest software toolsets.
- Develop a clustered environment with deployment server.
- Implement CitectAnywhere for the full application across all facilities.
- Integrate Wonderware Historian and add Insight Client.
- Determine if CMMS system will be integrated to the SCADA system for automation of work orders.
- Implement Equipment Model in the Citect environment.
- Train operations on new alarm management tools and how to rationalize alarms.
- Implement Active Directory security into the application.

Chapter 5

NETWORK AND COMMUNICATIONS ASSESSMENT

5.1 Introduction

This chapter presents information related to the Manatee County water reclamation facility communications network and server hardware infrastructure. The County utilizes Ethernet communications networks for its plant process control systems as well as for connectivity to the IT network for inter-facility and remote system access. Additionally, radio communications are used for connectivity to remote sites. As the County continues to expand systems and automate more processes at the, reliance on these communications networks for proper operation increases and the necessary reliability and functionality must also increase.

In addition to communications systems, the County relies heavily on server and computer system infrastructure to host its SCADA services. Server hardware is utilized to host core SCADA system servers as well as data historians, and workstations are used to host SCADA clients, all providing operations access to monitoring and control functionality. The server infrastructure will need to grow in order to keep up with expanding cyber security requirements and data management as well as providing more efficient and operator friendly accessibility to these system resources.

Recommendations presented are based on findings from workshops, peer comparisons, County staff interviews, infrastructure analysis, Carollo's experience, and industry best practices.

5.2 SCADA System Network

The County has noted a number of issues with the existing communications systems. One common problem is with the Data Flow Systems (DFS) radios. Remote communications are critical, and the County has had issues with very high latency when polling remote sites. Wireless radio broadcast storms have also taken down the network in the past. All county network devices are backed up on a 24-hour interval or whenever a change is made. The County's IT department proposed a stackwise solution and uses that for all critical applications.

The County has approximately 50 unmanaged Ethernet switches. As noted in Chapter 3, utilizing managed switches instead would help address broadcast storms and increase network management capabilities. In order to get these benefits, managed switches do require configuration. Current SCADA maintenance staff are not currently trained in switch configuration and the County's IT department does not maintain the SCADA network, so moving to managed switches may require additional responsibility for the County's IT staff or additional training for plant staff.

The recommended solution is the use of managed Allen-Bradley Stratix Ethernet switches due to their direct compatibility with the PLC system to integrate network data into the SCADA system, its modular form factor, graphical user interface for configuration, and Cisco IOS command line environment that is familiar to IT staff. Another advantage is the ability of these switches to interface with the Rockwell Automation Asset Center solution for device management. Asset Centre provides the ability to automatically backup and re-load a device configuration as well as manage passwords for switches and PLCs. Additionally, Rockwell PLCs have pre-built add on instructions for direct interface with Stratix switches for monitoring within the SCADA system. The County's IT department currently uses the Cisco 3850 series of switches as their standard. The County may be able to more easily manage Stratix switches because the same command line interface (CLI) and network assistant is used with both Cisco and Stratix, simplifying configuration, deployment, and ongoing management for all switches in the network.

At the Manatee County SEWRF, the overall network is in a ring topology, whereas the other plants use more of a star/bus topology. Each Plant is its own network down to the control devices. Plants are interconnected using a County owned single mode fiber with the exception of the SEWRF which is the last plant using the redundant Metro-E network. The existing fiber to SEWRF has been damaged due to construction on I-64, and the County has been reliant on the Metro-E link (20 Mbps) instead of the much higher speed County fiber connection. During discussions on remote site communications, the County's IT department was unaware of the number of existing remote sites and noted that they primarily focus on supporting the 3 main plants: SEWRF, SWWRF, and North WRF. Network architecture diagrams for these facilities were developed during Phase 1 and are included in the appendix to provide a summary of facility network topologies.

There are also existing networked physical security devices like door cards, and a few cameras. These devices are not on their own separate network but reside on the plant control system networks. Information from these devices are not directly used in the control system and should be segmented onto their own network. Ownership and maintenance of these devices are a gray area between utilities and IT. It is recommended that if IT manages security devices in other areas of the County that these devices be managed by the IT department for a single point of responsibility in the County and to reduce the maintenance burden on utility staff in having to support another system.

5.2.1 Existing Plant Network

At the Manatee County Water Reclamation Facilities (WRFs) each system network architecture has very limited redundancy. No redundant process control communication links are in place with the exception of the SEWRF. The aggregation of single links to a single cabinet that is then backhauled through a single link also creates an architecture that further decreases the communication reliability through a single point of failure that increases the number of systems that could be affected by a single communication failure and also creates a choke point in the network where bandwidth could become an issue.

In assessing the in-plant networks, the following issues were identified:

1. Within cabinets, using non-redundant network devices and topologies increases the likelihood that a single device failure can decrease communication reliability and disrupt the operation of an entire or multiple process systems.
2. Cabinets are susceptible to power failures caused by non-redundant power supplies or single UPS that do not have automatic power transfer capabilities.

3. Single points of failure within cabinets can disrupt network communication within WRF sites and are not easily discoverable due to lack of alarms for these conditions.
4. The networks at each WRF are not monitored and a network failure cannot be easily diagnosed or repaired.

The following are overall recommendations to replace the existing Ethernet switches at each level of the network:

1. Upgrade all existing industrial network switches to Rockwell Stratix 5700.
2. All server class switches located within the plant level ring be replaced with ring compatible 5410 Stratix switches stacked for redundancy. Other server class switches should be the Cisco 2960 series switch and stacked for redundancy.
3. Layer three switches not within the ring that connect to outside networks, tie into firewalls, or require VLAN capability, it is recommend to use the Cisco 9300 series switch.

The following sections discuss the local plant networks in greater detail.

5.2.1.1 North WRF

The North WRF Plant Network is segmented into seven specific segments as shown in Figure 5.1 and facility block diagram found in the appendix. Each segment originates from the central administration building and forms a star topology. The only segment not connected to a single PLC is the segment connected in a bus topology to the old headworks and new headworks buildings. Both PLCs are connected in series. If communication is lost to the old headworks PLC, then communication will be lost to the entire headworks system.

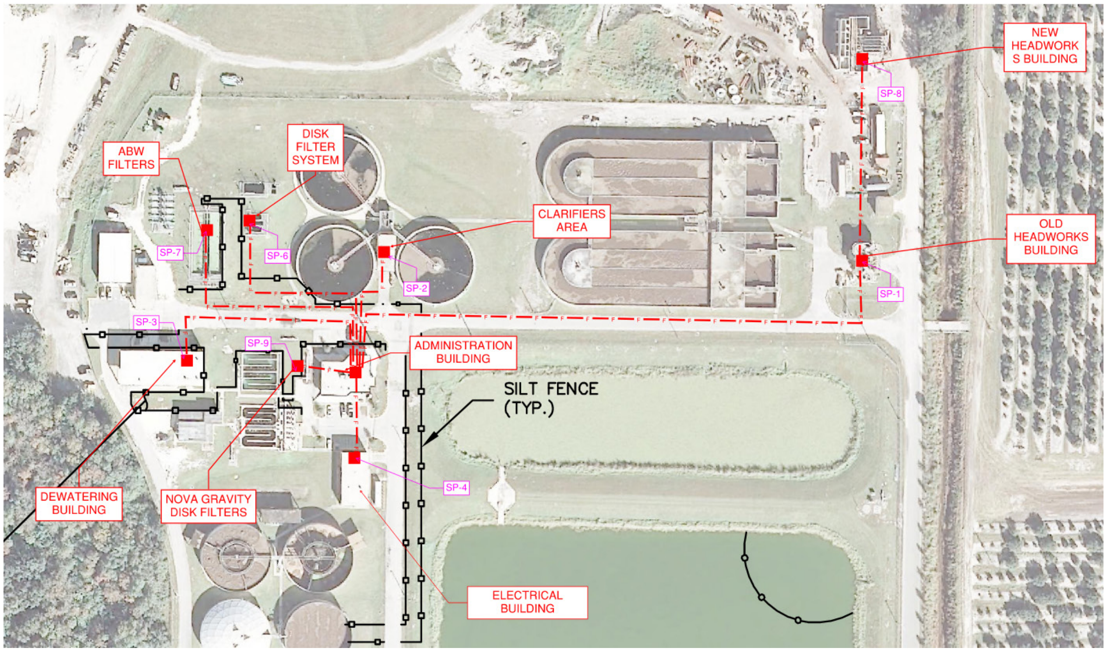


Figure 5.1 N WRF Existing Route is a Star Topology Originating From the Administration Building

Five remote sites also communicate back to the central administration building PLC cabinet via two radios. This system is a master/slave topology with a single master radio communicating to all remote sites without the use of repeaters. A polling loop is then used for the master to poll remote site information in a sequential manner establishing individual links to each location and then moving on to the next location. Two separate radios accommodate all five remote sites. The first radio communicates to the Rye Road MCMRS and Spencer Parish MCMRS sites. The first radio communicates via a 900 MHz frequency hopping spread spectrum (FHSS) unlicensed radio. The second radio communicates to the Golf Course Lake Pump Stations No. 1, 2, and 3. The second radio system communicated via a data flow systems (DFS) licensed 200 MHz system. The DFS system is not connected to the County's Citect SCADA system. These radio systems then become two additional segments routed back to the administration building PLC.

In general, if communication is lost from the central operator console network switch to the plant locations, operation should still continue normally through the PLC system but visibility and set point adjustment from the SCADA system will be lost. Each major process has its own PLC for continued system operation. However, loss of communication will currently result in loss of historical data during that time period affecting both the historical data trends and the Hach WIMS system, requiring manual data entry in some cases.

It is recommended to add additional fiber optic pathways to supplement the existing fiber optic communication system and add reliability. The new fiber optic pathways will form a ring that will encompass the plant site. These recommendations continue utilization of existing fiber optic cable and communication pathways in order to reduce costs and maintain communication during the upgrade process. Refer to Figure 5.2 for the recommended fiber route.

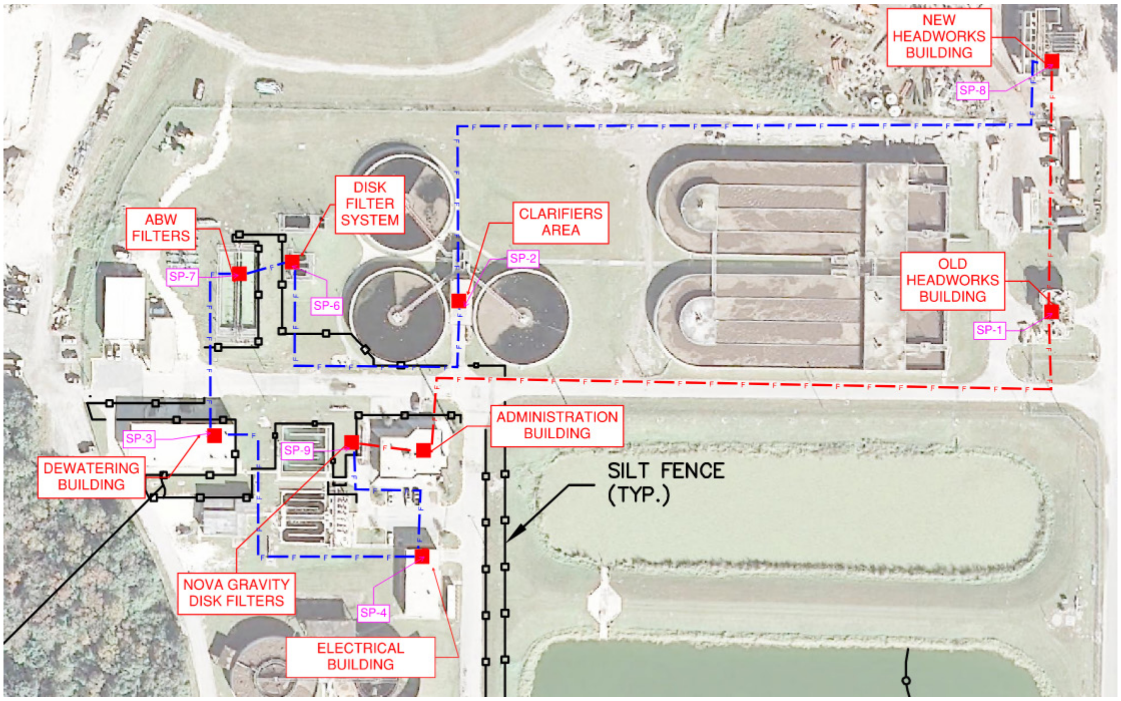


Figure 5.2 N WRF Route Proposes a Redundant Fiber Ring Around the Entire Plant Site.

5.2.1.2 South West WRF

The South West WRF Plant Network is segmented into four specific segments as shown in figure 5.3 and the facility block diagram included in the appendix. As shown in these documents, the current system topology is a hybrid star and bus. The core of the network is located at the administration building.

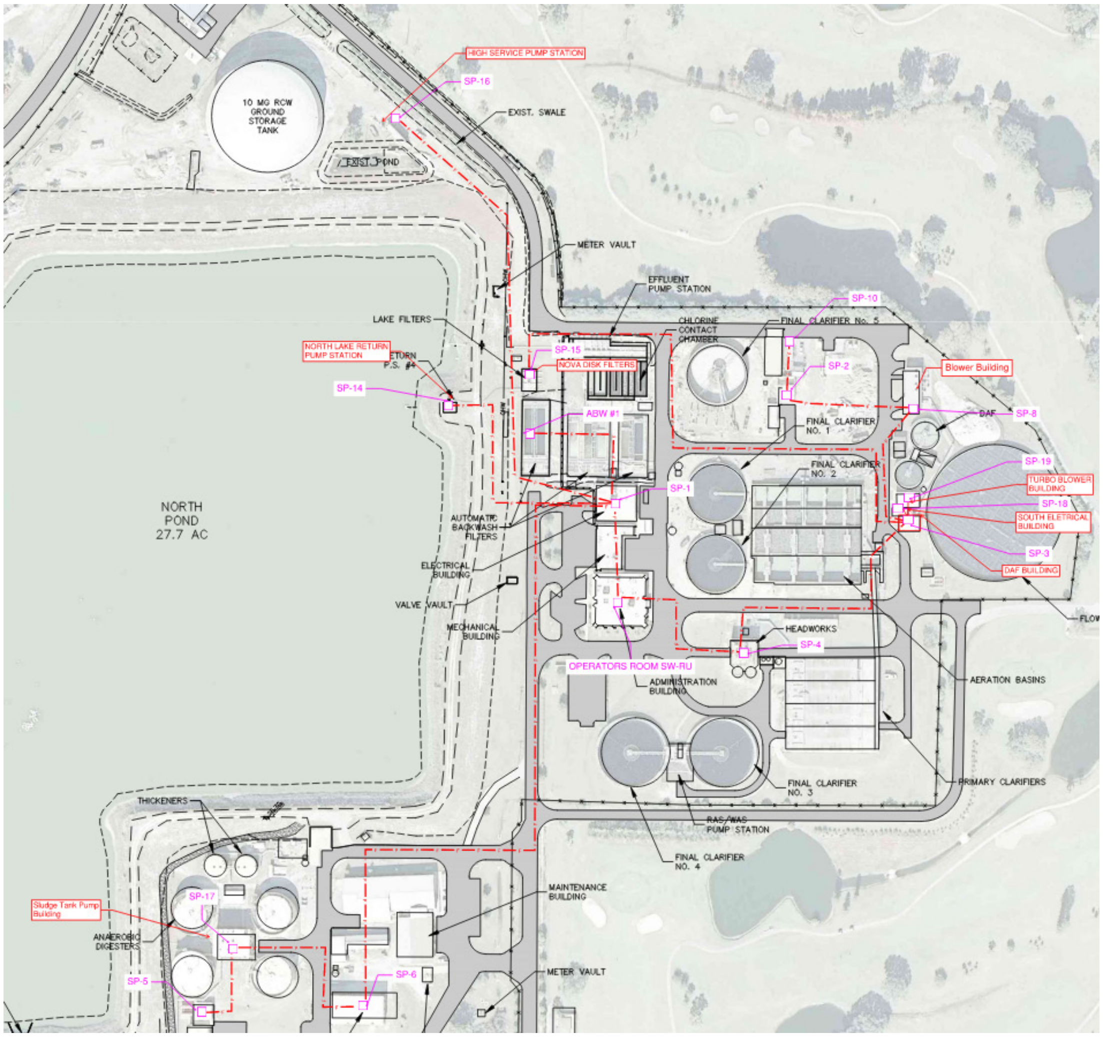


Figure 5.3 SW WRF Existing Fiber Route

Communications to PLCs within the SW WRF is accomplished through two fiber optic communication segments. Each of these segments has its own topology as well. This portion of the system architecture makes up the SW WRF Plant Network.

Two remote sites also communicate back to the central administration building PLC cabinet via radio. This system is a master/slave topology with a single master radio communicating to all remote sites without the use of repeaters. A polling loop is then used for the master to poll remote site information in a sequential manner establishing individual links to each location and then moving on to the next location. This radio system communicated via a data flow systems (DFS) licensed 200 MHz system. The DFS system is not connected to the County's Citect SCADA system. This radio system then becomes a third segment back to the administration building PLC.

The first segment connects to the electrical room control panel (SP-1), then splits off in to three daisy chained segments in a star/bus hybrid topology to following equipment:

1. High Service Pump Station.
2. North Lake Reclaimed Pump Station.
3. Dewatering Building.
4. Sludge Tank Pump Building.
5. SCADA Panel SP-5.
6. ABW #1.

If the link to the electrical room control panel is broken or fail, all downstream equipment will lose communication creating a widespread failure at the facility.

The second segment is in a bus topology with subsystems daisy chained down the line that connects to the following equipment:

1. Headworks Building.
2. DAF Building.
3. Blower Building.
4. Chemical Building.
5. ASR Well.

Three remote sites also communicate back to the chemical building PLC cabinet via a wireless access point (WAP). This WAP is an EnGenius EOC-5610. This WAP communicates to North Lake Influent Valve (SP-11), North Lake Reject Return Pump Station (SP-12), Effluent Pump Station (SP-13), and ABW#1 Bridge. This WAP is a risk to the security of the plant as this poses as a potential easy point of entry into the network. Wireless Ethernet networks are high susceptible to security threats due to the inability to properly secure authentication since the advent of the key reinstallation attack (KRACK).

If any of the links in these segments are broken or fail, all downstream equipment will lose communication. Each major process has its own PLC for continued system operation. However, loss of communication will currently result in loss of historical data during that time period affecting both the historical data trends and Hach WIMS systems, requiring manual data entry in some cases.

It is recommended to add additional fiber optic pathways to supplement the existing fiber optic communication system and add reliability. The new fiber optic pathways will form two separate rings that will encompass the plant site as shown in Figure 5.4. These recommendations continue utilization of existing fiber optic cable and communication pathways in order to reduce costs and maintain communication during the upgrade process. It is also recommended to use firewalls to secure the WAP. All traffic communicating through this access point should be encrypted and secured through a VPN tunnel and access for all other devices denied.

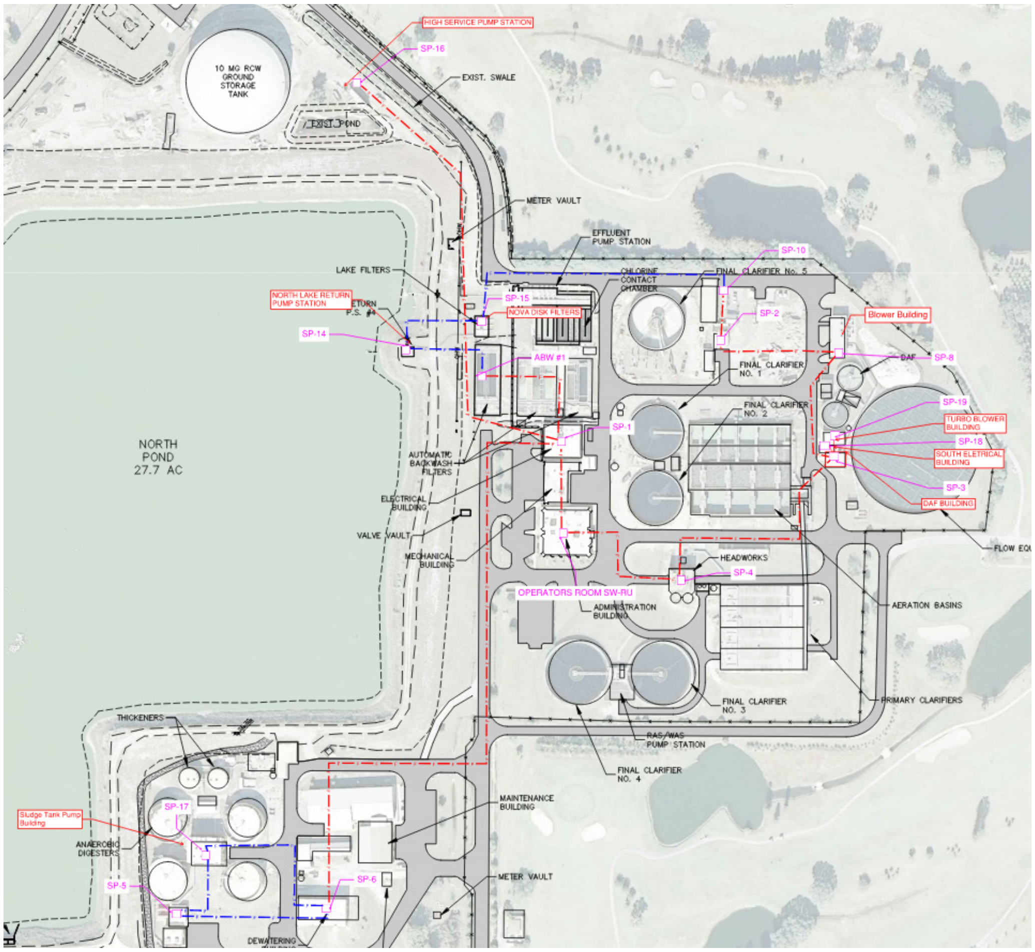


Figure 5.4 SW WRF Route Proposes Two Fiber Rings Around the Entire Plant Site

5.2.1.3 South East WRF

The South East WRF Plant Network encompasses the entire plant in a single fiber optic Ethernet ring backbone as shown in Figure 5.5.

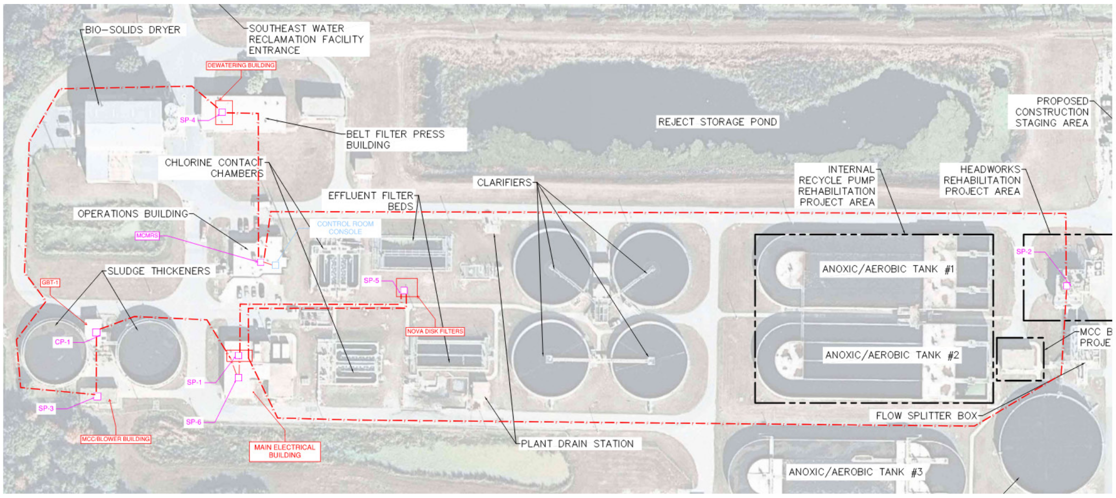
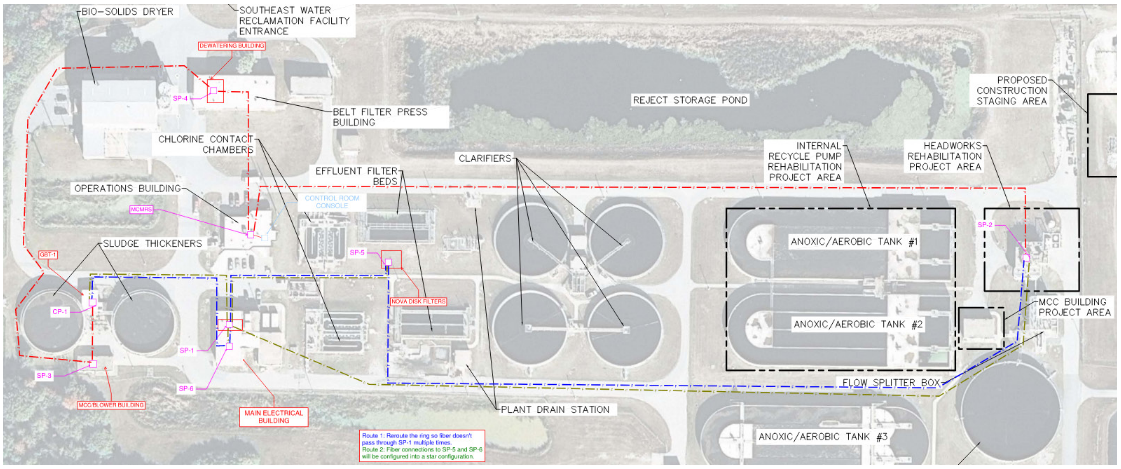


Figure 5.5 SE WRF Existing Fiber Route

Seven remote sites also communicate back to the central administration building PLC cabinet via radio. This system is a master/slave topology with a single master radio communicating to all remote sites without the use of repeaters. A polling loop is then used for the master to poll remote site information in a sequential manner establishing individual links to each location and then moving on to the next location. Two separate radios accommodate all five remote sites. The first radio communicates to the 63rd street MCMRS. The first radio communicates via a 900 MHz frequency hopping spread spectrum (FHSS) unlicensed radio. The second radio communicates to the East Lake Pump Station Site, South Lake No.1 Influent Site, South Lake No.1 Effluent Site, South Lake No.2 Influent Site, and South Lake No.2 Effluent Site. The second radio system communicated via a data flow systems (DFS) licensed 200 MHz system. The DFS system is not connected to the County's Citect SCADA system. These radio systems then become two segments back to the administration building PLC.

The fiber ring passes through and is patched multiple time in the main electrical building control panel (SP-1). The fiber segments that pass through the electrical building are connected within the ring topology but are routed in a fashion that creates a single point of failure at SP-1 affecting multiple sub-connections. Even though there is a logical network ring topology the physical routing negates any benefit at these points, and even creates a higher level of failure. The two points of failure are the fiber connections to the High Service Pump Station Room (SP-6) and Nova Disk Filters (SP-5) panel.

It is recommended to add additional fiber optic pathways to supplement the existing fiber optic communication system and add reliability. To achieve this reliability there are two options as shown in Figure 5.6. The first solution would be to reroute the fiber from the headworks building (SP-2) control panel to the SP-5 control panel along a different path to avoid having to terminate in the SP-1 panel. The second solution to reduce points of failure would be to remove the SP-5 and SP-6 control panels from the Fiber ring network and connect them in a star configuration to SP-1 using separate switches at SP-1.



Route 1: Reroute the ring so fiber doesn't pass through SP-1 multiple times.
Route 2: Fiber connections to SP-5 and SP-6 will be configured into a star configuration.

Figure 5.6 SE WRF Fiber Route Options

In order to provide the highest level of reliability, Route 1 is recommended to develop a full fiber optic ring. Costs associated with this route can be reduced by intercepting and splicing existing fiber near the effluent filter beds.

5.3 Remote Site Wireless Communication

The County presently uses radio communication systems to communicate with remote sites. The majority of communications with remote sites occurs through the existing DFS system and is managed by the DFS hyper SCADA system servers. Operators noted that they have experienced high latency when using the DFS system, and it can take as much as 30 minutes to receive acknowledgment. The system operates with redundant polling servers at each plant on different frequencies in the 200MHz spectrum. The DFS system operates on a serial communication protocol to remote units. Remote units include valves and pump stations for each plant's associated lakes. In addition to the high system latency, the following are other issues experienced with the DFS system:

- Lightning damage due to the need for poles up to 200ft.
- Unknown intermittent communication issues as the North Plant.
- UPS failures.

The DFS system at the SW WRF seems to perform the best. This is most likely because of higher transmitting power at this location.

In the past, the County has had cellular communication to some of its sites. The County noted that the MARS sites were on the Verizon cellular network, but that this did not work well, and performance has improved since the installation of Ethernet radios to replace the cellular devices. With the Verizon system, dropouts seemed to happen frequently, especially on days of inclement weather. Cellular technology has changed greatly over the years with reliability and bandwidth increasing substantially. The use of cellular has also gained an increased acceptance in the utility industry and may now be a viable option to be considered.

Another wireless network is also used for communication to remote lake valve and pump station sites. This network is a 900MHz network using GE MDS radios. The GE MDS iNET radios operate using frequency hopping spread spectrum (FHSS) in the 900 MHz spectrum. This network has had a few issues but is working well overall. Communications still have occasional issues, and the County is in need of improved troubleshooting tools and network visibility when issues arise. Additionally, all wireless networks should utilize encrypted communications for enhanced security.

At the SW WRF, a WiFi wireless access point (WAP) is also utilized for communications to remote lake valve and pump stations as previously noted. This is then a third type of wireless communication currently used within the control system.

Overall, each wireless communication system in use has its pros and cons and varying degrees of reliability and points of failure. Having a single wireless technology for associated facility lake valves and pump stations would decrease system complexity and aid in troubleshooting.

5.4 SCADA Network, DMZ, and Backhaul

The SCADA network extends between all County facilities and all have points of interconnection through the County Wide Area Network (WAN). Each facility has its own dedicated SCADA system infrastructure and local network; however, data is exchanged between sites over this network to relay remote site information. The overall SCADA network topology is what is known as a flat topology. This means that every device on the network has a similar network address to all other devices on the network and is on the same subnet. This topology does not match the current SCADA application topology where each site has a separate and dedicated SCADA system. The network topology currently employed, allows all devices to communicate with each other. Potential issues with this type of topology include the following:

- Higher potential for network errors such as IP duplication.
- Higher potential for excessive bandwidth usage and broadcast storms from multicast messages and other system communications.
- Larger system attack surface.
- More difficultly in controlling and managing network traffic.

In this type of network, a higher potential exists for devices communicating with each other that have no real need for communication. This can lead to improper system operation or network latency and even outages. It is generally recommended to segment control systems for better system control and to limit communications to those necessary for proper system operation. A description of this type of network segmentation is further discussed in the cybersecurity section of this TM.

The County currently has limited defined and implemented segmentation in the control system network and this network is actually flat. Additionally, some computer systems within this network are dual homed between the control system and County IT system networks. This practice bridges these two networks together providing a direct connection between control system and IT networks without having any type of routing or network security devices in place to control and secure traffic. This practice also exposes control system assets to the Internet to the potential exposure to malware and ransomware that could spread between networks through these connections. It is recommended to use completely separate infrastructure for IT and control system networks. Any type of connectivity between networks should be done through network security appliances. Additional security considerations are also listed in Chapter 7 of the report.

The County is currently undergoing some network upgrades to better segment and secure their systems. The main focus of these upgrades are centered on connectivity to the County WAN between facilities. Current upgrades include the addition of dual firewalls at each facility to secure traffic and create VPN tunnels between facilities. This will add a layer of segmentation that previously did not exist within the network. The use of high availability firewalls in this system is also a great benefit to eliminate network downtime due to upgrades or changes in the firewall system as firewalls can be managed individually and rebooted separately to prevent network outages. The control system network is still lacking full segmentation and a DMZ layer between control system and enterprise level IT networks.

As upgrades are made to the County's control system, network addressing, and network architectures should also be revised to add segmentation and flexibility to expand as more and more devices are being added with network capabilities. The County currently utilizes network connectivity to new motor control and VFD devices and has expressed interest in network connectivity to instruments as well including the use of Ethernet and HART protocols. Having segmentation provides an ability to control network traffic and implement security for high reliability. An example is shown in the following figure. In this example applied to the County, each facility would have its own dedicated SCADA network. Within each facility specific sub networks for control, maintenance, and security would be used to segment devices that do not need to communicate to each other. These networks would be brought back to a local firewall or layer 3 device that would coordinate communications to specific servers as required at the facility. A facility firewall device would then control communications between facilities and back to any centralized SCADA devices. At this level, a DMZ connection to the Enterprise level would be established as necessary for data sharing to Enterprise resources and for any type of needed remote or mobile access to the system.

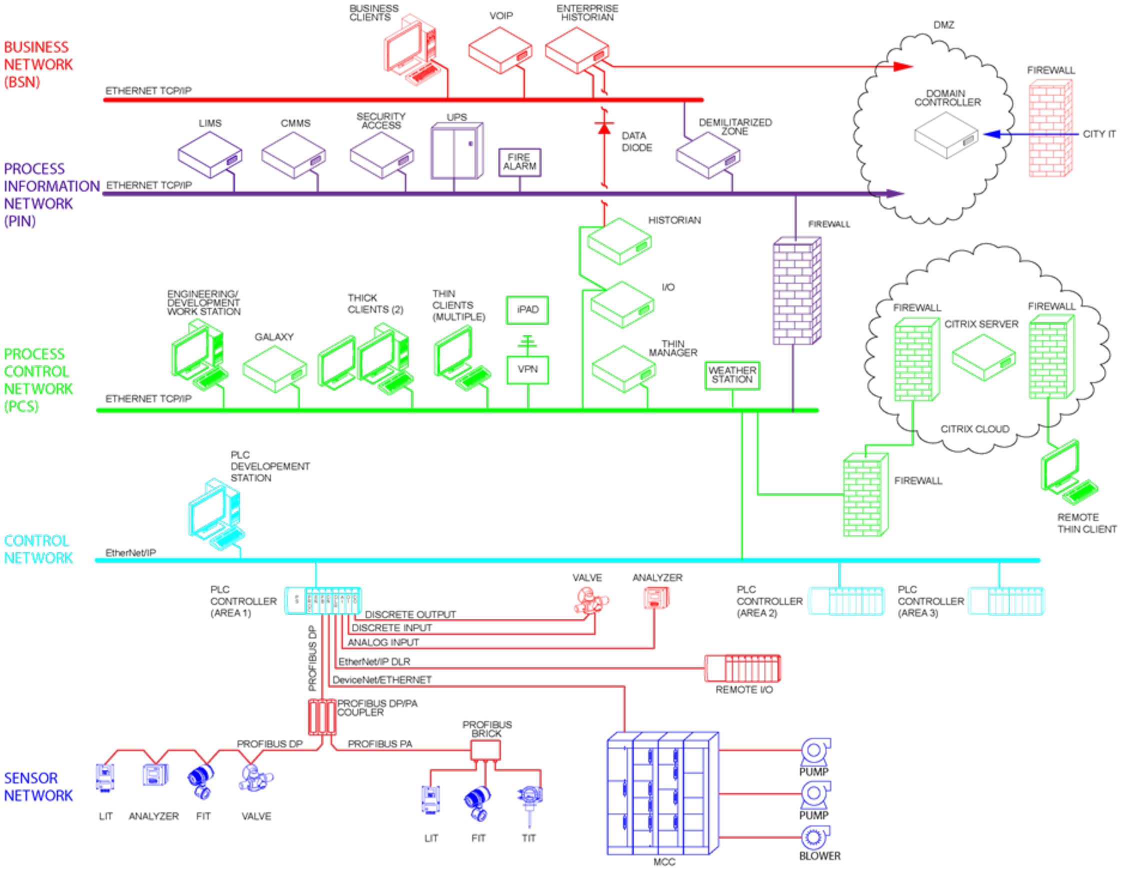


Figure 5.7 Example Control System Network Segmentation

5.5 SCADA System Server Infrastructure

The County's SCADA server infrastructure consists mainly of workstations used to run SCADA server applications and SCADA clients that are both workstation and touchscreen PCs. The following is a summary of the computer system infrastructure:

Table 5.1 SW WRF SCADA PC Summary

Description	Device Type	Quantity
SCADA Server	Workstation	2
SCADA Client	Workstation	2
SCADA Client	Touchscreen	6
Programming Computer	Laptop	1

Table 5.2 SE WRF SCADA PC Summary

Description	Device Type	Quantity
SCADA Server	Workstation	4
SCADA Client	Workstation	3
SCADA Client	Touchscreen	2

Table 5.3 N WRF SCADA PC Summary

Description	Device Type	Quantity
SCADA Server	Workstation	2
SCADA Client	Workstation	1
SCADA Client	Touchscreen	5

Table 5.4 MCMRS SCADA PC Summary

Description	Device Type	Quantity
SCADA Client	Touchscreen	3

The following table outlines the totals for the County SCADA PC devices

Table 5.5 Total SCADA PC Summary

Description	Device Type	Quantity
SCADA Server	Workstation	8
SCADA Client	Workstation	6
SCADA Client	Touchscreen	16
Programming Computer	Laptop	1
	TOTAL PCs	31

In total, there are 31 computers that must be maintained in the system. This infrastructure utilizes workstation operating systems such as Windows XP, Windows 7, and Windows 10 that do not have nearly the security features or hardening available from server class operating systems and require constant patching to minimize vulnerability threats. Additionally, the lack of a true server environment limits the ability to implement the following server functions directly on the control system network:

- Authentication security and group policies using active directly.
- DHCP and DNS network functions.
- Network Time Servers for coordinated network time.
- Software update services and patch management.
- Network Management.
- System Logging.
- Anti-Virus management.
- System Backups.

Currently, the County does not employ any of these features on the control system network. This make the SCADA environment difficult to manage and secure. It is recommended to implement a server environment with the above listed functions in order to reduce security risks and increase the ability to manage and monitor these systems.

5.6 Summary of Current Performance

- Non-managed Ethernet switches.
- Flat control system network topology.
- No true server infrastructure.
- Limited network path redundancy.
- No formal written cyber or physical security plans or policies.
- Limited cyber security implementation.
- Limited resources for cyber security support.
- Limited physical security implementation.

5.7 Best Practices

- Fully managed network switches throughout the network.
- Plant wide network redundancy utilizing ring or similar topology.
- Formal and comprehensive security programs in place.
- Cybersecurity practices and implementations completed in accordance with the NIST Framework and AWWA Cybersecurity Use Case Tool recommendations.
- Dedicated and responsible security support staff.
- Multi-layered physical security implementation in accordance with industry standards.
- Staff trained in their roles and responsibilities for security at all staff levels.

5.8 Initial Recommendations for Assessment

Based upon the information obtained, the following is a listing of initial system recommendations:

- Utilizing Rockwell Stratix network switches for Plant Level.
- Utilizing Cisco layer 2 and layer 3 network switches for HMI level management and routing.
- Implementation of a virtualized server infrastructure and backup and recovery system.
- Upgrade plant fiber optic networks to a ring topology and minimize single points of failure.
- Develop a Cybersecurity Plan and Policies to base implementation around.
- Developed a layered SCADA network system architecture.
- Add network security components and solutions during SCADA system upgrades.
- Develop a Physical Security Plan and Policies.
- Determine roles and responsibilities of staff to manage, maintain, and upgrade security system components.

5.9 Summary

Overall, the County SCADA system network components do not meet current industry standards for networking features and management. Limited cybersecurity implementations are currently in place, and physical security implementations do not meet industry best practices. The County should upgrade their in plant network infrastructure at each facility to increase reliability and security. Computer systems should also be upgraded, and server services configured to provide additional security and management within the SCADA system.

Chapter 6

ENTERPRISE DATA INTEGRATION ASSESSMENT

6.1 Introduction

This chapter presents the present state of information flow between process information systems and the utility software applications, as well as data exchange procedures and the staff's user interfaces. The goals of this chapter are to identify the current enterprise data integration gaps and provide a road map for the desired future data exchange needs throughout the utility.

6.2 Present State

Currently, Hach WIMS is used as the central database where enterprise level process data is stored and accessed for system benchmarking, developing key performance indicators, and generating reports. Data from the SCADA system is currently integrated automatically into the WIMS system through the use of a data collector integrated with the Wonderware Historian system. The Hach WIMS platform is a fairly new addition to the County's process data management system and continues to be further developed and utilized to streamline data management and provide staff with useful information and a platform for generating system reports.

Currently, these systems are managed by the Utility Maintenance Supervisor including both development and system maintenance, licensing, and upgrading. Having a dedicated application manager such as this is a best practice approach to ensuring this system is well maintained and utilized to its fullest extent. The Utility Maintenance Supervisor has completed a lot of development within the Hach WIMS system and made it a useful tool for staff. The following are some key benchmarking tools that the WIMS system should provide:

- Chemical Usage.
- Electricity Usage.
- Facility Flow Report.
- Compliance Data Reporting.
- Solid Handling.

These benchmarks should be fully automated with automated data flow from SCADA with possibly some manually entered data. The goal moving forward is to automate as much of this information as feasible. Additionally, information in this system should be utilized to make changes in system operation. A starting point would be to first use information in the WIMS system to provide a baseline for comparison for future changes or modifications to operation or system components.

In addition to system benchmarking and monitoring, the WIMS system can also be utilized in developing the following monthly reports:

- Polymer use.
- kW / MG treated effluent.

- Number of Corrective vs. Preventive Work Orders.
- Recycle flow.
- Irrigation flow.
- Treated flow.
- Biosolids Quantity.

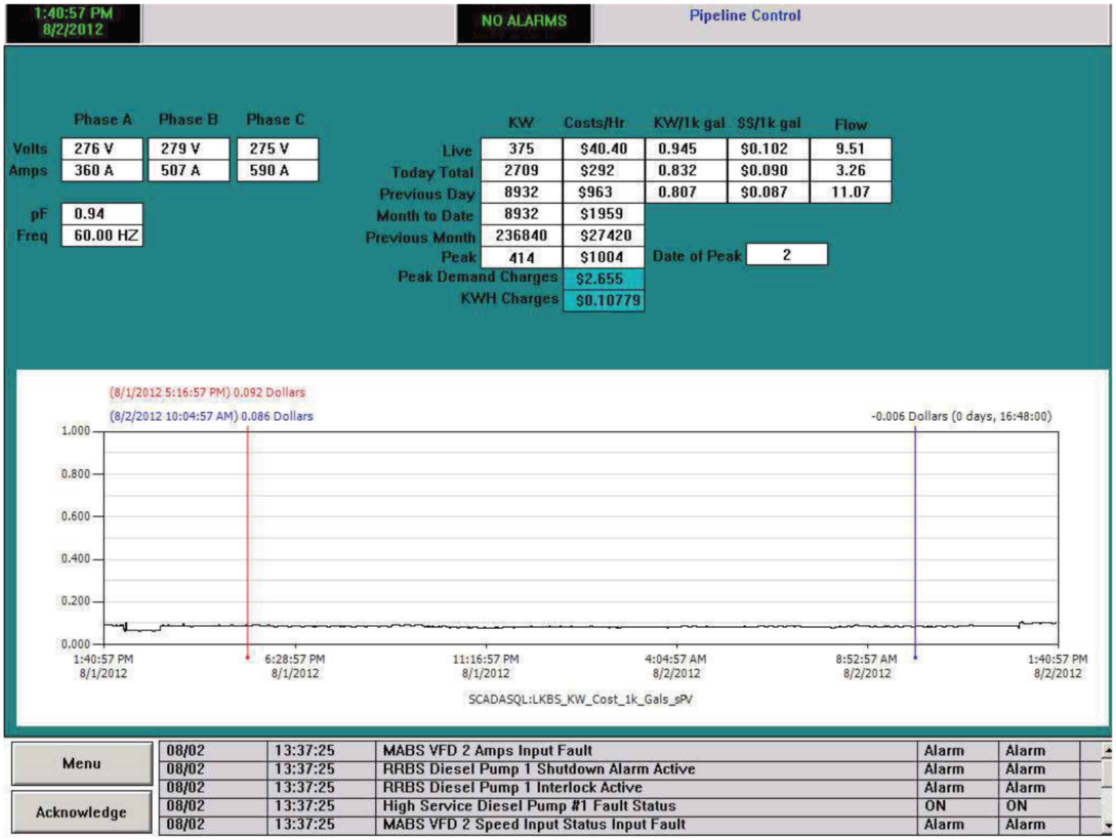
Most of this report information could be driven out of Hach WIMS with data from the SCADA system. Other daily and custom reports should also be developed in the HACH WIMS system to support operations and management. Additionally, engineering staff should be trained in the use of Hach WIMS and provided access in order to view and extract data.

Hach has also developed a mobile utility add-on called Claros that can be used to enter and view data within the WIMS system. This addition to the WIMS system provides functionality for a higher level of instrument management, manual data entry, general data management, and process monitoring and optimization. A key feature of the Claros system is the ability to manage instruments including preventive and predictive maintenance and verifying instrument data. This can be used along with the Hach instruments already installed in the County's system to provide a higher degree of instrument management and calibration.

6.3 SCADA and Operational Data

At this time, it does not appear that more instrument or sensor data is necessary in the County's WRF system as the appropriate level and type of instrumentation is installed at each facility. As new equipment is being added, it is generally being added with digital interfacing such as HART or Ethernet for instrumentation, motor controllers, drives, and electrical gear that does provide more information which can be used to integrate with future systems for enhanced predictive maintenance and maintenance troubleshooting. The Hach Claros system also has an instrument management module that integrates directly with Hach's Prognosys predictive diagnostic system and Hach WIMS. The Prognosys system also provides mobile sensor management through Claros to allow monitoring and management from anywhere at any time. While this might not be a current need for the County, the progress and development of Claros systems and add-ons should be monitored as potential future solutions for issues that may arise at the County's facilities including a potential solution to assist in calibration consistency and troubleshooting.

Some items that could currently be explored during the SCADA platform migration is integration of more real-time power management functions into either the SCADA or Hach WIMS system. Currently kW-h/MG treated can be calculated but real-time values and trends are not available. This information along with inputs for cost, peak demand hours and levels along with kW-h/MG versus gpm trends can aid in finding optimal flow points as well as determining most efficient operating scenarios and equipment. This can be used to determine points where equipment replacement may be cost favorable on an energy use basis instead of an operate to fail basis and would generate a useful baseline for any potential energy service type funding or loan contracts where capital improvements are paid for through energy savings potential. The following provides an example of an energy management overview screen.



1:40:57 PM 8/2/2012 | NO ALARMS | Pipeline Control

	Phase A	Phase B	Phase C
Volts	276 V	279 V	275 V
Amps	360 A	507 A	590 A

pF	0.94
Freq	60.00 HZ

	KW	Costs/Hr	KW/1k gal	$$/1k gal	Flow
Live	375	$40.40	0.945	$0.102	9.51
Today Total	2709	$292	0.832	$0.090	3.26
Previous Day	8932	$963	0.807	$0.087	11.07
Month to Date	8932	$1959			
Previous Month	236840	$27420			
Peak	414	$1004	Date of Peak	2	
Peak Demand Charges		$2.655			
KWH Charges		$0.10779			

08/02	13:37:25	MABS VFD 2 Amps Input Fault	Alarm	Alarm
08/02	13:37:25	RRBS Diesel Pump 1 Shutdown Alarm Active	Alarm	Alarm
08/02	13:37:25	RRBS Diesel Pump 1 Interlock Active	Alarm	Alarm
08/02	13:37:25	High Service Diesel Pump #1 Fault Status	ON	ON
08/02	13:37:25	MABS VFD 2 Speed Input Status Input Fault	Alarm	Alarm

Figure 6.1 Example Energy Management Screen

6.4 Asset Management

Asset management and work order tracking also provide useful data in optimizing system performance, planning equipment upgrades, and monitoring maintenance efficiency and effectiveness. Some information such as corrective vs. preventive work orders are being monitored but as noted previously, very little on the SCADA system is being monitored. Past information could have been useful in quantifying the effectiveness of the use of external integrators for SCADA system maintenance and for planning of equipment replacements due to age, condition, cost of maintenance. As the SCADA system is upgraded and continues to depend on more technology requiring additional maintenance and system updates, the following system statistics should be considered:

- Financial:
  - SCADA system expense as a percentage of overall utility system expense.
  - Amount/percentage spent on external vs. internal labor and support.
  - Amount/percentage spent on new vs. replacement equipment and systems.
- Assets:
  - Mean time between component failures.
  - Mean time to repair.
  - Average age of major components.
  - Highest repair frequency by component.
  - Highest cost repairs by component.

- Performance:
  - Percentage of system fully patched and updated.
  - Downtime of SCADA system (hours, minutes).
  - Percentage Uptime / Availability.
  - Percentage of known vulnerabilities mitigated.
  - Work order processing time.
- Staff:
  - Yearly percentage of positions filled.
  - Percentage of required training completed.
  - Missed hours.
  - Average turnover per position.

6.5 Effective Utility Management

A major driver for the County is to empower staff with data and use this data to make informed decisions. Data is now not just used to analyze and report, but the real value of data is to drive business decisions and make more informed decisions about operations, upgrades, and business changes and directives. The AWWA, along with the U.S. EPA and nine other association partners, has defined a program known as Effective Utility Management (EUM) help water and wastewater utility managers make informed decisions and practical, systematic changes to achieve excellence in utility performance. This program can be actively participated in to provide utility benchmarking and the methods and tools can also be used independently in order to better the management of a utility. EUM is based on the following ten attributes:

- Product Quality.
- Customer Satisfaction.
- Employee and Leadership Development.
- Operational Optimization.
- Financial Viability.
- Infrastructure Strategy and Performance.
- Enterprise Resiliency.
- Community Sustainability.
- Water Resource Sustainability.
- Stakeholder Understanding and Support.

The EUM primer can be found in the appendix which outlines the ten attributes, five keys to management success, self-assessment, and implementation of EUM. In addition to this information, the following outlines the AWWA's list of utility benchmarking performance indicators in the areas of Organizational Development, Business Operations, Customer Service, Water Operations, and Wastewater Operations.

- Organizational Development:
  - Organizational Best Practices.
  - Staffing Levels:
    - Total FTEs.
    - FTEs by Job Category (%).
  - Training (hours per employee).
  - Emergency Response Readiness Training (hours per employee).
  - Customer Accounts (accounts per employee).

  - Employee Turnover (%).
  - Retirement Eligibility (%).
  - Employee Health and Safety Severity Rate.
  - Recordable Incidents of injury or illness.
  - Near Misses.
  - Strategic Workforce Planning.
  - Employee Vacancies.
- Business Operations:
  - Debt Ratio (%).
  - Return on Assets (%).
  - Days of Cash on Hand.
  - Debt-Service Coverage Ratio.
  - Days of working capital.
  - Operating Ratio (%).
  - Bond Rating.
  - Insurance Claims:
    - Severity of Insurance Claims.
    - Average Severity.
  - System Inspection (%).
  - System Renewal/Replacement (%).
  - Triple-Bottom-Line Index (%).
  - Sustainability:
    - Nutrient Recovery.
    - Biosolids Reuse (%).
    - Nonportable consumptive use (%).
    - Habitat/watershed protection goals.
    - Green Infrastructure planning.
    - Energy Optimization planning.
- Risk and Resiliency:
  - Risk Assessment and Response Preparedness.
  - Emergency Response Plan.
  - Recovery and Mitigation.
  - Cybersecurity Preparedness.
- Customer Service:
  - Service Complaints:
    - Customer Service Complaints/1,000 accounts.
    - Customer Service Complaints/population served.
    - Technical Service Complaints/1,000 accounts.
    - Technical Service Complaints/population served.
- Call Center Indicators:
  - Average Talk Time (minutes).
  - Average Wait Time (minutes).
  - Abandoned Calls (%).
  - Average Calls per Call Center Representative.
  - First Call Resolution.
- Customer Service Cost per Account ($/account).

- Residential Service Charges:
  - Residential Cost of Water Service ($/month).
  - Residential Cost of Wastewater Service ($/month).
  - Residential Cost of Stormwater Service ($/month).
- Bill Accuracy (Errors/10,000 billings):
  - Frequency of Billing.
  - Estimated Billing Rate.
  - Metering Prevalence.
  - Metering: Frequency of Meter Reads.
  - Metering: Read Success Rate.
- Per Capita Consumption (gal/person/day).
- Service Affordability:
  - Water Service Affordability (%).
  - Wastewater Service Affordability (%).
  - Stormwater Service Affordability (%):
    - Delinquency Rate.
    - Low-income assistance program offered.
    - Low-income billing assistance rate.
    - Stakeholder Outreach Index.
    - Customer Service - Preferred Method of Contact.
    - Water Service Disruptions:
      - Disruptions of water service (outages/1,000 accounts):
        - Planned by Event Duration (< 4hr, 4-12 hr, >12hr).
        - Unplanned by Event Duration (<4 hr, 4-12 hr, >12 hr).
    - Average Time to Address Water Service Disruptions (hr).
    - Disruption Frequency of Water Service.
  - Wastewater Service Disruptions:
    - Disruptions of wastewater service (outages/1,000 accounts):
      - Planned by Event Duration (< 4hr, 4-12 hr, >12hr).
      - Unplanned by Event Duration (<4 hr, 4-12 hr, >12 hr).
    - Average Time to Address Wastewater Service Disruptions (hr).
    - Disruption Frequency of Wastewater Service.
- Water Operations:
  - Regulatory Compliance - Water (%).
  - Water Produced (MGD per employee).
  - Water Supply:
    - Current Water Demand (%).
    - Available Water Supply (years).
  - Water Distribution System Integrity:
    - Leaks/100 miles of pipe.
    - Breaks/100 miles of pipe.
    - Combined Leaks and Breaks.
  - Hydrant effectiveness / out of service rate.
  - O&M Costs for Water Services:
    - ($/account).
    - ($/MG).

        - ($/100 miles of pipe).
        - Treatment O&M Costs.
        - Distribution O&M Costs ($/100miles of pipe).
        - O&M Percentage of Water Services.
    - Maintenance – Water:
        - Planned Maintenance (%) [Overall, Linear, Vertical Ratios].
        - Corrective Maintenance to Production (hr/MG).
        - Planned Maintenance to Production (hr/MG).
        - Corrective Maintenance to Distribution System Length (hr/100 miles of pipe).
        - Planned Maintenance to Distribution System Length (hr/100 miles of pipe).
    - Energy Consumption - Water (kBTU/year/MG).
    - AWWA Water Audit Software.
- Wastewater Operations:
    - Wastewater Compliance Rate:
        - Wastewater Treatment Operations (%).
        - Collection System Operations (%).
    - Wastewater Processed per employee.
    - Non-Capacity Sewer Overflow Rate (per 100 miles of pipe).
    - Capacity Sewer Overflow Rate (per 100 miles of pipe).
    - Collection System Integrity (failures/100 miles of pipe).
    - O&M Costs for Wastewater Services:
        - ($/account).
        - ($/MG).
        - ($/100 miles of pipe).
        - Collection O&M Costs ($/100miles of pipe).
        - Treatment O&M Costs ($/MG).
        - O&M Percentage of Wastewater Services.
        - O&M Percentage of Stormwater Services.
    - Maintenance – Wastewater:
        - Planned Maintenance (%) [Overall, Linear, Vertical Ratios].
        - Corrective Maintenance to Treatment (hr/MG).
        - Planned Maintenance to Treatment (hr/MG).
        - Corrective Maintenance to Collection (hr/100 miles of pipe).
        - Planned Maintenance to Collection (hr/100 miles of pipe).
    - Energy Consumption - Wastewater (kBTU/year/MG).

These benchmarks can be used to self-assess and track progress and used to compare to other utilities to discovery potential areas of improvement. While some of these benchmarks may not currently be tracked, this list does offer guidance for the development of future systems in order to provide more automated tracking of these data points in asset management and customer service systems. While the majority of these are not directly correlated to the SCADA system or SCADA data outputs they can be used as a basis of SCADA system benchmarking as well and adapted for use on SCADA related systems and components. Additionally, the use of the SCADA system and its data can be used to greatly impact utility performance and the corresponding benchmarking KPIs. Optimization strategies can be used with the help of automation in order to reduce operating costs, SCADA data can be used to shift maintenance into more of a preventive mode, and SCADA can be used to lower energy costs among other solutions. By monitoring these KPIs and looking for ways to improve, each function within the utility, including SCADA, can provide methods of more effective utility operation.

6.6 Future Trends

The following are currently some of the fastest growing trends in the industry:

- Higher level system visualization.
- Increased IoT / IIoT.
- Increased migration to the Cloud.
- Artificial Intelligence.

6.6.1 High Level System Visualization

In line with Effective Utility Management and benchmarking is the desire to have this information real-time in order to immediately see areas of improvement and change them as soon as they are noticed instead of waiting for annual reports to be compared. To provide this level of information in a way that can be quickly processed, business intelligence or BI systems have been developed to quickly and intuitively provide visualization of key data and performance indicators much like a SCADA system. Systems in this market include Microsoft Power BI, Tableau, and CRM Saleforce among a very crowded space. These software systems have the ability to connect to a multitude of databases like SQL, Oracle, and SAP to pull in financial data as well as connect to almost any Application Programming Interface (API). These systems can be premise based or hosted in the cloud with the majority being cloud hosted due to easier integration with other cloud based and web-based systems.

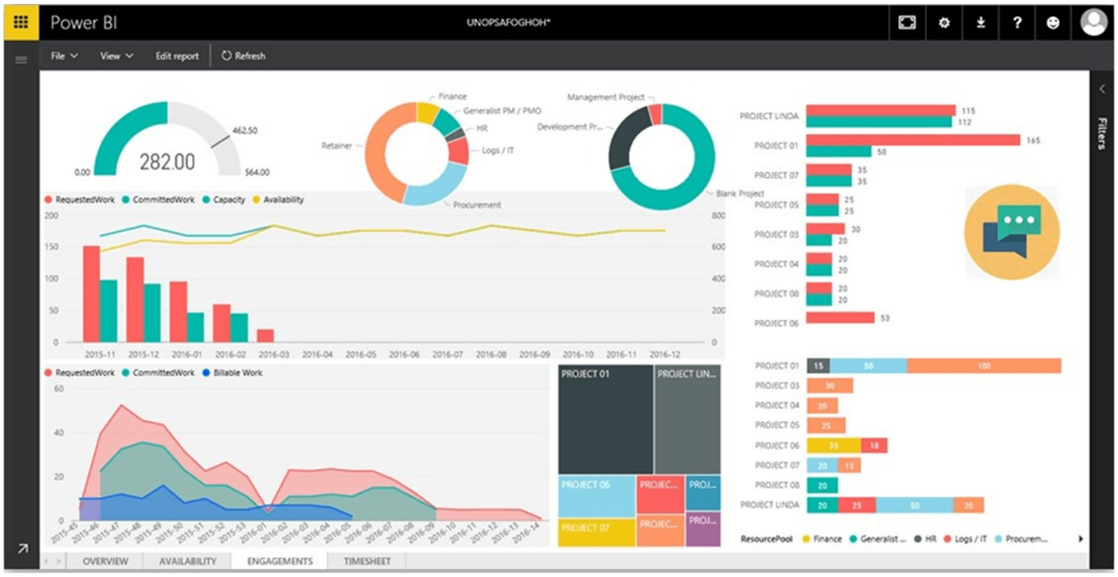


Figure 6.2 Example BI Dashboard

These systems are ready for use with any business. A starting point for many utilities is to utilize EUM benchmarks and KPIs as a starting point and develop additional KPIs and data relationships as necessary for effective business management. These tools can be used at all levels of the organization but similar to SCADA systems must be developed and customized to meet exact needs of the business. These systems much simpler to develop and general IT professionals have the skills in order to develop most necessary tools. With the systems that the County already has in place, implementation within the Hach WIMS system or use of the AVEVA Insight system would provide a simplified integration for developing higher level visualization into the facilities.

6.6.2 Increased IoT and IIoT

The Internet of Things (IoT) and Industrial Internet of Things (IIoT) continue to expand with more and more devices and sensors gaining integral transmitters and numerous applications being developed to read these sensors and perform computations to provide instant useable information. This area will continue to expand with the desire to have smart cities for better operations and management. Common uses today within utilities are the following:

- Advanced Metering Infrastructure (AMI) for water meter reading.
- Distribution and PRV pressure monitoring.
- Fire Hydrant pressure monitoring.
- Collection system levels, flows, pressure, and valve and gate positions.

A host of other options exist and basically any parameter that can be measured with a discrete or 4-20mA signal can be monitored as an IIoT device. Integration is split between cloud hosted data systems and SCADA systems and in many cases both. The main use case for these systems is pairing them with useful indicators and analytics in order to make decisions where previously data could not be efficiently gathered or analyzed. These systems will become increasingly prevalent with an increased use in analytics systems to make informed decisions.

6.6.3 Increased Migration to the Cloud

As more systems have direct cloud integration and as cloud-based systems gain more acceptance, more and more systems will shift to being cloud based. We are already seeing this with many commercial software packages where we interact more with web-based cloud hosted systems than we do with installed software systems. SCADA and other automation system software is migrating in this direction mainly from vendors following industry trends and to provide solutions for IoT infrastructure.

Some SCADA systems have gone fully cloud based such as XiO and solutions from companies such as Xylem. Most SCADA based systems found in the cloud are used to support specific hardware such as Mission and Ayyeka who have built cellular based packaged RTUs and cloud-based applications that pair with these devices for rapid deployment. One item to note is that this concept can be built into a non-traditional cloud-based system by following a similar model of creating a packaged or standard RTU design for similar systems, employing reliable and quickly deployable communications, and developing standard software templates to go along with these systems. This is the recommendation for the County's remote sites in order to make migration to new equipment fast and efficient and future maintenance simple.

Another item to note about cloud-based systems as well is that there are three service models for cloud computing and four deployment models.

Service Models:

1. Software as a Service (SaaS).
2. Platform as a Service (PaaS).
3. Infrastructure as a Service (IaaS).

Deployment Models:

1. Private Cloud.
2. Community Cloud.
3. Public Cloud.
4. Hybrid Cloud.

The most prevalent perception of cloud-based SCADA solutions follows the Software as a Service (SaaS) model using a public cloud deployment method as these are the most heavily marketed cloud-based solutions. Currently, public cloud deployments of the SCADA environment are not recommended, however, cloud-based solutions do provide current benefits such as hosted virtualization schemes and may prove to offer enhanced security and data integration in the future as these systems continue to improve

The National Institute of Standards and Technology (NIST) has begun developing documentation and best practices for the utilization of cloud computing for government and critical infrastructure:

1. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.
2. NIST SP 800-145: The NIST Definition of Cloud Computing; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
3. NIST SP 800-146: Cloud Computing Synopsis and Recommendations; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf.
4. NIST SP 500-299: DRAFT NIST Cloud Computing Security Reference Architecture; http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf.

These standards continue to evolve, and new standards produced as the industry changes, and current guidelines referenced for any type of cloud-based deployment.

6.6.4 Artificial Intelligence

Artificial Intelligence or AI continues to gain ground in many industries where enormous amounts of data can be analyzed in order to make better decisions. Utilities are one of these industries that generates a lot of data through SCADA systems and hosts a lot of associated financial system data making it a good candidate for potential AI solutions. Additionally, with utilities deploying more and more IIoT and IoT devices this data continues to increase creating a need for solutions to analyze this information for more informed decision making.

Currently in the industry, most of the work in this sector is being done to optimize water distribution, waste and storm water collection, and to prevent combined sewer overflows in order to maximize the use and capacity of current infrastructure to avoid costly capital expenditures for new and larger infrastructure to handle these demands. Systems being made by companies such as Optimatics and Emnet, now owned by Xylem, have developed AI solutions also known as Real Time Decision Support Systems (RTDSS) to provide operations staff suggested control settings in order to optimize operations.

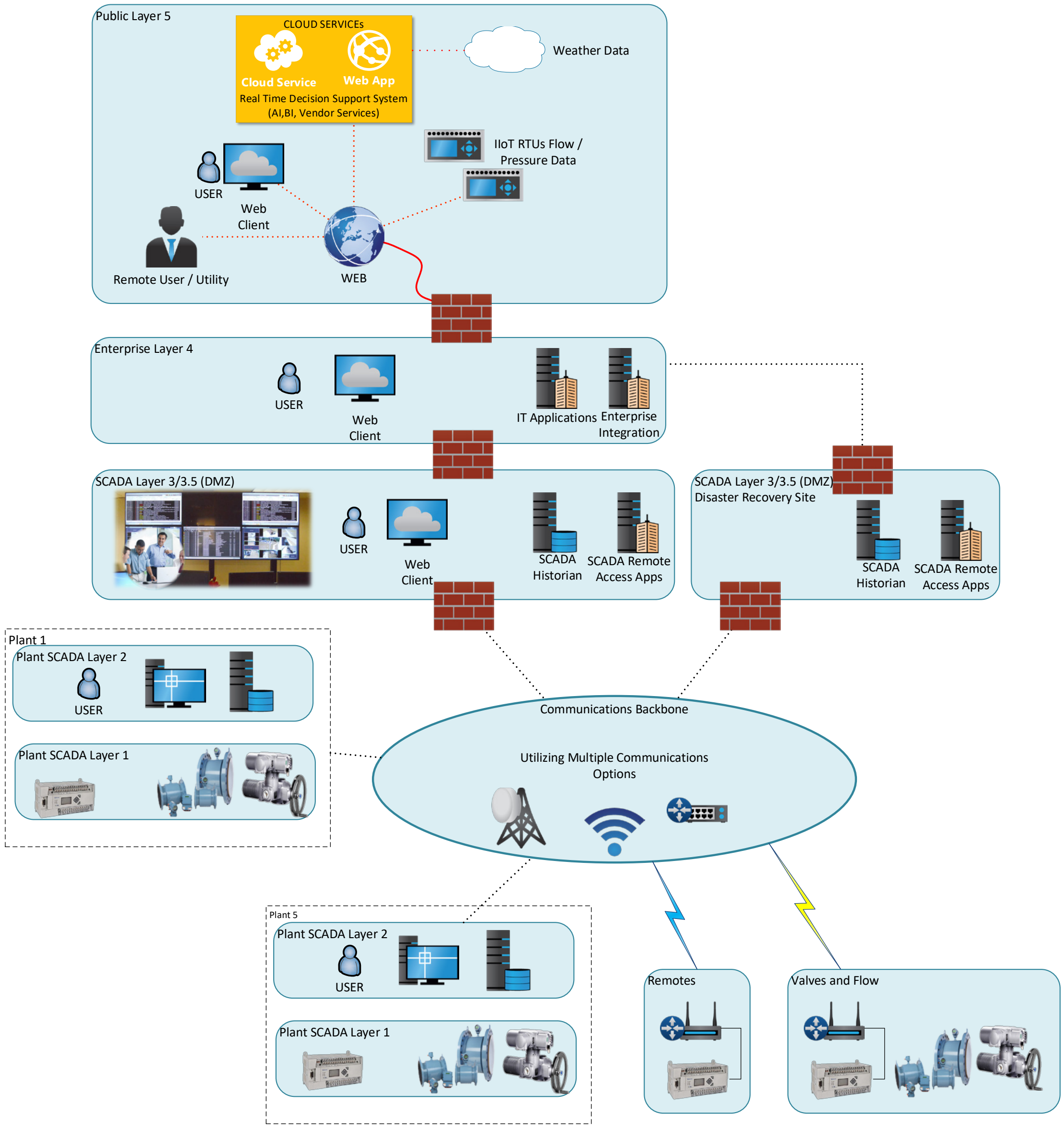


Figure 6.3 Example RTDSS System Architecture

In these systems a digital copy or digital twin of the real-life system is made using a computer model calibrated with historical data that can accurately mimic the real-world system. This model is then given current system conditions through SCADA and IIoT information and produces a response predicting a future scenario and developing a mitigation or optimization strategy to address these conditions. These systems are primarily cloud based since the cloud offers these benefits for these systems:

- Developers can tweak one overall AI engine for all customers.
- Developer can tune the AI engine using data from multiple customers.
- Easier data transfer with IoT and IIoT sensors.
- Easier ability to incorporate data from other sources such as weather NOAA and USGS.

This is also part of the reason why these systems are not currently directly connected to SCADA systems, but the future will likely bring more automation in the response to the outputs of these systems and direct tie-ins with control systems for real-time optimization.

With all of these future technologies, there is need to rush into them. The main item to consider in the development of current systems and technology is to not build systems that would have to be completely reworked in order to work with potential future solutions. Current system needs to maintain flexibility and adaptability to prevent large scale future projects and system replacements. The County's current approach and ideals follow this goal and concept. A key in maintaining and driving this approach will be the governance strategies and technology leaders within the County to ensure current technology continues to be updated and re-evaluated.

6.7 Summary

Currently, the County has a centralized data repository with its Hach WIMS infrastructure that provides a user-friendly source of system process data for reporting. Key Performance Indicators (KPIs) and benchmarking data continue to be developed with this system and the WIMS system continues to be modernized and enhanced. Add-on packages such as Hach Claros could provide a useful mobile interface to aid in instrument maintenance and potential future analytics. The County has made a goal of empowering staff with data and have taken the correct steps in order to see this goal become a reality. Development of these data driven systems needs to continue and expand following industry best practices and by providing staff high levels of data relations beyond standard visualization of data points in the SCADA system.

Chapter 7

CYBER AND PHYSICAL SECURITY ASSESSMENT

7.1 Introduction

This chapter presents a review of cyber and physical security systems at the Manatee County Water Reclamation Facilities. Cyber and physical security was reviewed using the AWWA Cybersecurity Use Case Tool and the following industry standards:

- NIST Cybersecurity Framework.
- NIST SP 800-53.
- NIST SP 800-82.
- ISA/IEC-62443.
- ISO/IEC-27001.
- DHS Catalog of Control System Security (CAT).
- AWWA/ANSI G-430.
- Guidelines for Physical Security of Wastewater/Stormwater Utilities.

The AWWA Cybersecurity Use Case Tool was utilized because it is recognized by the EPA as the minimum standard of care for cybersecurity in the industry. As a part of this Master Plan, physical security recommendations were developed primarily in regard to protecting control system infrastructure, but many also apply more broadly to the overall WRF security posture.

7.2 Cybersecurity

As the County upgrades and expands the use of automated controls and increases availability of data, expanding and enhancing cybersecurity controls and strategies must also be included. Currently, having limited internal SCADA support resources, the County also has limited internal cybersecurity support for its process control networks. The County is not meeting all standards and requirements for cybersecurity in the industry. There is a cybersecurity plan in place, but only for IT. There is not currently a cybersecurity plan for SCADA. Over the past year, the County's IT department has implemented a cybersecurity training program and has two full-time security employees. Still, more specific training is needed for both SCADA and plant operations staff.

IT has had some responsibility for providing security for the Manatee County SCADA network, but has historically limited support down to the firewall located at each Manatee County wastewater facility. As a part of more recent projects, IT has provided input on network switch selection but has still not taken an active role in the network security of the County's SCADA system. Additionally, a service level agreement (SLA) does not exist between the Utility and IT to cover services for the wastewater SCADA systems or for any type of control system network.

The County's IT department has researched and provided input on firewall options for upgrading communications between facilities. The solution for each site was to implement redundant Fortinet firewalls at each location to secure communications and provide reliability. This also provide IT with a method to manage security up to this point in the SCADA network. Additionally, the IT department also uses Symantec Norton AntiVirus for additional end point protection which can be further leveraged by the SCADA department for use on workstations and servers.

County IT presently uses SolarWinds and NetBrain as network diagnostic tools. These platforms and other existing diagnostic tools are supported, used, and understood, but standard operating procedures and additional data would improve the system. These tools are currently used on the IT network but not the SCADA network. Leveraging these tools on the SCADA network would provide the desired network monitoring and management. Deployment should be done to ensure continued separation of networks utilizing a dedicated network management network.

Since the County has not had dedicated internal support for their SCADA and associated network services, system maintenance items such as software patching and updating have not occurred. Additionally, the implementation of network security solutions and practices has also not occurred leading to vulnerabilities within the Manatee County control system. Staff are aware that vulnerabilities that exist within their system but are unsure of how to best address these issues.

The utility department would like IT to play a greater role in assisting with network management and network security for utility system process control networks. A starting point to ensure an appropriate level of service and support response would be to develop an initial SLA between the departments outlining expectations. A current setback is that the IT department does not currently have the staff necessary to support management and assistance with more systems and components. Similarly to having internal support for the County's SCADA systems, additional internal support for network management of these control systems needs to be added to the County's staffing plans. Having limited labor resources within the County also emphasizes the need for an SLA to ensure necessary levels of support are provided for all departments and resources are not monopolized by a particular department. It is recommended that utility staff and IT begin the process of creating a cyber security master plan to share insight on their systems and to accommodate technology needs to support network management and security but also staffing requirements for system maintenance and support.

In terms of general cybersecurity management and support, the County IT department does have global policies and resources that can be leveraged to support the SCADA network. Generally, the SCADA cybersecurity policies would reference general IT cybersecurity policies such as:

- Authentication.
- Private Information.
- Training.
- Acceptable Use Policy.

These policies and procedures can be referenced and leveraged for initial the SCADA system network security policy development. In addition to cybersecurity network policies and procedures, the County IT department also has the following resources implemented that can be leveraged to varying extents to improve the security posture and network management of the SCADA system:

- Existing Fortinet firewalls at each wastewater facility site.
- Symantec Norton Antivirus.

- Active Directory:
  - Single sign-on password management.
  - User and Group Policies.
- Solarwinds:
  - Automated network device configuration management and backup.
  - Automated logfile storage.
- NetBrain:
- VMware vRealize Operations.

These systems can be leveraged to varying degrees to provide additional support within the SCADA network environment. A key element of leveraging systems between networks is to continue to maintain separation of the operation of the networks. This includes development of a DMZ between the IT and SCADA system networks and implementation of data exchange between networks through systems located in the DMZ. Examples of DMZ located systems would include update services such as windows server update service (WSUS) and anti-virus management, logfile servers, and data replication and backup. In some cases, such as for Active Directory, this does require duplication of certain systems or services as required to maintain proper separation and overall network security in accordance with industry standards. In addition to existing systems that can be leveraged, there are also numerous available open source network security tools that can be effectively utilized. As with any system or product being put on the network, an analysis of the tool to verify its suitability and safety for use on the network should be evaluated before any implementation.

Another key element to appropriately implementing solutions and leveraging existing technology is having a comprehensive Cybersecurity Plan and Program. This plan outlines how cybersecurity will be addressed and outlines how solutions will be implemented to ensure a comprehensive Defense-in-Depth strategy. A Cybersecurity Plan needs to be developed for Manatee County.

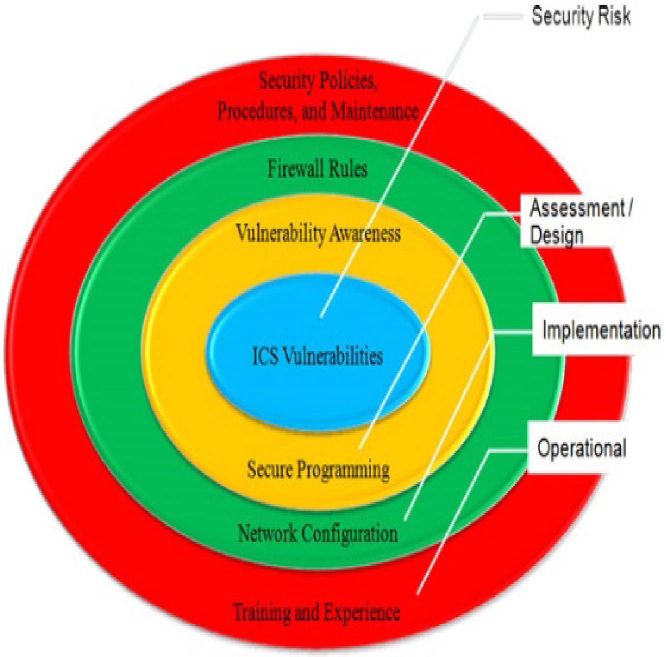


Figure 7.1 Defense-In-Depth Strategy

A key element to any cybersecurity plan is to follow the basic NIST Cybersecurity Framework shown below. This framework outlines the key strategies to protect and defend a network following a defense-in-depth strategy. The NIST framework consists of standards, guidelines, and best practices to manage cybersecurity related risk. This approach was developed specifically to promote protection and resilience for critical infrastructure and should be used as the starting point for a cybersecurity program.

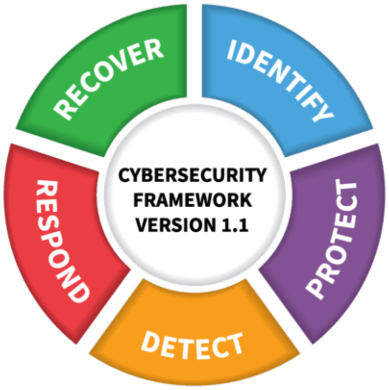


Figure 7.2 NIST Cybersecurity Framework

The Cybersecurity Plan for the Manatee County wastewater SCADA system should include and address the following main topics:

- Risk and Vulnerability assessments in accordance with the AWWA cybersecurity use case tool and ICS-CERT CSET utility, also including penetration testing.
- Mitigation planning.
- Roles and Responsibilities.
- Internal and External Service Level Agreements (SLAs).
- Audit Policies and Requirements.
- Architecture and Security Configuration Policies, Requirements, and guidelines.
- Data Security Policy and Procedures.
- Device Security Policy and Procedures.
- Access Control Policies and Procedures.
- Intrusion Detection Design Considerations.
- Personnel Security.
- Incident Response.
- Design Considerations - Cybersecurity Requirements.
- Training.
- Security Governance.
- Asset management.
- Recovery Plans.

One of the most critical aspects of this planning process is the development of recovery plans and methods of backup and recovery. The current climate of cybersecurity is not if an event will happen but when and preparing for when an event happens. This means being able to detect that an event has occurred, know how to stop the event, and then knowing how to recover. The cybersecurity plan must include information on how systems are being securely backed up and how they would be re-deployed in the case of a cyber event. Currently, the most common threat is ransomware. Ransomware can infect any type of computer system through multiple paths including email, web links, webpages, flash drives, and from other infected machines. Ransomware encrypts the contents of the infected machine holding the data hostage and rendering the machine virtually useless until the ransom is paid and files unencrypted and restored. Being prepared to deal with threats such as ransomware is critical to the reliable operation of the SCADA control system and must be addressed as part of the cybersecurity planning process.

In addition to Cybersecurity Planning, it is recommended that the County work with their local Department of Homeland Security (DHS) representative to find out what assistance the County may be eligible to receive and what programs DHS offers that may be of benefit in developing a more robust cybersecurity program. Some available programs include:

- Assistance and review of ICS-CERT CSET Analysis.
- Cyber Resiliency Review.
- Cyber Hygiene Assessment.
- Architecture Analysis.
- External Dependencies Management.
- Vulnerability Scans using Nessus.

These are potential low-cost methods of managing cybersecurity risks with limited staff and resources. In addition to DHS services available, free training for staff is available through the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT), including instructor led training directly relating to ICS systems, and additional services are available through both Water and Multi-State Information and Sharing Analysis Centers (ISACs). The services from all of these entities can be leveraged to assist in rounding out a complete cybersecurity program.

7.2.1 AWWA Cybersecurity Use Case Tool Review

The AWWA Cybersecurity Use Case Tool was utilized to perform an initial analysis of the SCADA network. This tool is endorsed by the EPA as the minimum standard of care for cybersecurity compliance within the industry and was developed by the AWWA to provide water sector utility owner/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber events as recommended in ANSI/AWWA G430. The tool addresses the following practice categories:

- Governance and Risk Management.
- Business Continuity and Disaster Recovery.
- Server and Workstation Hardening.
- Access Control.
- Application Security.
- Encryption.
- Telecommunications, Network Security, and Architecture.
- Physical Security of PCS Equipment.
- Service Level Agreements (SLAs).
- Operations Security (OPSEC).
- Education.
- Personnel Security.

These categories are described in further detail along with additional recommended practices in the AWWA Cybersecurity Guide found in the Appendix. In order to generate an initial assessment, the applicable Use Cases were selected for Manatee County SCADA system network including the following:

- Architecture:
  - AR1: Dedicated process control network.
  - AR5: Licensed wireless Wide-Area (site-to-site) Network.
  - AR11: Connection to non-SCADA network.
- Program Access:
  - PA1: Outbound messaging.
  - PA5: Data Exchange.
- PLC Programming and Maintenance:
  - PLC1: Local PLC programming and maintenance.
- User Access:
  - UA2: Plant system access with control from fixed locations.
  - UA5: Remote system access with web view from fixed locations.

These selections then generated a list of recommend controls with each control having a listed priority that was determined by the selected use cases according to the following workflow.

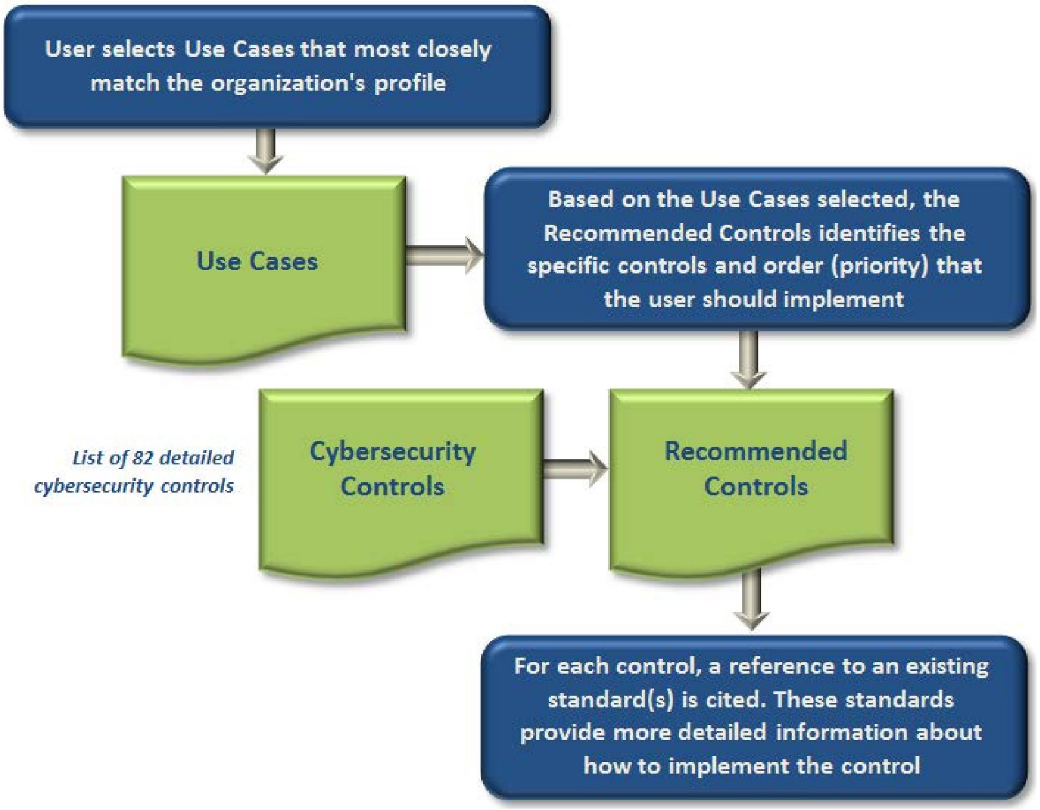

User selects Use Cases that most closely match the organization's profile
Use Cases
Based on the Use Cases selected, the Recommended Controls identifies the specific controls and order (priority) that the user should implement
List of 82 detailed cybersecurity controls
Cybersecurity Controls
Recommended Controls
For each control, a reference to an existing standard(s) is cited. These standards provide more detailed information about how to implement the control

Figure 7.3 AWWA Cybersecurity Use Case Tool Workflow

The complete output of this report can be found in the Appendix. A list of 88 recommended cybersecurity controls were output from the tool. The following is a breakdown of the recommended cybersecurity controls by priority.

Table 7.1 Recommended Cybersecurity Control Priorities Summary

Control Priorities	QTY
1	30
2	29
3	21
4	8
Total Controls	**88**

Priority 1 controls are viewed as the highest priority being basic cybersecurity requirements that must be implemented for minimum security compliance. As priority numbers increase controls either address less broad ranges of cyber threats or provide enhanced application of higher priority controls. The recommended controls from the tool were then organized in a spreadsheet for tracking current level of implementation and project assignment as shown in the table below. The entire spreadsheet can be found in the Appendix.

Table 7.2 Recommended Cybersecurity Controls Tracking

Category	Control	Priority	Referenced Standards	Level of Implementation	Project	Notes
AT-1	A security awareness and response program established to ensure staff is aware of security policies and incident response/notification procedures.	Priority 3 Controls	• DHS CAT: 2.11 Security Awareness and Training • ISA 62443-2-1: A.3.2.4 Staff Training and Security Awareness	Not Implemented	Physical and Cyber Security Plan	
AT-2	Security training including Incident response training for employees, contractors and third-party users based on job roles.	Priority 3 Controls	• AWWA G430-14: 4.3 Defined Security Roles and Employee Expectations • DHS CAT: 2.11.3 Security Training	Not Implemented	Physical and Cyber Security Plan	
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.	Priority 1 Controls	• DHS CAT: 2.7.7 Investigation and Analysis	Not Implemented	Physical and Cyber Security Plan	Further enhanced through addition of logfile server in Core SCADA project.
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	Priority 3 Controls	• SA 62443-3-3: 6 Use Control • NIST 800-82r2:6.2.3 Audit and Accountability	Not Implemented	UTS Governance Project	
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.	Priority 2 Controls	• DHS CAT: 2.1 Security Policy, ISO/IEC 27001: Annex A:A.5 Information security policy	Not Implemented	Physical and Cyber Security Plan	Sub-policy to overall governance requirements
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.	Priority 2 Controls	• ISA 62443-2-1: A.3.2.3 Organizing for security, ISO/IEC 27005: 27005 Whole Document, NIST 800-53: Appendix F-AU: AU-1 Audit and Accountability Policies and Procedures	Not Implemented	UTS Governance Project	
AU-4	Information security responsibilities defined and assigned.	Priority 2 Controls	• ISO/IEC 27001: Annex A: A.6.1.1 Information systems roles and responsibilities NIST 800-53: Appendix F-AU: AU-1 Audit and Accountability Policies and Procedures	Not Implemented	UTS Governance Project	
AU-5	Risk based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of polices 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.	Priority 2 Controls	• DHS CAT: 2.12.2 Continuity of Operations Plan • ISA 62443-2-1: A.3.2.5 Business continuity plan • ISO/IEC 27003: 27003 8.2 Conduct risk assessment	Not Implemented	UTS Governance Project	
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	Priority 2 Controls	• NIST 800-124: 2.2.1-5 Lack of Physical Security Controls	Not Implemented	UTS Governance Project	Should reference a broader City-wide plan

As seen on the spreadsheet, the current level of implementation of each control was documented for the SCADA network. Levels of implementation include Fully Implemented and Maintained, Partially Implemented, Not Implemented, and Not Applicable. Based on an analysis of the implemented controls, the following summary of implementation was developed.

Table 7.3 Current Cybersecurity Controls Implementation Summary

Control Priorities	Fully Implemented	Partially Implemented	Not Implemented	Not Applicable
1	1	8	20	1
2	0	3	26	0
3	0	6	14	1
4	0	3	5	0

As seen in the summary, only one of the controls are fully implemented and maintained. Implementation of more control should be a priority for the County. The next step in addressing the implementation of these recommended cybersecurity controls is to develop a mitigation or emergency response plan to plan for how these controls will be implemented or addressed. To meet this requirement, each recommended control will be associated with a planned SCADA Master Plan project where at least partial implementation of the control would be addressed. In cases where controls will not be implemented as part of a planned project, they will be assigned to a future project. In cases where controls are not planned to be implemented or where implementation is seen as unfeasible then it is noted that the associated risk is accepted, and no project is assigned. The following sections outline some of the specifics related to each particular use case.

7.2.2 Architecture

This use case reviews the system network architecture and segmentation. Manatee County network includes a process control network, licensed and unlicensed radio system, wireless access point, and a connection to a non-SCADA network through connection to the IT network.

The County network topology is currently a non-segmented topology where all devices have direct network access to each other and to any other devices added to the network but do have the ability for segmentation and access control for devices communicating through onsite firewall systems. The County SCADA network topology needs to be revised to meet industry best practices. Current best practices, as outlined in the NIST and IEC standards, recommend a layered topology following the Purdue model as shown in the following figure.

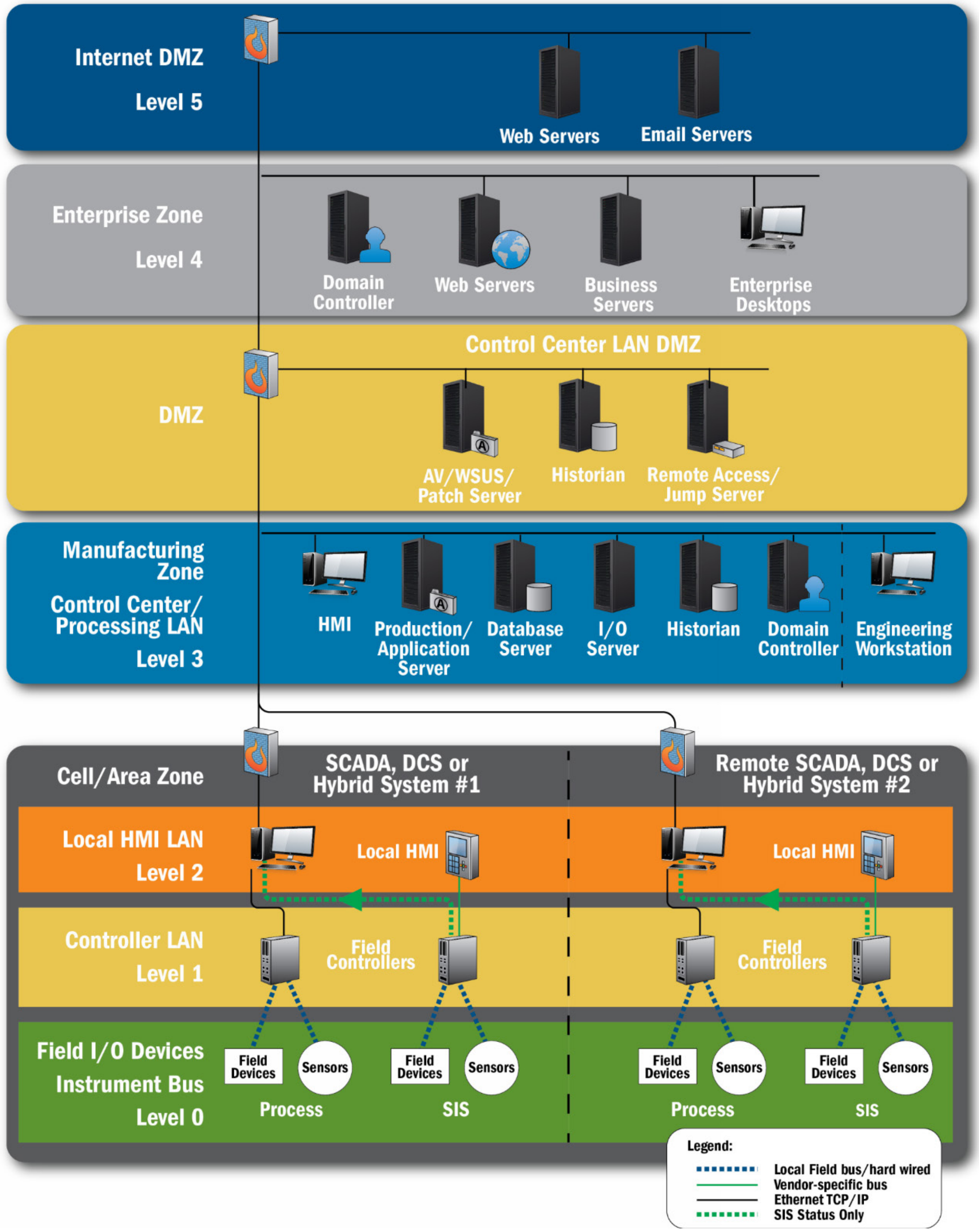


Figure 7.4 Title Recommended Secure Network Architecture

As shown above, based on the function of specific components, they are segmented in different network layers to minimize access from unnecessary systems. This control limits the attack surface of the control system and also aids in better network performance. As the networks at Manatee County are upgraded and evolve, network segmentation should be added to the overall system topology.

7.2.3 Program Access

Program access refers to both manual and automatic data transfer within the SCADA system by any means. Examples of data transfer would be information sent to the Hach WIMS system or the system Historian, data and files uploaded or downloaded via USB drives, and download and loading of patches and updates among other methods of data access. The SCADA system currently has all of these methods of data access.

Data access and data and file transfers are the main function of a SCADA system. These are also sources of vulnerability. Because of this, increase attention must be paid to the way data is accessed and transferred within the SCADA system. A starting point for securing data transfer is to use network segmentation as noted previously. The next control is to have a data management plan as part of system governance. This plan outlines approved methods of data transfer and notes allowed pathways for data to be transferred within the network architecture. The data transfer plan should outline exactly what systems send data to the centralized Hach WIMS system. After data transfer rules such as these are created, the network architecture can then be analyzed to determine what controls need to be put in place to implement this rule.

In addition to these rules, personnel rules and responsibilities need to be established as well such as the use of approved USB drives and who is allowed to use them. Additional controls also include authentication or login policies for data access. The goal of securing data access is not to limit access to data. Data must be used to empower staff and help staff make informed decisions and perform their job functions. Securing data is meant to ensure the data used by staff is available and reliable.

As the Manatee County SCADA system expands and as technology continues to move in the direction of more and more distributed data systems with the continued growth of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) also known as Industry 4.0, securing data becomes increasingly important and more challenging. The implementation of a data management plan and system governance aids in providing the framework necessary for proper control implementation.

7.2.4 PLC Programming and Maintenance

This use case includes how system programming and maintenance are performed, how systems are accessed, and who is performing programming and maintenance services. At Manatee County most new programming of the Manatee County SCADA system is performed by third party integrators. The majority of system maintenance programming for both PLCs and SCADA HMI are provided by the County’s SCADA maintenance staff.

Managing changes to systems manages risks. System modifications, especially in controls systems where programming is involved, can result in unintended system operation and failures if not thoroughly developed and tested and training provided to operational staff. A formal Change Management program helps to minimize these risks. A change management program should include the following steps:

1. Method of requesting and informing staff of upcoming modifications and maintenance.
2. Scheduling and assigning tasks to a qualified technician.
3. Documenting the intended modifications and outcomes.
4. Developing a backup plan or change rollback in case the modification does not go as planned.

5. Modification and maintenance testing and closeout.
6. Staff training as required.
7. Documentation of the completed task along with any updated O&M information.

There are many methods of implementing a change management program and many systems that can be used to make this implementation simpler and more automated. The County currently is in the process of adding a computerized maintenance and management system (CMMS). A CMMS is an industry standard system for integration of all the steps noted above. By adding SCADA assets to this system and adding third party integrators as technicians within this system, the County can begin tracking changes within the SCADA system. This not only provides documentation of system changes but will aid in management of third-party integrators and provide a method of tracking costs and volume of work performed by these integrators.

Additional tools that can be used to support change management are document repository systems. The County already utilizes SharePoint for document management. SharePoint does allow for user-based access and incorporation of group policies for security and to limit access to allowed content and supports a variety of documents. The County could leverage SharePoint in order to manage documents such as Test Forms, Staff Training, Applications, and O&M material related to SCADA system modifications if these do not integrate easily within the CMMS system. Additionally, other specialized systems such as Rockwell Asset Center, MDT Autosave, and Versiondog exist that can automate system backups, log changes, and compare files for more automated change management.

For managing changes to system network configurations, County IT is currently using Solarwinds and NetBrain. This system can also be leveraged to manage network configuration changes on the SCADA network.

In order to minimize risk of implementing changes or updates that create unintended system operation or failures, a test environment can be used. A test environment mimics the production environment but does not actually control any systems or equipment. By using a test environment, modifications and maintenance can be performed and tested to verify if any problems occur, and if they do, solutions can be developed before the production equipment is modified which could lead to downtime or a reduction in system quality or efficiency. A test environment also provides the added benefit of allowing training on a non-production system as well. Again, the advantages of having a test environment is that work can be done without affecting the production system. This type of environment does come with additional costs that vary depending on the quality of the test environment. Simple test environments can provide testing to ensure systems are not corrupted or break during modifications but generally cannot be used to test actual control functions or true operation.

7.2.5 User Access

User access includes both control level and view only access types as well as local and various forms of remote system access. This area focuses mainly on access to the SCADA system HMI but guidelines and techniques should be considered in all forms of remote access for any type of network configuration, monitoring, or maintenance within the SCADA network. Currently the Manatee County SCADA HMI system can be accessed both locally and remotely within the Manatee County network but cannot be accessed remotely over an Internet or non-County network connection. At local workstations, shared account credentials are used to access workstations and servers, and these are generally logged on at all times. Access to the SCADA HMI is secured through an application level username and password._In general, this is also being used as a shared login and systems generally left logged on at all times.

User access also requires a defined governance policy in order to establish user groups and the necessary system access for each user group. In many SCADA systems, the following user groups are utilized:

- View Only:
  - Often used as a default on system auto-logout so processes can be viewed locally by operators but not adjusted.
  - Used for remote connections where control is not allowed offsite.
  - Used for staff who need to view data but not control or data functions.
- Engineer Access:
  - Often used for utility staff who need to access SCADA system data.
  - Can view most pages but not operate equipment or acknowledge alarms.
  - Cannot modify the system.
- Maintenance Access:
  - Often used for maintenance staff who need to view the SCADA system and be able to operate specific equipment in order to test its operation.
  - Can view most pages but not adjust control or alarm setpoints.
  - May be able to acknowledge all or specific alarms.
- Operator Access:
  - Often used for operations staff who need to operate the facility.
  - Can view all pages and manage all alarms.
  - Can adjust most control setpoints but not alarm setpoints.
  - May be able to make system modifications.
- Supervisor Access:
  - Often used for the plant supervisor who needs to manage operation of the facility.
  - Can view all pages and adjust all parameters.
  - Can modify security privileges and system access.
  - May be able to make other system modifications.
- Developer Access:
  - Often used for third party integrators who need to modify the system and make programming changes.
  - Can view all pages and make system changes.
  - If system allows, may be prohibited from making security changes and actual operational changes.
- Administrator Access:
  - Used for the system manager and trusted internal development staff.
  - Full system access and ability to modify the application including security changes.
  - Internal policy needed to address ability to operate.

Depending on the level of granularity desired within the organization, these groups can be expanded or condensed to meet the operational needs of the organization. It is very common to condense the Engineer, Maintenance, and Operator groups into a single group and Supervisor, Developer, and Administrator groups into a single group depending on total number of system users and the level of trust within the organization.

The implementation of these groups and associated user and group policies should be administered through Active Directory. The Active Directory system should be developed to also consider other potential system access outside of SCADA as well. Other system access to consider when developing policies may include server and workstation administrator privileges, access to other systems such as CCTV, and remote access and VPN connectivity. The best practice for deploying Active Directory in the control system environment is that it is not shared with the IT Active Directory structure and should be a stand-alone system dedicated to the control system environment. This does require additional maintenance support.

In addition to user and group policies, secure methods of remote access must also be established if this method of access will be allowed. First, the risks associated with remote access must be weighed with the benefits and a clear understanding developed and agreed upon for why remote access is being provided. These risks should be weighed carefully as remote access greatly increases the attack surface of a control system. If the County is not prepared to implement remote access in accordance with industry best practices, then it is recommended to not implement this technology. After establishing a decision, and if remote access will be allowed, the necessary controls must be put into place to secure this form of communication. There are many available controls for better securing remote access such as the use of two-factor authentication for VPNs, internal system jump servers for control system access, and utilizing thin client solutions such as Rockwell ThinManager, Citrix, or VM Horizon View to minimize access to physical hosts among others. These solutions must be tailored to the organization’s risk and budget constraints.

User access again must be provided so that the user experience is not diminished, and users have access to all the data and systems they need. Security should be implemented so that non-authorized users cannot access systems and users can only access the systems they need. The use of Active Directory and single sign-on greatly simplifies user experience and system management. As with all aspects of cybersecurity, this is not a simple implement and forget technology. These system controls must be constantly maintained and updated requiring system management and maintenance.

7.2.6 Consequence-driven Cyber-Informed Engineering

This use case and associated controls are not yet part of the AWWA Cybersecurity Use Case Tool and Guidance but are a critical aspect of a cyber security program. Consequence driven Cyber- -informed Engineering (CCE) includes the safe and secure design of systems and components before implementation to minimize future work in assessment and mitigation of threats and vulnerabilities. The idea behind this approach is to think like a hacker but act like an engineer. Implementation of CCE is a four-step approach:

1. Consequence Prioritization:
   a. Determine critical functions and high consequence events.
   b. Identify what is not allowed to fail.
   c. Prioritize failures based on consequences.
2. System of Systems Analysis:
   a. Examine how the critical function is achieved.
   b. Identify the key information, access, and actions an attacker must take to produce an effect.

3. Consequence-based Targeting:
   a. Illuminate where the control system is vulnerable by thinking like an attacker.
   b. Consider all avenues; network, supply chain, on premise.
4. Mitigation and Protections:
   a. Engineer-out the cyber risk.
   b. Interrupt the attacker's progress with simple and complex engineering controls.

CCE cannot be integrated into existing systems. As discussed above in the previous use cases, these use cases and controls are intended to strengthen the security posture of an existing system. The concept of CCE is to build in these controls before system deployment to minimize future mitigations and "bolt-on" solutions. Actual implementation of CCE can be done in two major forms:

1. CCE in the product. Using and procuring products with built-in security.
2. CCE in the design. Designing process systems with security controls in place.

CCE is being used by many product manufacturers. Security is being built into products such as using techniques like Transport Layer Security (TLS) for device level authentication, managing supply chains, and mitigating vulnerabilities to exploits among other solutions. To aid in determining if products are developed securely, certification bodies such as ISO and ISASecure, have developed certification standards that products can be listed under. When purchasing products, it is important to understand what the certifications mean, and the importance of the device being certified in the overall process. Currently, few products in the industry have security certified offerings. As CCE and associated certification programs evolve it is recommended to consider security certified control system products.

CCE can be implemented on any new process system design at the CCE. Implementation can range from simple to complex solutions of widely varying cost. Some examples of simple solutions include the following:

- Hardwired interlocks to override PLC control in the case a PLC is compromised.
- Local control capability to take equipment out of automatic/PLC control.
- Backup solutions and redundancy designed into the control system.

Complex solutions could range from implementation of systems to detect abnormal system operation or network traffic to a full system hazard analysis including a risk and vulnerability assessment as a part of the design process. A major factor to keep in mind is that by implementing CCE in the design process, the costs associated with risk and vulnerability assessments are now incorporated in the design which increases the overall design cost. The intent is that solutions are developed during design which later reduces the cost of future mitigations. However, by incorporating these solutions as part of the design and construction, it is likely that the overall upfront construction costs will also be increased. In general, this approach does not equate to a reduction in costs but does provide system security up front strengthening the overall security posture of the system and reducing future expenditures.

7.2.7 Supply Chain Management

Another use case can set of controls not currently incorporated in the AWWA Cybersecurity Use Case Tool is Supply Chain Management. Supply chain management refers to the management of materials, products, and services through every step of their shipment, production, or development. Supply chain management can seem very onerous. Some of the major areas that can be effectively managed are the following:

- External dependencies.
- Use of industry standard products and procurement methods.
- Service Level Agreements.

An analysis of external dependencies should be considered including product and service providers. The different providers should be assessed individually to determine depth and stability of the provider and trust in the provider, and as a whole to determine redundancy of providers such that if one provider fails another can be used in its place. An example is the County's reliance on external SCADA support providers. In the case of the WQCF, three service providers are under contract for support all with in state offices and varying depths of qualified staff. This provides the County with three support options which minimizes the risk of a single point of support failure.

Utilizing industry standard products and procurement methods further reduces the County's supply chain risk by verifying the following conditions are in place:

Ensuring proper protections are in place such as insurance, indemnification, and limitations of liability:

- Supplier financial stability and visibility.
- Third party certifications, listings, and labels.

Utilizing SLAs with providers, especially service providers, helps to guarantee protection and level of service. Critical concerns for the County should be incorporated into SLAs such as data protections and protections on what happens in the case of a company's failure. SLAs should be carefully reviewed and developed with input from the County's risk management department.

The key aspect to supply chain management is to consider the source of supply and the level of trust the County has with the supplier. Products should be purchased from known and reputable manufacturers and vendors and services should be supplied through known and stable service providers. If providers are unknown, then information verifying their stability, company status, and company qualifications should be submitted to the County for review and consideration as an approved vendor. Coordination with the County's procurement department on proper methods of approval and selection under procurement requirements must also be considered.

7.3 Physical Security

Similar to cybersecurity, physical security at Manatee County is necessary to protect this critical infrastructure. Much like the NIST Cybersecurity Framework, the following are the key elements of a physical protection system:

- Deterrence.
- Detection.
- Delay.
- Response.

These elements encompass a complete physical security program. Deterrence can be security measures such as lighting, cameras, and signage. Detection include sensors to alarm on intrusion such as motion detectors, video analytics, and door and window intrusion sensors. Delay refers to physical barriers intended to slow down an intruder such as fences and locks. Response includes actions taken to interrupt a threat actor and to notify authorities. These elements together create a program very similar to the defense-in-depth strategy of cybersecurity.

7.3.1 Manatee County Physical Security

Currently, the County wastewater facilities have limited physical security implementations. The security implementation includes perimeter fencing, cameras, locks, and intrusion detection. There is not a formal security plan or governance procedures for the system.

The County does not have a formal security officer for their facilities. Security requirements fall on the facility Maintenance and Operations Supervisors who are not formally tasked with this responsibility. The job responsibilities of these supervisors should be reviewed to ensure they include specific functions for managing system security such as responsibility for system auditing, maintenance, and enhancements and that this is the correct position to have these responsibilities. Additionally, the responsibility for the deployment of electronic security systems is not formally defined. Most of the responsibility seems to fall on the County IT department for camera systems and card readers with limited input from the utilities department. The application and responsibility of physical security controls should be outlined between departments and SLAs developed where necessary. Requirements for camera systems should also be reviewed to ensure that proper retention of video is being done.

All of the water reclamation facilities are enclosed by a chain link fence approximately 6 feet in height. Each fence has a vehicle entrance gate that is closed nights and weekends but not during the day. Currently, traffic is not verified to ensure that all vehicles that enter the facility leave by the end of the day, but visual inspection can be used to verify. Gates to these facilities should remain closed at all times. If particular areas require access to non-County employees and need to remain open for access, then separate fencing and gates should be utilized. Access to these areas should be authorized only and gates to these locations closed at all hours. All other gates at the facility, such as back entrances, do remain locked at all times.

All facility doors and entrances have locks but are not locked at all times. Additionally, control equipment inside of buildings is not locked which potentially allows access to this and other similar sensitive equipment with no access controls in place. Doors, especially exterior doors to buildings and equipment should remain locked at all times. All control enclosures and equipment panels remote from the water reclamation facilities remain locked at all times. Intrusion switches are located on control panel doors at remote sites. Systems are not in place to actively monitor these devices at all times.

Currently, the water reclamation facilities have security components in place but does not have a comprehensive physical security program in place. A security plan and implementation should be undertaken to assess physical security risks, develop a security system plan and governance, and implement mitigation strategies and projects. The following analysis highlights some of the key areas that should be included in the physical security planning and implementation.

7.3.2 Physical Security Analysis

For physical security, there are four common types of threat actors that are summarized in the table on the following page.

As risks are assessed and solutions developed, all types of threat actors should be considered, and mitigation techniques applied to the broadest range of threat actors possible. Security measures and mitigation solutions of the following categories should be implemented as part of a comprehensive security plan:

- Perimeter security.
- Site security (area between perimeter and facilities).
- Facility Structures and buildings.
- Water Quality Monitoring.
- CCTV monitoring and alarming.
- Power and wiring systems.
- SCADA physical security.

Current systems should be benchmarked against industry standards in each of these areas and appropriate mitigation techniques employed to reduce risk and increase overall system security. As a part of this SCADA System Master Plan, the following outlines recommended SCADA physical security controls for the County's wastewater systems:

- Locked PLC/RTU Enclosures.
- Tamper/Intrusion switch on enclosure.
- All instrumentation and communication wiring in conduit.
- Monitoring of signal integrity of system I/O, i.e., failsafe wiring and monitoring of out of range 4-20mA signals.
- Backup power sources for control panels and communications equipment.
- Physically secured SCADA system servers and communication devices.

Additionally, for networked security components such as IP video cameras and access control systems such as card readers and VoIP callboxes, networks should be kept physically separated from control system networks. This not only eliminates threats from interference from these IP based devices but also eliminates these potential remote access points into the control system network. If information from these networks is necessary at the control system level, it is recommended to provide this information through secured data exchange between the IT and control system networks as discussed in the cybersecurity section of this chapter.

Table 7.4 Design Basis Threat Capability Matrix

Characteristic	Vandal		Criminal		Saboteur		Insider[1]	
Objective	Damage, deface, or destroy targets of opportunity		Theft of valuable assets		Disruption, destruction, or contamination; destroy public confidence in utility/governmental agency		Property damage, theft, disruption, destruction, or contamination	
Motivation	Thrill, dare, grudge		Financial gain, grudge		Political, doctrinal, or religious causes, grudge		Revenge, financial gain, political cause, collusion with outsider	
	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced
Planning/system knowledge	Little or none	Possible	Little, opportunistic	Definite	Definite	Definite	Limited access to equipment, facilities, SCADA, or computer networks	Extensive access to equipment, facilities, SCADA, networks, and security systems; greater system knowledge
Weapons	None	None	Unlikely	Knives, hand guns, or rifles	Knives or hand guns, toxic materials	Automatic and semi-automatic weapons, toxic materials	Unlikely	Knives, handguns, or rifles, toxic materials
Tools and implements of destruction	Readily available hand tools or equipment available at the facility, spray paint	Basic hand tools (e.g., pliers, wire cutters, hammers, crowbars), baseball bats, or firecrackers.	Hand tools or readily available tools or equipment at the facility (as needed)	Sophisticated hand and/or power tools	Basic hand tools (e.g., pliers, wire cutters, hammers, crowbars)	Unlimited variety of hand, power, and thermal tools (including tools such as cutting torches, contaminant agents, IEDs, and IIDs)	Tools or equipment available at the facility.	Tools or equipment available at the facility.
Contaminants	None	Possible	None	None	Probable	Probable	Possible	Possible
Asset damage	Minimal	Possible	Minimal	Possible	Possible	Significant	Significant	Significant
Injuries	None	Possible (unintentional)	Possible	Possible	Possible	Possible	Possible	Possible
Fatalities	None	Possible (unintentional)	Possible	Possible	Possible	Possible	Possible	Possible

Notes:

(1) The insider may possess similar objectives or motivations to the other DBT categories but will have access to facilities without causing suspicion. Insiders include: employees, vendor representatives, delivery persons, consultants, and onsite contractors.

7.4 Summary of Current Performance

- Non-managed Ethernet switches.
- Flat control system network topology.
- No true server infrastructure.
- Limited network path redundancy.
- No formal written cyber or physical security plans or policies.
- Limited cyber security implementation.
- Limited resources for cyber security support.
- Limited physical security implementation.

7.5 Best Practices

- Fully managed network switches throughout the network.
- Plant wide network redundancy utilizing ring or similar topology.
- Formal and comprehensive security programs in place.
- Cybersecurity practices and implementations completed in accordance with the NIST Framework and AWWA Cybersecurity Use Case Tool recommendations.
- Dedicated and responsible security support staff.
- Multi-layered physical security implementation in accordance with industry standards.
- Staff trained in their roles and responsibilities for security at all staff levels.

7.6 Initial Recommendations for Assessment

Based upon the information obtained, the following is a listing of initial system recommendations:

- Develop a Cybersecurity Plan and Policies to base implementation around.
- Developed a layered SCADA network system architecture.
- Add network security components and solutions during SCADA system upgrades.
- Develop a Physical Security Plan and Policies.
- Determine roles and responsibilities of staff to manage, maintain, and upgrade security system components.
- Implement network security starting with the following key elements:
  - Enhance network segmentation by separating control system networks from security, network management, remote user, and visualization networks.
  - Create a SCADA DMZ for locating centralized resources that require access to the IT network or for remote users.
  - Implement a patch management policy using a WSUS server and add AntiVirus to the SCADA network for additional protection.
  - Implement a backup and recovery method along with change management procedures.

7.7 Summary

Overall, the County SCADA system network components do not meet current industry standards for networking features and management. Limited cybersecurity implementations are currently in place, and physical security implementations do not meet industry best practices. The County should upgrade their in plant network infrastructure to increase reliability and security. The County would benefit from formalizing their security plans, policies, and staff roles and responsibilities through the development of Cyber and Physical security governance practices. Additionally, assessment of the scope of security responsibility between the Utilities and other departments such as City IT should be determined and documented for a clear delineation and development of service level agreements for support.

Chapter 8
SCADA PROJECT PLANNING

8.1 Introduction

This section outlines proposed SCADA projects based on the recommendations outlined in technology assessments and reviews. These projects are meant to define a SCADA system CIP for upgrades and new infrastructure in order to adjudicate system gaps, replace outdated components, and follow industry best practices and standards. Recommendations and projects were developed to address the core principles developed with the County that include:

- Standardized solutions and implementations.
- Replacement of outdated equipment.
- Increased system reliability.
- Increased system security.
- Access to data.

These were the drivers for the recommendations made in Chapters 2 through 7 along with the data gathered from the workshops and surveys conducted at the various stages of the master planning process. The following projects were developed to address these recommendations through coordinated projects in order to logically perform similar work under a single project design and construction. Projects may be further combined or phased at the County's desire to execute work under budget and schedule constraints. These projects are intended to outline project scopes and major outcomes and are not detailed designs. Detailed designs will be required for many of the projects listed.

Additionally, one of the key projects of the master plan is SCADA system governance. This project is not meant to hold up the progress of other projects, but key elements of this project should be put in place in order to drive SCADA projects and ensure maintenance practices and documentation are in place. The biggest aspect of this project to start is to identify a responsible staff member to be accountable for delivery of the SCADA projects and manage their delivery by tracking progress against the plan. Another critical aspect is the development of a SCADA governance committee. This committee should assist the person responsible for delivering the SCADA projects and also provide oversight and input on the progress of the plan as well as continue to plan beyond the current projects listed here. This will ensure projects are properly coordinated with other County projects, changing priorities, newly developed needs, and that staff within utilities and in supporting departments are aware of project impacts.

8.2 Core SCADA System Project

8.2.1 Scope and Description

The core SCADA system project will provide the foundation for the County's water, wastewater, and remote site SCADA system. This project will include the implementation of server applications at the existing centralized core server system at the IT (EMC) datacenter that will provide the following server functions:

a. Implement centralized AVEVA CitectSCADA (Plant SCADA) server at IT Datacenter with following functions:
   i. Hosts global application to allow access to all sites.
   ii. Provides backup server services to all facilities.
   iii. Single point for graphical changes to specific sites and global objects.
   iv. Master Alarm server for remote notification of alarms.
b. CitectSCADA Web Server for remote client deployment.
c. Rockwell ThinManager for thin client management.
d. Master Wonderware Historian.
e. Centralized Hach WIMS implementation.
f. Centralized remote alarm notification.
g. Application Change Management Administration (Rockwell Asset Center).
h. Applications Programming through Studio 5000.
i. Test Environment.
j. (Optional) Integration with DFS system.
k. Implementation of server management functions:
   i. Active Directory.
   ii. DNS, DHCP.
   iii. WSUS and Patch Management.
   iv. Network Time.
   v. Server and Virtualization Management.
   vi. Localized system storage.
l. Implementation of Network Security:
   i. Anti-Virus Management.
   ii. System logfile storage and management.
   iii. VPN tunnels to each site.
   iv. Update routing and ACL rules.
m. Network Time Server.
n. Implement SCADA system governance (Could be separate project):
   i. Policies and procedures.
   ii. Security Plans.

In addition, the core server system project will include network components to upgrade security, segmentation, and reliability of the network. Network design upgrades will also be completed for increased segmentation using separate subnets and VLANs along with routing and access control requirements between separate VLANs within the control system to further secure communications. The addition of a SCADA DMZ will provide a secured location for access to system data the ability to remotely access systems for support and remote monitoring. These additions will include a stacked set of layer 3 switches for routing between the separate VLANs within the control system, updates or upgrades to the existing firewall system for securing and routing between the control system network and other associated networks, and upgraded enterprise level switches and servers for the SCADA system located at the IT data center.

The County wide CitectSCADA (Plant SCADA) application will also be modified as a part of this project. The IT data center, the North WRF, South East WRF, South West WRF, Biosolids Facility, and the Mars Booster Station SCADA application will be redeveloped in the latest version of AVEVA Plant SCADA. The CitectSCADA application development will be organized to allow for all facilities to be managed in a single application and to allow for additional future systems to be added into the application as well to reduce application management requirements. The upgrade process will follow the following general migration and include the following main features:

- Operation of Existing CitectSCADA system will remain as-is during the extent of the migration until the new SCADA application, or major subcomponent, is fully completed and tested. Existing applications will be redeveloped in the new system to take advantage of the Context Aware graphics and other embedded features in the new software such as enhanced alarm functionality. Each facility application will be developed as a separate cluster within the overall application.
- New CitectSCADA application is setup at the IT datacenter and includes local servers and the main system Historian.
- Remote alarm capabilities are added to the central server system using WIN-911 for remote alarm annunciation through text messaging or email so that operations staff can obtain alarms while performing plant walk-throughs.
- The SCADA DMZ will be created and SCADA server services such as WSUS and Active Directory are configured.
- Central Wonderware Historian is connected to the Hach WIMs server and further build-out of the Hach WIMS system to ensure that all necessary data is integrated into this server system. Development of any additional KPIs desired by the County.
- Remote access is implemented using a VPN having two factor authentications. An engineering workstation is developed in DMZ and advertised using the thin client infrastructure for remote access.
- Thin client infrastructure is developed using Rockwell ThinManager to support application viewing locally and remotely.
- Standard tags and graphical templates are developed for standard objects.
- Network security appliances are deployed or reconfigured at remote facilities to secure links to these sites and separate IT infrastructure from SCADA infrastructure and to allow the appropriate services from the central SCADA system to communicate to the appropriate devices at each facility.
- Network management software deployed for network monitoring of performance, health, and security of the SCADA network.
- SCADA clients are made available through the Citect web server through the thin client manager to allow for mobile client interface.
- Graphics at each facility are updated to match new graphics developed for the central server system and the new central application is deployed system wide.
- As part of other projects as PLCs are upgraded, tags and drivers are readdressed as required but graphics will then remain the same for operations.
- System is tested and SCADA, IT, and operations and maintenance staff are trained on the new system.

8.2.2 Design

Design will include the following main aspects:

- Server system application architecture and design.
- Communication network and network security design.
- Application programming requirements and design specifications:
  - Development of draft graphical standards through staff workshops.
  - Development of a listing of KPIs to add to the system.
- Incorporation of existing applications into the County wide CitectSCADA System.
- Construction sequencing and testing requirements.
- Design specifications for the following:
  - General I&C Requirements.
  - Construction Sequencing.
  - Control Strategies.
  - SCADA Programming Requirements.
  - Standard software Requirements and Configuration.
  - Applications software Requirements.
  - Network Rack and Cabling Components.
  - Ethernet Network Components.
  - Network Security Requirements.
  - System Testing and Commissioning.
- Design Drawings:
  - Legends.
  - Communications block diagrams.
  - Server and application architecture diagrams.
  - Rack Layouts.
  - Photo Drawings showing upgrade requirements.
- Bid Assistance.
- Construction/Commissioning Assistance.

8.2.3 Construction

Construction requirements will include the following:

- Submittals and shop drawings:
  - Software development and configuration workshops.
  - Graphical display workshops.
  - Network configuration workshops.
- Server and network configuration.
- Integration and configuration of software packages.
- Integration of new CitectSCADA server and application and verification of operation.
- SCADA HMI application coordination and implementation.
- Individual testing of each software package and configuration.
- Performance testing period.
- Penetration testing for baseline security analysis and to verify implementation of specified controls and configurations. Listing of recommendations for further system hardening.
- Provide final O&M documentation and training.

8.2.4 Estimated Costs

The estimated costs associated with the new core SCADA server and network system are summarized in the following table:

Table 8.1 Core SCADA System Project Cost Estimate

Activities	Cost
Design	
Specifications	10,000
Drawings	155,000
Meetings	10,000
Project Management	25,000
Commissioning	75,000
Design Total	**275,000**
Construction	
Server Rack and Components	25,000
Servers	40,000
Network Storage	20,000
Network Components	50,000
Rockwell Asset Center	50,000
Alarm Software and Implementation	10,000
Software OS and General	50,000
Software Implementation	25,000
Hach WIMS Modifications	15,000
Thin Client System	50,000
Test System (Sandbox)	25,000
Drawings	20,000
Testing	50,000
HMI Application Dev	300,000
Submittals	15,000
O&M	15,000
Training	10,000
Electrical	100,000
Construction Total	**870,000**
Subtotal	1,145,000
Contingency 25%	286,250
Total	**1,431,250**

8.2.5 Purpose

The purpose of the Core SCADA Project is to develop the centralized CitectSCADA application and develop a server infrastructure with management, thin client, and security services encompassing the entire WRF SCADA system. This project includes complete build-out of the SCADA infrastructure at the County IT datacenter to complete CitectSCADA system integrated architecture, add server services, implement additional network security, and enhance system governance. This project is meant to address the following major items discussed during staff workshops and recommendations of the SCADA Master Plan:

- System Standardization.
- Enhance system governance through change management, centralized group policies and authentication, and ease maintenance.
- Migration to the latest version of CitectSCADA (Plant SCADA) for all applications within a single County wide application architecture using clustering for reliability and application organization.
- Implement more thin clients and develop a mobile client solution.
- Migrate Historian to the central datacenter and integrate with Hach WIMs for reporting and generating key performance indicators.
- Implement Active Directory security along with other server services such as pathing and anti-virus for security.
- Develop a core SCADA server and network architecture to develop a segmented infrastructure and implement security.
- Virtualize server systems and implement a virtual machine backup and recovery system.
- Add network management including configuration backup and recovery systems.

8.3 SE WRF Upgrades

8.3.1 Scope and Description

This project includes the replacement of existing Legacy PLC systems and associated network hardware, OITs, and the addition of fiber optic cabling for modernization and standardization of equipment and added system resiliency at the SE WRF and includes upgrades for the MARS and Dryer systems as well. A new CitectSCADA HMI application will be developed for the SE WRF facility and added to the central CitectSCADA HMI system. The facility level HMI system will be based on a local redundant set of CitectSCADA HMI servers with local WIN-911 alarm system and local Historian capabilities to buffer data to the master historian. The local CitectSCADA system will be part of SE WRF cluster connected back to the central HMI server. There is an option to not use local redundancy but to use the central HMI server as a remote backup as well as being the location for a central WIN-911 system. Due to past communication issues, it is still recommended to keep local redundancy, but this can be re-evaluated at the time of system design. The MARS and Dryer application has been recently updated and is currently its own application and cluster within the CitectSCADA system. This application should be upgraded to the latest version of CitectSCADA and associated PLCs upgraded as required for consistency. Some of the MARS system is communicated through the N WRF and coordination will be required with projects there. Thin clients will be managed using ThinManager and a local domain controller will be added. Additionally, the facility control room will be upgraded to provide modern monitors having resolution to match the application. Network and computer equipment will be removed from the existing control console and moved to a locked room within the building having air conditioning and sufficient space to house servers and network components. Thin clients will be provided in the control room at operator work areas and wall mounted large screen modular video wall solution will be utilized to allow operations staff to select content for display such as SCADA screens, security cameras, or news and weather information necessary for plant operation during normal and emergency conditions.

Existing PLCs to be replaced include legacy Rockwell Automation Allen-Bradley SLC PLCs. New PLCs will be based on the County's standard Rockwell Automation Allen-Bradley CompactLogix L33 Series. PLCs can be replaced using either of the two options presented in the report based on constraints and preferences during the design. The first option is to maintain exists SLC I/O and migrate the I/O to new CompactLogix controllers using the 1747-AENTR adaptor module. This option would minimize any re-wiring and re-termination of I/O and provide a fast and lower cost replacement. I/O could then be transferred at a later date depending on need and continued availability of SLC I/O cards. The second option would be to completely replace SLC controllers and I/O. This would upgrade the entire system including I/O to more modern components but would increase time and cost of the transition. Specialized wiring arms could be utilized in this option that mate directly to the existing SLC terminals in order to speed wiring. Unless significant I/O changes are planned, or replacement of entire PLC cabinets is desired, it is recommended to transition using the first option in order to reduce the time and cost of the transition. This upgrade will provide a consistent level of programming environment, equipment support, and a higher level of standardization on control hardware.

As part of the upgrades to this facility, integration of the existing DFS HyperSCADA server into the CitectSCADA application for higher visualization into the lift station system should be considered. While the lift station system was not specifically evaluated as a part of this master plan, integration of lift stations into the CitectSCADA application would provide additional standardization, maintenance, and operator access benefits. This migration could also provide a means of lift station controller migration and allow for other controller platforms to be used.

Additionally, network components will be replaced at the time of PLC component replacements to upgrade network hardware to the Rockwell Automation Stratix series managed switches. The Stratix switches should be monitored by the new PLC system using the pre-built Rockwell add-on instruction for Stratix switches in the Studio 5000 PLC programming system. Additionally, all Rockwell network switches, PLCs, and motor control components should be connected to the central Rockwell Asset Center server for management and security. This upgrade will provide higher reliability, security, and manageability and standardize network components to aid in maintenance. Fiber optic cabling will be extended to provide redundant pathways around the SE WRF for higher communications reliability and be coordinated with network component upgrades to minimize downtime. Additional details related to this project can be found in Chapters 3 and 5 of the report and a summary table of PLC modifications in the appendix.

No modifications are planned to wireless systems at this facility as a part of this project. Existing wireless systems should be evaluated to ensure that security features such as encryption are turned on for all radio systems and that these systems are routed through firewalls where strong security features cannot be enabled and known vulnerabilities exist. No WiFi networks are planned to be added to facilities. WiFi is an expensive and insecure addition to plant sites for operator mobile access. Instead of the use of WiFi, it is recommended to use cellular if operator mobile access is desired. Mobile cellular access can be deployed in either a private M2M network or using public interfacing cellular with VPN access used similar to remote system access. For buildings have weak cellular service, cellular repeaters should be used in order to boost signal strength. This will provide boosted service for remote access as well as the benefit of staff cellular phones working within these buildings as well for calls. It is recommended for the County to deploy this system in coordination with their IT department.

8.3.2 Design

The design phase of this project should finalize the CitectSCADA architecture for the facility as well as WIN-911 architecture and thin client deployments based on County preferences at the time of design and known reliability of the communication between SE WRF and the IT datacenter. New SCADA graphics and PLC logic should be specified to be developed through a series of workshops to take place during construction and facilitated by the design engineer to ensure consistency of graphics and programming logic. New graphics should be context aware type graphics with standard objects and templates designed to match up with standard PLC add-on instructions. Design will include the following major aspects:

- Selection of hardware and networking components.
- Design specifications for the following:
  - General I&C Requirements.
  - Construction Sequencing.
  - Control Panel Requirements.
  - PLC Programming Requirements.
  - PLC Components.
  - Ethernet Network Components.
  - Fiber Optic Cabling and Testing.
  - System Testing and Commissioning.
  - Conduit Systems.
- Design Drawings:
  - Legends.
  - Communications block diagrams.
  - Fiber Optic Cable routing diagrams.
  - Photo Drawings showing upgrade requirements.
  - Example wiring details.
  - PLC I/O Layout or I/O List.
  - Electrical duct bank and fiber routing drawings.
  - Building power and fiber drawings to support upgrades.
- Bid Assistance.
- Construction services and commissioning assistance.

8.3.3 Construction

Construction requirements will include the following:

- Submittals and shop drawings for each control panel for O&M documentation.
- PLC replacements with new programming.
- PLC program conversion, corrections, and documentation.
- SCADA HMI applications programming.
- Integration with core SCADA system.
- Network switch configuration.
- Fiber Optic Cable installation and testing.
- Performance testing.
- Decommission existing systems.

- System commissioning.
- Penetration testing and baseline cybersecurity report.
- Provide final O&M documentation and training.

To facilitate a smoother integration, the entire PLC and HMI system should be developed and tested at the integrator's facility. This includes all HMI programming and PLC logic. The full updated HMI program should be deployed and either have existing I/O temporarily addressed to the new system and then transitioned or run the existing and new HMI systems in parallel until all PLCs are replaced. Hardware should be replaced sequentially following expansion of the fiber optic cable system to ensure that work at one PLC location will not negatively impact other areas of the plant.

8.3.4 Estimated Costs

The estimated costs associated with upgrading the PLC system are summarized in the following table. Costs are associated with the proposed Route 2 fiber optic cabling upgrades presented in Chapter 5 and based on full PLC replacements including replacement of all I/O.

Table 8.2 SE WRF SCADA System Project Cost Estimate

Activities	Cost
Design	
Specifications	25,000
Drawings	200,000
Meetings	15,000
Project Management	25,000
Construction Services	90,000
Design Total	**355,000**
Construction	
PLC Upgrades	770,000
Drawings	50,000
Testing	50,000
HMI Application Updates	250,000
Server Hardware and software	80,000
Control Room Upgrades	100,000
Fiber Optic Cable	160,000
Pull Boxes	75,000
Ethernet Switches	20,000
Fiber Patch Panels	10,000
Submittals	25,000
O&M	25,000
Construction Total	**1,615,000**
Subtotal	1,970,000

Activities	Cost
25% Contingency	447,500
Total	**2,462,500**

8.3.5 Purpose

This project is meant to address the following major recommendations of the SCADA Master Plan:

- Upgrade outdated equipment and standardize PLC systems at the SE WRF.
- Add resiliency to the Fiber Optic Network.
- Add network management, standardization, and reliability to the Ethernet network.
- Standardize PLC programming platform and applications.
- Provide operations staff easier access to the information necessary to operator the facility.

8.4 SW WRF Upgrades

8.4.1 Scope and Description

This project includes the replacement of existing Legacy PLC systems and associated network hardware, OITs, and the addition of fiber optic cabling for modernization and standardization of equipment and added system resiliency at the SW WRF. A new CitectSCADA HMI application will be developed for the SW WRF facility and added to the central CitectSCADA HMI system. The facility level HMI system will be based on a local redundant set of CitectSCADA HMI servers with local WIN-911 alarm system and local Historian capabilities to buffer data to the master historian. The local CitectSCADA system will be part of SW WRF cluster connected back to the central HMI server. There is an option to not use local redundancy but to use the central HMI server as a remote backup as well as being the location for a central WIN-911 system. Due to past communication issues, it is still recommended to keep local redundancy, but this can be re-evaluated at the time of system design. Thin clients will be managed using ThinManager and a local domain controller will be added. Additionally, the facility control room will be upgraded to provide modern monitors having resolution to match the application. Network and computer equipment will be removed from the existing control console and moved to a locked room within the building having air conditioning and sufficient space to house servers and network components. Thin clients will be provided in the control room at operator work areas and wall mounted large screen modular video wall solution will be utilized to allow operations staff to select content for display such as SCADA screens, security cameras, or news and weather information necessary for plant operation during normal and emergency conditions.

Existing PLCs to be replaced include legacy Rockwell Automation Allen-Bradley SLC PLCs. New PLCs will be based on the County's standard Rockwell Automation Allen-Bradley CompactLogix L33 Series. PLCs can be replaced using either of the two options presented in the report based on constraints and preferences during the design. The first option is to maintain exists SLC I/O and migrate the I/O to new CompactLogix controllers using the 1747-AENTR adaptor module. This option would minimize any re-wiring and re-termination of I/O and provide a fast and lower cost replacement. I/O could then be transferred at a later date depending on need and continued availability of SLC I/O cards. The second option would be to completely replace SLC controllers and I/O. This would upgrade the entire system including I/O to more modern components but would increase time and cost of the transition. Specialized wiring arms could be utilized in this option that mate directly to the existing SLC terminals in order to speed wiring. Unless significant I/O changes are planned, or replacement of entire PLC cabinets is desired, it is recommended to transition using the first option in order to reduce the time and cost of the transition. This upgrade will provide a consistent level of programming environment, equipment support, and a higher level of standardization on control hardware.

As part of the upgrades to this facility, integration of the existing DFS HyperSCADA server into the CitectSCADA application for higher visualization into the lift station system should be considered. While the lift station system was not specifically evaluated as a part of this master plan, integration of lift stations into the CitectSCADA application would provide additional standardization, maintenance, and operator access benefits. This migration could also provide a means of lift station controller migration and allow for other controller platforms to be used.

Additionally, network components will be replaced at the time of PLC component replacements to upgrade network hardware to the Rockwell Automation Stratix series managed switches. The Stratix switches should be monitored by the new PLC system using the pre-built Rockwell add-on instruction for Stratix switches in the Studio 5000 PLC programming system. Additionally, all Rockwell network switches, PLCs, and motor control components should be connected to the central Rockwell Asset Center server for management and security. This upgrade will provide higher reliability, security, and manageability and standardize network components to aid in maintenance. Fiber optic cabling will be extended to provide redundant pathways around the SW WRF for higher communications reliability and be coordinated with network component upgrades to minimize downtime. Additional details related to this project can be found in Chapters 3 and 5 of the report and a summary table of PLC modifications in the appendix.

Additional security is planned to be added to the existing Engenius wireless links at the facility to further secure these links. Other existing wireless systems should be evaluated to ensure that security features such as encryption are turned on for all radio systems and that these systems are routed through firewalls where strong security features cannot be enabled and known vulnerabilities exist. No WiFi networks are planned to be added to facilities. WiFi is an expensive and insecure addition to plant sites for operator mobile access. Instead of the use of WiFi, it is recommended to use cellular if operator mobile access is desired. Mobile cellular access can be deployed in either a private M2M network or using public interfacing cellular with VPN access used similar to remote system access. For buildings have weak cellular service, cellular repeaters should be used in order to boost signal strength. This will provide boosted service for remote access as well as the benefit of staff cellular phones working within these buildings as well for calls. It is recommended for the County to deploy this system in coordination with their IT department.

8.4.2 Design

The design phase of this project should finalize the CitectSCADA architecture for the facility as well as WIN-911 architecture and thin client deployments based on County preferences at the time of design and known reliability of the communication between SW WRF and the IT datacenter. New SCADA graphics and PLC logic should be specified to be developed through a series of workshops to take place during construction and facilitated by the design engineer to ensure consistency of graphics and programming logic. New graphics should be context aware type graphics with standard objects and templates designed to match up with standard PLC add-on instructions. Design will include the following major aspects:

- Selection of hardware and networking components.

- Design specifications for the following:
  - General I&C Requirements.
  - Construction Sequencing.
  - Control Panel Requirements.
  - PLC Programming Requirements.
  - PLC Components.
  - Ethernet Network Components.
  - Fiber Optic Cabling and Testing.
  - System Testing and Commissioning.
  - Conduit Systems.
- Design Drawings:
  - Legends.
  - Communications block diagrams.
  - Fiber Optic Cable routing diagrams.
  - Photo Drawings showing upgrade requirements.
  - Example wiring details.
  - PLC I/O Layout or I/O List.
  - Electrical duct bank and fiber routing drawings.
  - Building power and fiber drawings to support upgrades.
- Bid Assistance.
- Construction services and commissioning assistance.

8.4.3 Construction

Construction requirements will include the following:

- Submittals and shop drawings for each control panel for O&M documentation.
- PLC replacements with new programming.
- PLC program conversion, corrections, and documentation.
- SCADA HMI applications programming.
- Integration with core SCADA system.
- Network switch configuration.
- Fiber Optic Cable installation and testing.
- Performance testing.
- Decommission existing systems.
- System commissioning.
- Penetration testing and baseline cybersecurity report.
- Provide final O&M documentation and training.

To facilitate a smoother integration, the entire PLC and HMI system should be developed and tested at the integrator's facility. This includes all HMI programming and PLC logic. The full updated HMI program should be deployed and either have existing I/O temporarily addressed to the new system and then transitioned or run the existing and new HMI systems in parallel until all PLCs are replaced. Hardware should be replaced sequentially following expansion of the fiber optic cable system to ensure that work at one PLC location will not negatively impact other areas of the plant.

8.4.4 Estimated Costs

The estimated costs associated with upgrading the PLC system are summarized in the following table. Costs are associated with the proposed fiber optic cabling upgrades presented in Chapter 5 and based on full PLC replacements including replacement of all I/O.

Table 8.3 SW WRF SCADA System Project Cost Estimate

Activities	Cost
Design	
Specifications	25,000
Drawings	220,000
Meetings	15,000
Project Management	25,000
Construction Services	90,000
Design Total	**375,000**
Construction	
PLC Upgrades	800,000
Drawings	50,000
Testing	50,000
HMI Application Updates	250,000
Server Hardware and software	80,000
Control Room Upgrades	100,000
Fiber Optic Cable	110,000
Pull Boxes	100,000
Ethernet Switches	40,000
Fiber Patch Panels	20,000
Submittals	25,000
O&M	25,000
Construction Total	**1,650,000**
Subtotal	2,025,000
25% Contingency	506,250
Total	**2,531,250**

8.4.5 Purpose

This project is meant to address the following major recommendations of the SCADA Master Plan:

- Upgrade outdated equipment and standardize PLC systems at the SW WRF.
- Add resiliency to the Fiber Optic Network.
- Add network management, standardization, and reliability to the Ethernet network.
- Standardize PLC programming platform and applications.
- Correct existing logic errors and increase automation.

- Provide operations staff with greater visibility into plant systems.

8.5 N WRF Upgrades

8.5.1 Scope and Description

This project includes the replacement of existing Legacy PLC systems and associated network hardware, OITs, and the addition of fiber optic cabling for modernization and standardization of equipment and added system resiliency at the N WRF. A new CitectSCADA HMI application will be developed for the N WRF facility and added to the central CitectSCADA HMI system. The facility level HMI system will be based on a local redundant set of CitectSCADA HMI servers with local WIN-911 alarm system and local Historian capabilities to buffer data to the master historian. The local CitectSCADA system will be part of N WRF cluster connected back to the central HMI server. There is an option to not use local redundancy but to use the central HMI server as a remote backup as well as being the location for a central WIN-911 system. Due to past communication issues, it is still recommended to keep local redundancy, but this can be re-evaluated at the time of system design. Thin clients will be managed using ThinManager and a local domain controller will be added. Additionally, the facility control room will be upgraded to provide modern monitors having resolution to match the application. Network and computer equipment will be removed from the existing control console and moved to a locked room within the building having air conditioning and sufficient space to house servers and network components. Thin clients will be provided in the control room at operator work areas and wall mounted large screen modular video wall solution will be utilized to allow operations staff to select content for display such as SCADA screens, security cameras, or news and weather information necessary for plant operation during normal and emergency conditions.

Existing PLCs to be replaced include legacy Rockwell Automation Allen-Bradley SLC PLCs. New PLCs will be based on the County’s standard Rockwell Automation Allen-Bradley CompactLogix L33 Series. PLCs can be replaced using either of the two options presented in the report based on constraints and preferences during the design. The first option is to maintain exists SLC I/O and migrate the I/O to new CompactLogix controllers using the 1747-AENTR adaptor module. This option would minimize any re-wiring and re-termination of I/O and provide a fast and lower cost replacement. I/O could then be transferred at a later date depending on need and continued availability of SLC I/O cards. The second option would be to completely replace SLC controllers and I/O. This would upgrade the entire system including I/O to more modern components but would increase time and cost of the transition. Specialized wiring arms could be utilized in this option that mate directly to the existing SLC terminals in order to speed wiring. Unless significant I/O changes are planned, or replacement of entire PLC cabinets is desired, it is recommended to transition using the first option in order to reduce the time and cost of the transition. This upgrade will provide a consistent level of programming environment, equipment support, and a higher level of standardization on control hardware.

As part of the upgrades to this facility, integration of the existing DFS HyperSCADA server into the CitectSCADA application for higher visualization into the lift station system should be considered. While the lift station system was not specifically evaluated as a part of this master plan, integration of lift stations into the CitectSCADA application would provide additional standardization, maintenance, and operator access benefits. This migration could also provide a means of lift station controller migration and allow for other controller platforms to be used.

Additionally, network components will be replaced at the time of PLC component replacements to upgrade network hardware to the Rockwell Automation Stratix series managed switches. The

Stratix switches should be monitored by the new PLC system using the pre-built Rockwell add-on instruction for Stratix switches in the Studio 5000 PLC programming system. Additionally, all Rockwell network switches, PLCs, and motor control components should be connected to the central Rockwell Asset Center server for management and security. This upgrade will provide higher reliability, security, and manageability and standardize network components to aid in maintenance. Fiber optic cabling will be extended to provide redundant pathways around the N WRF for higher communications reliability and be coordinated with network component upgrades to minimize downtime. Additional details related to this project can be found in Chapters 3 and 5 of the report and a summary table of PLC modifications in the appendix.

Existing wireless systems should be evaluated to ensure that security features such as encryption are turned on for all radio systems and that these systems are routed through firewalls where strong security features cannot be enabled and known vulnerabilities exist. No WiFi networks are planned to be added to facilities. WiFi is an expensive and insecure addition to plant sites for operator mobile access. Instead of the use of WiFi, it is recommended to use cellular if operator mobile access is desired. Mobile cellular access can be deployed in either a private M2M network or using public interfacing cellular with VPN access used similar to remote system access. For buildings have weak cellular service, cellular repeaters should be used in order to boost signal strength. This will provide boosted service for remote access as well as the benefit of staff cellular phones working within these buildings as well for calls. It is recommended for the County to deploy this system in coordination with their IT department.

Upgrades at the N WRF should be coordinated with the SE WRF to ensure operation of the MARS system is not impacted by the upgrade process. Some upgrades may need to be incorporated into the SE WRF project to ensure a well-integrated MARS upgrade.

8.5.2 Design

The design phase of this project should finalize the CitectSCADA architecture for the facility as well as WIN-911 architecture and thin client deployments based on County preferences at the time of design and known reliability of the communication between N WRF and the IT datacenter. New SCADA graphics and PLC logic should be specified to be developed through a series of workshops to take place during construction and facilitated by the design engineer to ensure consistency of graphics and programming logic. New graphics should be context aware type graphics with standard objects and templates designed to match up with standard PLC add-on instructions. Design will include the following major aspects:

- Selection of hardware and networking components
- Design specifications for the following:
  - General I&C Requirements.
  - Construction Sequencing.
  - Control Panel Requirements.
  - PLC Programming Requirements.
  - PLC Components.
  - Ethernet Network Components.
  - Fiber Optic Cabling and Testing.
  - System Testing and Commissioning.
  - Conduit Systems.
- Design Drawings:
  - Legends.

  - Communications block diagrams.
  - Fiber Optic Cable routing diagrams.
  - Photo Drawings showing upgrade requirements.
  - Example wiring details.
  - PLC I/O Layout or I/O List.
  - Electrical duct bank and fiber routing drawings.
  - Building power and fiber drawings to support upgrades.
- Bid Assistance.
- Construction services and commissioning assistance.

8.5.3 Construction

Construction requirements will include the following:

- Submittals and shop drawings for each control panel for O&M documentation.
- PLC replacements with new programming.
- PLC program conversion, corrections, and documentation.
- SCADA HMI applications programming.
- Integration with core SCADA system.
- Network switch configuration.
- Fiber Optic Cable installation and testing.
- Performance testing.
- Decommission existing systems.
- System commissioning.
- Penetration testing and baseline cybersecurity report.
- Provide final O&M documentation and training.

To facilitate a smoother integration, the entire PLC and HMI system should be developed and tested at the integrator's facility. This includes all HMI programming and PLC logic. The full updated HMI program should be deployed and either have existing I/O temporarily addressed to the new system and then transitioned or run the existing and new HMI systems in parallel until all PLCs are replaced. Hardware should be replaced sequentially following expansion of the fiber optic cable system to ensure that work at one PLC location will not negatively impact other areas of the plant.

8.5.4 Estimated Costs

The estimated costs associated with upgrading the PLC system are summarized in the following table. Costs are associated with the proposed fiber optic cabling upgrades presented in Chapter 5 and based on full PLC replacements including replacement of all I/O.

Table 8.4 N WRF SCADA System Project Cost Estimate

Activities	Cost
Design	
Specifications	20,000
Drawings	185,000
Meetings	15,000
Project Management	25,000
Construction Services	80,000

Activities	Cost
Design Total	**325,000**
Construction	
PLC Upgrades	350,000
Drawings	50,000
Testing	50,000
HMI Application Updates	200,000
Server Hardware and software	80,000
Control Room Upgrades	100,000
Fiber Optic Cable	110,000
Pull Boxes	70,000
Ethernet Switches	25,000
Fiber Patch Panels	15,000
Submittals	25,000
O&M	25,000
Construction Total	**1,100,000**
Subtotal	1,425,000
25% Contingency	356,250
Total	**1,781,250**

8.5.5 Purpose

This project is meant to address the following major recommendations of the SCADA Master Plan:

- Upgrade outdated equipment and standardize PLC systems at the N WRF.
- Add resiliency to the Fiber Optic Network.
- Add network management, standardization, and reliability to the Ethernet network.
- Standardize PLC programming platform and applications.
- Correct existing logic errors and increase automation.
- Provide operations staff with increased system access and visibility.

8.6 SCADA Governance

8.6.1 Scope and Description

This project includes the creation of a SCADA Governance plan. The purpose of the SCADA Governance plan is to ensure consistent management and maintenance of system assets and that employees follow the proper workflows for optimal business performance and to meet strategic objectives. The critical starting point for this task is for the utility to first create a SCADA Governance team of stakeholders to ensure all system users and managers have a stake in policy development and review of the group’s activities. The SCADA Governance plan also outlines policies in the following key areas as they relate to the SCADA group and its management:

1. SCADA Group Organization.
2. Policy and Procedure Management.
3. Asset Management Policies.
4. Document Control Policies.
5. Change Management Procedures.
6. Work Order Policies.
7. Project Definition and Execution.

These areas are key in establishing principles to meet the key objectives of:

- Availability - Staff and procedures in place to ensure systems are operational.
- Accountability - Justification of actions and decisions.
- Compliance - Changes and modifications are reviewed, tested, and documented.
- Standardization - All work and systems executed similarly.

The SCADA Governance Plan also includes the following sub policies which are part of other projects:

- Operational Policies.
- Disaster Recovery Policies.
- Emergency Response Policies.
- Cybersecurity Plan.
- Physical Security Plan.
- Standards and Specifications.

An additional portion of this project is to address SCADA system governance for conformance with industry best practices for cyber and physical security. System governance plays a key role in the development and implementation of security plans and implementations. This project will be critical for establishing decision makers, roles and responsibilities, and outlining priorities for system security.

Once initial policies are set for asset management then SCADA system assets can be populated in the CMMS system and work orders developed for these assets. This is most critical for SCADA assets which are not currently tracked in the utility CMMS. This project includes design service related to creation of plans and policies.

A subtask of this project is to develop physical and cyber security plans. These should be started in order to properly plan system security, develop guidelines for risk and vulnerability assessments, and associated emergency response plans. Additionally, this should give the County a foundation to address future potential requirements, similar to the America's Water Infrastructure Act (AWIA) requirement, in order to meet these requirements and additionally secure systems.

This task includes the development of physical and cyber security plans, including risk and vulnerability assessments to address the utility's security needs and to develop internal policies for security. These plans will provide the foundation of the utility's security program and provide a basis for mitigation planning to better secure the facilities and related infrastructure.

Physical Security planning should include the following aspects:

- Risk and Vulnerability assessments in accordance with AWWA G430 and J100 standards.
- Mitigation planning.
- Guidelines for perimeter security including the following:

  - Fencing and gate requirements.
  - Intrusion and entry detection and monitoring.
  - Mitigation of entry points and entry risks.
- Access credential management plan.
- Facility exterior and interior access control requirements.
- Definition of areas requiring camera and intrusion detection.
- Lighting requirements.
- IP Video management plan.
- Equipment standards.
- Training.
- Response Planning.

Part of security planning and modifications should include increased security at facilities to ensure the following:

- Process facilities cannot be accessed by general traffic at any time day or night without authenticated access.
- Buildings within facilities remain locked.
- Control rooms and critical control equipment can only be accessed by authorized staff.
- Camera and access control systems not associated with process control are located on non-process networks.
- SLAs or similar agreements are put in place with IT for standard electronic security component deployment.

Cybersecurity planning should include the following aspects:

- Risk and Vulnerability assessments in accordance with the AWWA cybersecurity use case tool and ICS-CERT CSET utility.
- Mitigation planning.
- Roles and Responsibilities.
- Audit Policies and Requirements.
- Architecture and Security Configuration Policies, Requirements, and guidelines.
- Data Security Policy and Procedures.
- Device Security Policy and Procedures.
- Access Control Policies and Procedures.
- Intrusion Detection Design Considerations.
- Personnel Security.
- Incident Response.
- Design Considerations - Cybersecurity Requirements.
- Training.
- Security Governance.
- Asset management.
- Recovery Plans.

This project includes design services to assist in plan generation.

8.6.2 Design

Design will include the following main aspects:

- Creation of a SCADA Governance Plan outlining the critical aspects necessary to consistently manage and maintain utility technical services for operation focusing on developing new policies and oversight for the SCADA system.
- Integration of GIS and CMMS Planning Activities into governance planning for a complete SCADA Governance Plan.
- Coordination with other sub policies being developed concurrently such as cyber and physical security plans and review and reference of existing policies such as IT and other Division policies currently in place.
- Coordination and updating of existing County policies such as Emergency Response.

8.6.3 Estimated Costs

The estimated costs associated with development of a comprehensive SCADA Governance Plan and related policies are summarized in the following table. These costs are not currently included in the overall SCADA project plan budget as numerous tasks may be completed internally or as a part of other projects:

Table 8.5 SCADA Governance Project Cost Estimate

Activities	Cost Estimate
SCADA Governance Plan	200,000
GIS Plan	50,000
CMMS Plan	50,000
Cybersecurity Plan	100,000
Physical Security Plan	50,000
Coordination with other Division policies	25,000
Coordination with County policies	25,000
Total	**500,000**

8.6.4 Purpose

This project addresses the following main items that were developed during staff workshops and recommendations of the SCADA Master Plan:

- Creation of a Governance Committee.
- Development and maintenance of system documentation such as policies, procedures, specifications, and standards.
- SCADA system management and maintenance.
- SCADA asset management, change management, and document control.
- Adherence to cyber and physical security best practices.
- Development of disaster recovery plans and policies related to SCADA infrastructure.

8.7 Add-on Projects

As a part of each project, other integrations and upgrades may be beneficial to meet County goals. Some of these upgrades can be incorporated into design and construction aspects of the projects listed above with minimal cost impacts, while others may make more sense for the County to implement internally in order to maintain system consistency.

8.7.1 Hach WIMs Development

As systems are expanded, more data is available, and more data is concentrated in the central historian, the existing Hach WIMs system should also be expanded to use this data for additional key performance indicators (KPIs), operator and management dashboards, and enhanced system maintenance capabilities as discussed in Chapter 6 of this report. Expansion of the Hach WIMs system could be included in facility projects to expand monitoring of that facility, however, finding integrators with good Hach WIMs experience can be difficult. It is more common for internal staff to continue development and build their own customized reports and dashboards. It is recommended to continue in this fashion as the County has already begun. In addition to the current Hach WIMs administrator and developer, it is recommended to train a member(s) of the operations staff in development within the Hach WIMs system as well. This provides for a backup person to assist with the system as well as operator insight in dashboard and report management.

The use of Hach Claros should also be explored to assist with instrument maintenance and as a mobile interface for data access. This system can be further integrated with ThinManager to provide more secure and centralized access.

8.7.2 Power Monitoring

As a part of facility PLC upgrades, additional power monitoring should be added. Existing power monitoring equipment and motor control equipment that has Ethernet capabilities should be upgraded and connected as possible or replaced with new components to facilitate Ethernet integration of power monitoring data. By standardizing new power monitoring equipment on Allen-Bradley components, pre-built add-on instructions in the Allen-Bradley PLCs can be used to monitor these devices with minimal programming required. Existing system CTs and PTs can be utilized with upgraded power monitoring equipment to make transitions simpler and more cost effective. Facility power management screens should be developed to not only show power usage but to aid operations staff in making decisions to reduce power usage.

8.7.3 CMMS Integrations

As a part of CitectSCADA upgrades, the equipment model within CitectSCADA should be utilized to organize data based on equipment. This organization will facilitate connectivity to CMMS systems as noted in previous chapters. The County can work with their CMMS provider and CitectSCADA vendor in order to facilitate this integration and determine if middleware such as Avantis Condition Manager are required to facilitate connectivity based on the County's intended use of this integration. This first step for this integration is for the County to clearly determine their desired outcomes of this integration so that the necessary components can be developed. This work can be included in SCADA governance development to create a cohesive asset management program for SCADA assets and work order management.

8.8 Control System Team Purpose and Benefits

For each project, it is critical that the implementation is done consistently between facilities. To meet this criteria, the integration team will be critical to the success of all upgrades and will have a great impact on future maintenance and upgrade requirements. This section outlines the importance and requirements for the Control System Team (CST) in order to provide a cohesive approach to addressing immediate and long-term control (SCADA) system maintenance, planning, and quality control needs.

Implementing a CST to manage the overall control system for the county facilities will have the following advantages:

- Eliminates the risk currently associated with having only one or two personnel capable of implementing programming changes to the SCADA system.
- Improves communication between various Operations and Maintenance staff as it relates to control system needs and wants.
- Provides a basis for team members to cross train in the various aspects of the SCADA systems, such as the control systems at the various WWTPs and WTP.
- Allows future projects at the plant to be constructed and documented according to county standards. This group would ensure control system standards continue to develop as needed, are updated and most importantly are enforced for all projects.
- Allows for long range planning related to control system updates.
- Balances workload for control system staff because CST members can share workload due to cross training.
- Provides a forum for systematically performing and tracking routine control system maintenance and updating associated system documentation.

8.8.1 Roles and Responsibilities

- To support the SCADA systems long term, making a combined team of CST, Maintenance, Engineering, and IIO staffs responsible for certain control system functions is recommended. Recommended key functions for the Engineering, CST, Maintenance, and IIO staff include responsibilities to support the SCADA systems. A team effort is envisioned among these groups.

8.8.2 Engineering Responsibilities

- Overall control system implementation should continue to be structured as an Engineering effort. This includes management of the control system tasks in capital improvement and rehabilitation and replacement projects.
- Engineering oversight should be accompanied by team leader support from the CST and IIO teams for all control system projects. This includes participation and commitment from each team member for capital improvement program (CIP) and replacement project planning and budgeting.
- Engineering responsibilities not only include enforcing control system standards but also providing turnkey solutions with team involvement. This ensures involvement from correct support team and enforces as built documentation, startup, and system commissioning.

8.8.3 CST and Maintenance Responsibilities:

- Ideally, the CST and Maintenance staff will support and maintain all components and programming for the field level and PLC level. At the process control system (PCS) level, the CST will support he Citect applications. CST and maintenance staff should also support internal networks to PCS, PLC, and field network levels including instrumentation and controls for the respective SCADA system.

8.8.4 IIO Responsibilities:

- IIO Responsibilities typically include fiber optic backbone at the enterprise level. Networks, network components, firewalls, servers, backup and recovery schemes, and historians.
- Near Term control (SCADA) system support may require additional personnel for all staff: CST, Maintenance and IIO staff.

8.8.4.1 Hardware Replacement

Background:

The SCADA Master Plan identifies a wide range of SCADA equipment/programmable logic controllers (PLCs) installed. The equipment varies considerably in terms of age, feature set, communication protocol, software and vendor support. Furthermore, most of these systems have been built in a piecemeal manner over the years by a wide variety of contractors, vendors, integrators, each with its own hardware design and programming approach.

As noted previously in this report field investigation found that although there are many different controllers in the Manatee County plant facilities, Rockwell PLCs are the most prevalent, which is consistent with industry standards.

Budgetary Costs:

The SCADA Master Plan identifies budgetary costs associated with replacement of the PLC equipment only for each control panel listed. Additional costs could be incurred if Manatee County replaces additional equipment in each control panel and the enclosure. For those control panels that may require additional or replacement surge protection, power supplies, relays, etc. the hardware and installation costs will increase.

Sequencing:

In an effort to manage the hardware and more specifically PLC replacement, below are some guidelines to determine potential order or sequencing of the PLC replacement work. The guidelines are intended to address those control panels with a higher replacement severity level first.

- Problematic control issues.
- Problematic electrical issues.
- Physical condition assessment.
- Process and operational significance.
- Age of hardware.
- Software compatibility with SCADA.

The quantity of hardware replacement projects, specifically PLC's, HMIs, and UPS is excessive. Utilizing the above guidelines is an approach that has proven effectiveness. It is recommended to begin with any networking projects to ensure the new PLCs will communicate effectively with the SCADA system when installed.

PLC Replacement Guidelines:

There are considerable planning tasks to be completed prior to performing the PLC hardware upgrade. The list below of planning tasks have been found to be very beneficial.

- When developing a new Rockwell Automation (Allen Bradley) PLC system regardless of size, it is best to utilize Rockwell's Integrated Architecture Builder (IAB). See the link below for further details.

  Rockwell Integrated Architecture Builder

- Update all PLC related drawings. This includes but is not limited to:
  - Power Wiring.
  - I/O module wiring.
  - Wire numbers.
  - Terminal numbers.
  - Control Panel layout.
- Complete PLC program migration to Studio 5000. It should be noted not all of the PLC program will be converted with the Rockwell software conversion utility. It will be necessary to test and verify the new program to ensure the program converted successfully as well as all features and functions converted properly.
- Prepare to update tags in the SCADA system if required.
- Procure the hardware.
- Develop a cut over plan. A cut over plan will identify the required tasks to perform the PLC upgrade. The cut over plan will identify the following:
  - Cut over phases (if more than one).
  - Resources.
  - Task identification number.
  - Task description.
  - Sub-Task (if any).
  - County Staff Coordination (identify county staff by names).
  - Notes (include shut down duration(s) Estimated start and finish dates and times for each task.

Below is an example of previous cut over plans that have been successful:

- Removal of existing PLC hardware.
- Removal of existing wiring (if necessary).
- Installation of new PLC hardware.
- Installation of new wiring including wire numbers and labels.
- CEET (Complete end to end testing). Test all new wiring.
- Test communication from PLC to SCADA and or other network equipment.
- Test data to/from PLC to/from SCADA.
- Test manual operation of control panel functionality.
- Test automatic operation of control panel automation.
- Complete system documentation.

8.9 Summary

The County currently has a general CIP program and other planned upgrade efforts for County facilities. This SCADA Master Plan should be coordinated with these other efforts where possible. Development of a SCADA governance committee having quarterly review meetings would help this effort to ensure synchronized implementation of the recommended improvements.

The main items addressed with the projects in this plan are focused around empowering staff with useable information, standardizing control system components and programming, and upgrading legacy hardware systems that are becoming increasingly harder to maintain. The projects listed in this chapter are intended to address these major items.

The following is a summary of the SCADA Master Plan:

Table 8.6 SCADA Master Plan Project Summary Table

Project Name	Estimated Start	Estimated Complete	Actual Start	Actual Complete	Budget
Core SCADA System	10/2020	7/2022			$1,431,250
SE WRF System SCADA	5/2021	5/2024			$2,462,500
SW WRF System SCADA	8/2021	12/2024			$2,531,250
N WRF System SCADA	1/2022	7/2024			$1,781,250
SCADA Governance	10/2020	8/2021			$500,000
Total	10/2020	FY24/25			$8,706,250

FY 2020 – 2024
Category: Wastewater **Subcategory:** Wastewater Treatment
Project Title: Core SCADA System Project
Department: Public Works Projects
Project Manager:
Infra. Sales Tax:
Project # **Status:** Requested

Comprehensive Plan Information

CIE Project: **N** Plan Reference:
LOS/Concurrency: **N** Project Need:

Project Location

Countywide

Description and Scope

Development of a centralized SCADA platform and SCADA related networking and security services. Project will include design and construction of the core SCADA system infrastructure to support central application management and access.

Rationale

To provide centralized management of SCADA system applications to reduce application maintenance and increase security and standardization.

Schedule of Activities

Activity	Start	End	Amount
Design:	10/20	4/21	343,750
Land:			
Construction:	7/21	7/22	1,087,000
Equipment:			
Project Mgt:			
Total Budgetary Cost Estimate:			1,431,250

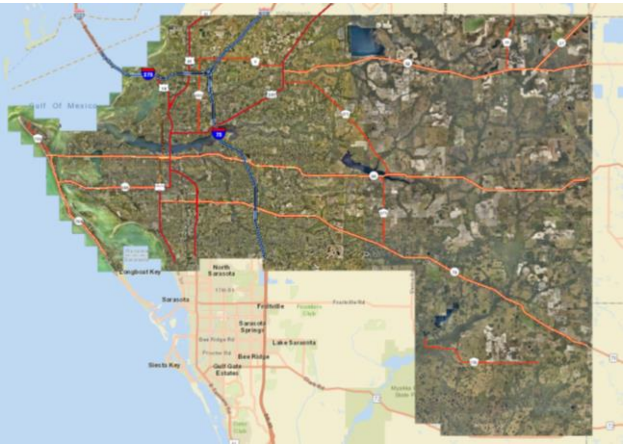
Operating Budget Impacts

Category	Fiscal Year	Amount
Personal:		
Non-Personal:		
Operating Capital:		
Operating Total:		

Programmed Funding

Expended to Date	Appropriated to Date	FY2021	FY2022	FY2023	FY2024	FY2025	Future
0	0	400,000	1,031,250	0	0	0	0

Project Map



Funding Strategy

Utility Rates

Means of Financing

Funding Source	Amount
Rates	1,431,250
Total Funding:	1,431,250

FY 2020 – 2024

Category: Wastewater **Subcategory:** Wastewater Treatment
Project Title: SE WRF SCADA Upgrades
Department: Public Works Projects
Project Manager:
Infra. Sales Tax:
Project # **Status:** Requested

Comprehensive Plan Information

CIE Project: **N** Plan Reference:
LOS/Concurrency: **N** Project Need:

Project Location

SE WRF

Description and Scope

This project includes the replacement of existing Legacy PLC systems and associated network hardware, OITs, and the addition of fiber optic cabling for modernization and standardization of equipment and added system resiliency at the SE WRF and includes upgrades for the MARS and Dryer

Rationale

Upgrade outdated equipment and standardize PLC systems at the SE WRF. Add resiliency to the Fiber Optic Network. Standardize PLC programming platform and applications.

Schedule of Activities

Activity	Start	End	Amount
Design:	5/21	5/22	443,750
Land:			
Construction:	6/22	5/24	2,018,750
Equipment:			
Project Mgt:			
Total Budgetary Cost Estimate:			2,462,500

Operating Budget Impacts

Category	Fiscal Year	Amount
Personal:		
Non-Personal:		
Operating Capital:		
Operating Total:		

Programmed Funding

Expended to Date	Appropriated to Date	FY2020	FY2021	FY2022	FY2023	FY2024	Future
0	0	185,000	595,210	1,009,380	672,910	0	0

Project Map

Cypress Strand

Funding Strategy

Utility Rates

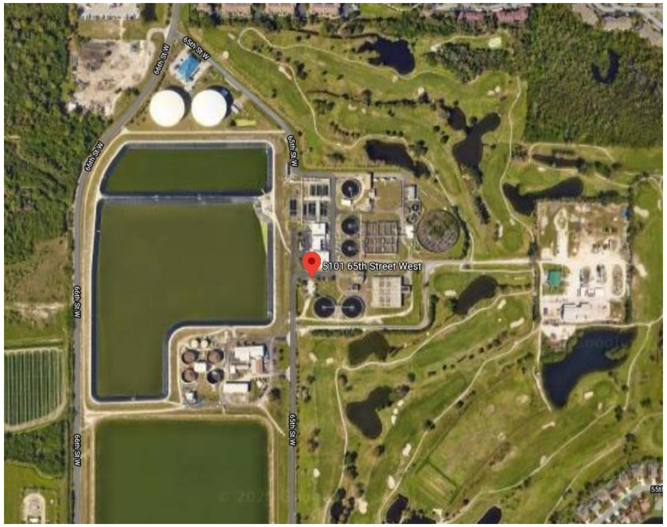
Means of Financing

Funding Source	Amount
Rates	2,462,500
Total Funding:	2,462,500

FY 2020 – 2024

Category: Wastewater **Subcategory:** Wastewater Treatment
Project Title: SW WRF SCADA Upgrades
Department: Public Works Projects
Project Manager:
Infra. Sales Tax:
Project # **Status:** Requested

Project Map



Comprehensive Plan Information

CIE Project: **N** Plan Reference:
LOS/Concurrency: **N** Project Need:

Project Location

SW WRF

Description and Scope

This project includes the replacement of existing Legacy PLC systems and associated network hardware, OITs, and the addition of fiber optic cabling for modernization and standardization of equipment and added system resiliency at the SW WRF

Rationale

Upgrade outdated equipment and standardize PLC systems at the SW WRF. Add resiliency to the Fiber Optic Network. Correct existing logic errors and increase automation.

Schedule of Activities

Activity	Start	End	Amount
Design:	8/21	8/22	468,750
Land:			
Construction:	9/22	12/24	2,062,500
Equipment:			
Project Mgt:			
Total Budgetary Cost Estimate:			2,531,250

Operating Budget Impacts

Category	Fiscal Year	Amount
Personal:		
Non-Personal:		
Operating Capital:		
Operating Total:		

Funding Strategy

Utility Rates

Means of Financing

Funding Source	Amount
Rates	2,531,250
Total Funding:	2,531,250

Programmed Funding

Expended to Date	Appropriated to Date	FY2020	FY2021	FY2022	FY2023	FY2024	Future
0	0	78,125	550,000	960,000	943,125	0	0

FY 2020 – 2024

Category:	Wastewater	**Subcategory:** Wastewater Treatment
Project Title:	North WRF SCADA Upgrades	
Department:	Public Works Projects	
Project Manager:		
Infra. Sales Tax:		
Project #		**Status:** Requested

Comprehensive Plan Information

CIE Project: **N**
LOS/Concurrency: **N**

Plan Reference:
Project Need:

Project Location

North WRF

Description and Scope

This project includes the replacement of existing Legacy PLC systems and associated network hardware, OITs, and the addition of fiber optic cabling for modernization and standardization of equipment and added system resiliency at the N WRF.

Rationale

Upgrade outdated equipment and standardize PLC systems at the N WRF. Add resiliency to the Fiber Optic Network. Standardize PLC programming platform and applications.

Schedule of Activities

Activity	Start	End	Amount
Design:	1/22	12/22	406,250
Land:			
Construction:	1/22	7/24	1,375,000
Equipment:			
Project Mgt:			
Total Budgetary Cost Estimate:			1,781,250

Operating Budget Impacts

Category	Fiscal Year	Amount
Personal:		
Non-Personal:		
Operating Capital:		
Operating Total:		

Programmed Funding

Expended to Date	Appropriated to Date	FY2020	FY2021	FY2022	FY2023	FY2024	Future
0	0	0	332,500	835,000	613,750	0	0

Project Map

© 2020 Google

Funding Strategy

Utility Rates

Means of Financing

Funding Source	Amount
Rates	1,781,250
Total Funding:	1,781,250

FY 2020 – 2024

Category:	Wastewater	**Subcategory:** Wastewater Treatment
Project Title:	SCADA Governance	
Department:	Public Works Projects	
Project Manager:		
Infra. Sales Tax:		
Project #		**Status:** Requested

Comprehensive Plan Information

CIE Project: **N** Plan Reference:
LOS/Concurrency: **N** Project Need:

Project Location

Countywide

Description and Scope

Development and maintenance of system documentation such as policies, procedures, specifications, and standards. SCADA asset management, change management, and document control. Development of disaster recovery plans and policies related to SCADA infrastructure.

Rationale

The purpose of the SCADA Governance plan is to ensure consistent management and maintenance of system assets and that employees follow the proper workflows for optimal business performance and to meet strategic objectives.

Schedule of Activities

Activity	Start	End	Amount
Design:	10/20	8/21	500,000
Land:			
Construction:			
Equipment:			
Project Mgt:			
Total Budgetary Cost Estimate:			500,000

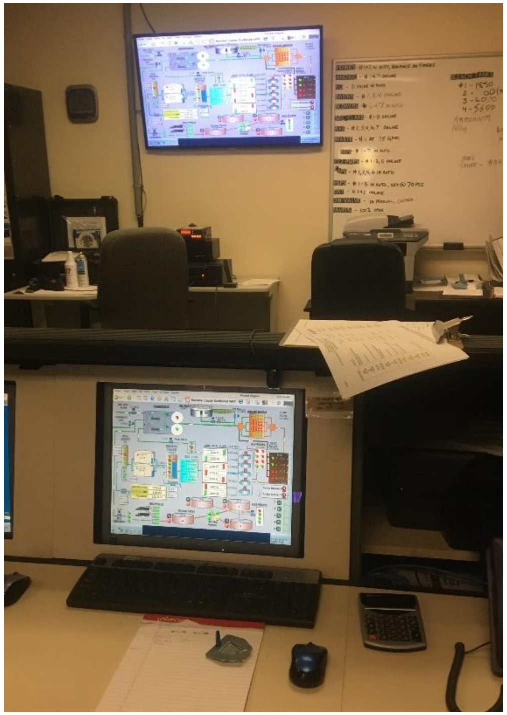
Operating Budget Impacts

Category	Fiscal Year	Amount
Personal:		
Non-Personal:		
Operating Capital:		
Operating Total:		

Programmed Funding

Expended to Date	Appropriated to Date	FY2020	FY2021	FY2022	FY2023	FY2024	Future
0	0	500,000	0	0	0	0	0

Project Map



Funding Strategy

Utility Rates

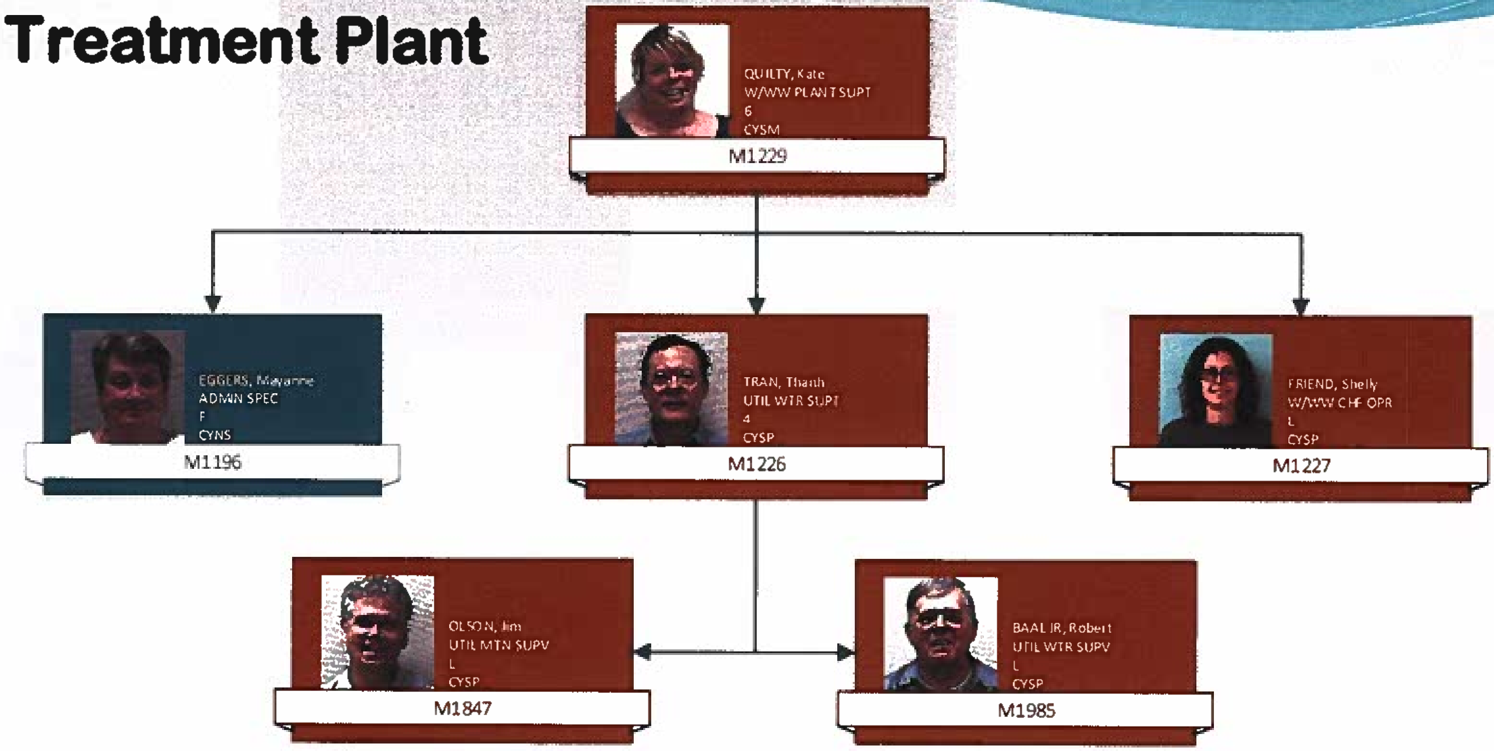
Means of Financing

Funding Source	Amount
Rates	500,000
Total Funding:	500,000

Appendix A
ORGANIZATIONAL CHARTS

UTILITIES

Water Treatment Plant



QUILTY, Kate
W/WW PLANT SUPT
6
CYSM
M1229

EGGERS, Mayanne
ADMN SPEC
F
CYNS
M1196

TRAN, Thanh
UTIL WTR SUPT
4
CYSP
M1226

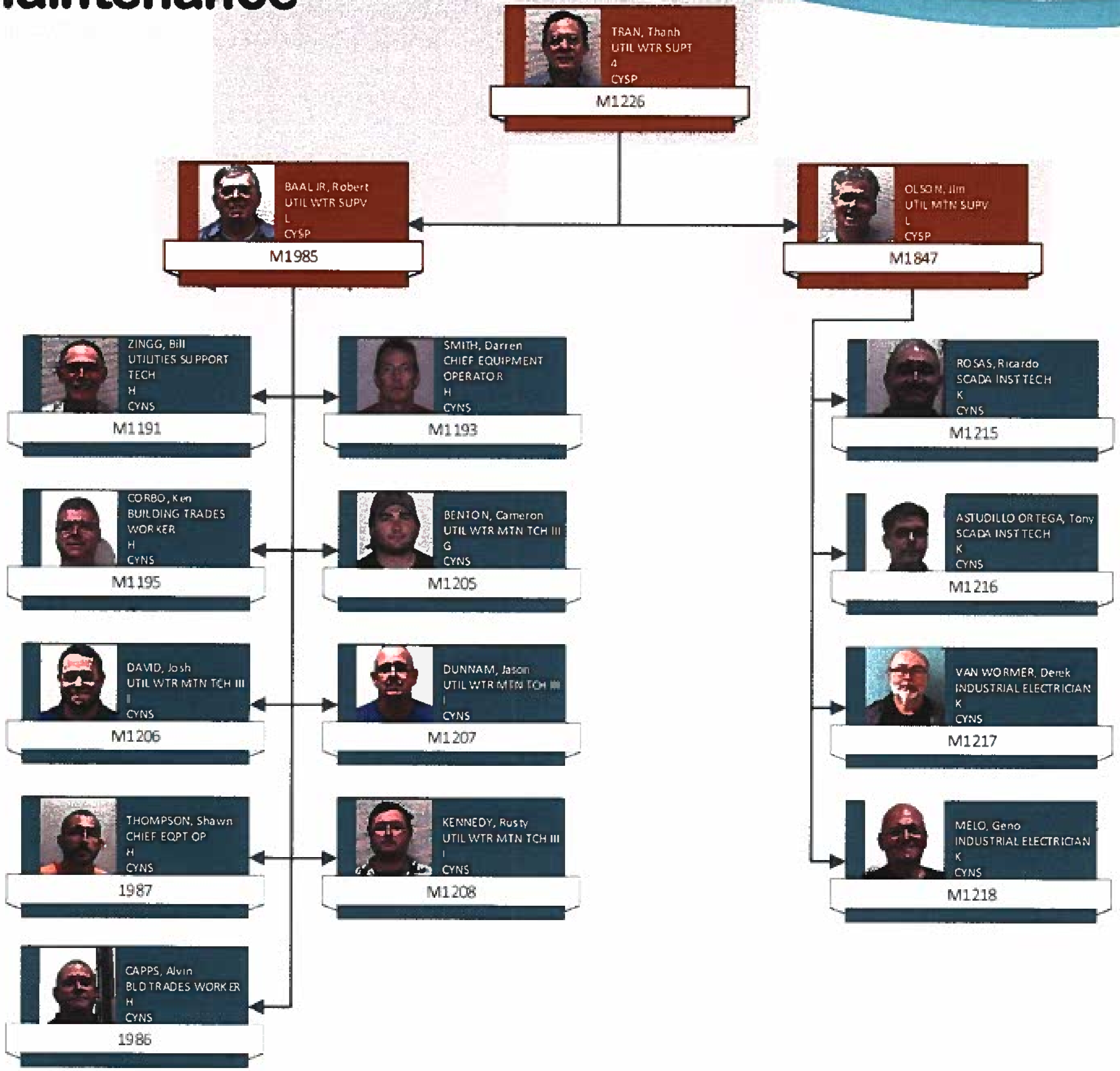
FRIEND, Shelly
W/WW CHF OPR
L
CYSP
M1227

OLSON, Jim
UTIL MTN SUPV
L
CYSP
M1847

BAAL JR, Robert
UTIL WTR SUPV
L
CYSP
M1985

Water Treatment Plant Maintenance

UTILITIES



TRAN, Thanh
UTIL WTR SUPT
4
CYSP
M1226

BAAL JR, Robert
UTIL WTR SUPV
L
CYSP
M1985

OLSON, Jim
UTIL MTN SUPV
L
CYSP
M1847

ZINGG, Bill
UTILITIES SUPPORT TECH
H
CYNS
M1191

SMITH, Darren
CHIEF EQUIPMENT OPERATOR
H
CYNS
M1193

CORBO, Ken
BUILDING TRADES WORKER
H
CYNS
M1195

BENTON, Cameron
UTIL WTR MTN TCH III
G
CYNS
M1205

DAVID, Josh
UTIL WTR MTN TCH III
I
CYNS
M1206

DUNNAM, Jason
UTIL WTR MTN TCH III
I
CYNS
M1207

THOMPSON, Shawn
CHIEF EQPT OP
H
CYNS
1987

KENNEDY, Rusty
UTIL WTR MTN TCH III
I
CYNS
M1208

CAPPS, Alvin
BLD TRADES WORKER
H
CYNS
1986

ROSAS, Ricardo
SCADA INST TECH
K
CYNS
M1215

ASTUDILLO ORTEGA, Tony
SCADA INST TECH
K
CYNS
M1216

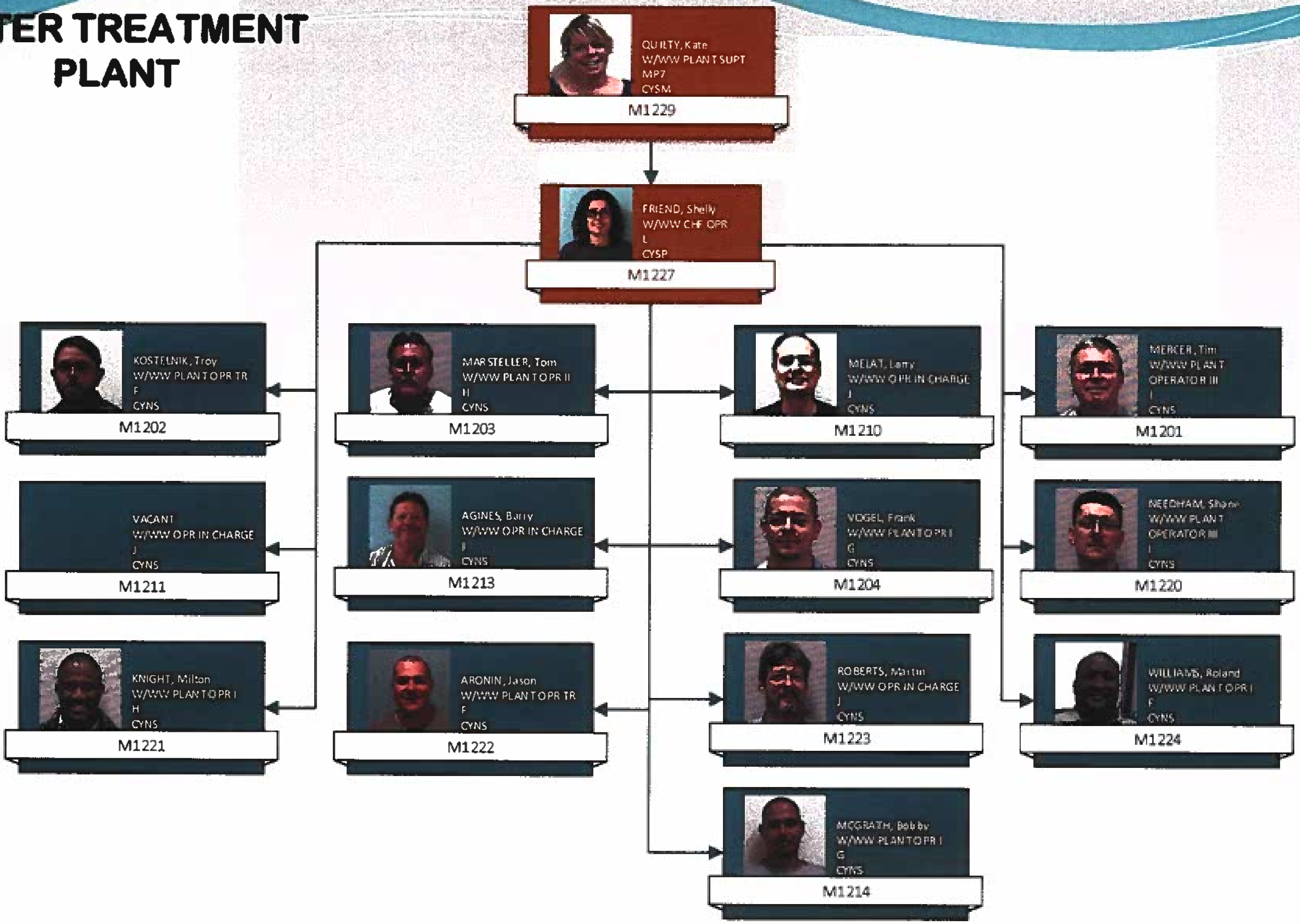
VAN WORMER, Derek
INDUSTRIAL ELECTRICIAN
K
CYNS
M1217

MELO, Geno
INDUSTRIAL ELECTRICIAN
K
CYNS
M1218

Manatee County
FLORIDA

UTILITIES

WATER TREATMENT PLANT



QUILTY, Kate
W/WW PLANT SUPT
MP7
CYSM
M1229

FRIEND, Shelly
W/WW CHF OPR
L
CYSP
M1227

KOSTELNIK, Troy
W/WW PLANT OPR TR
F
CYNS
M1202

VACANT
W/WW OPR IN CHARGE
J
CYNS
M1211

KNIGHT, Milton
W/WW PLANT OPR I
H
CYNS
M1221

MARSTELLER, Tom
W/WW PLANT OPR II
H
CYNS
M1203

AGINES, Barry
W/WW OPR IN CHARGE
I
CYNS
M1213

ARONIN, Jason
W/WW PLANT OPR TR
F
CYNS
M1222

MELAT, Larry
W/WW OPR IN CHARGE
J
CYNS
M1210

VOGEL, Frank
W/WW PLANT OPR I
G
CYNS
M1204

ROBERTS, Martin
W/WW OPR IN CHARGE
J
CYNS
M1223

MCGRATH, Bobby
W/WW PLANT OPR I
G
CYNS
M1214

MERCER, Tim
W/WW PLANT
OPERATOR III
I
CYNS
M1201

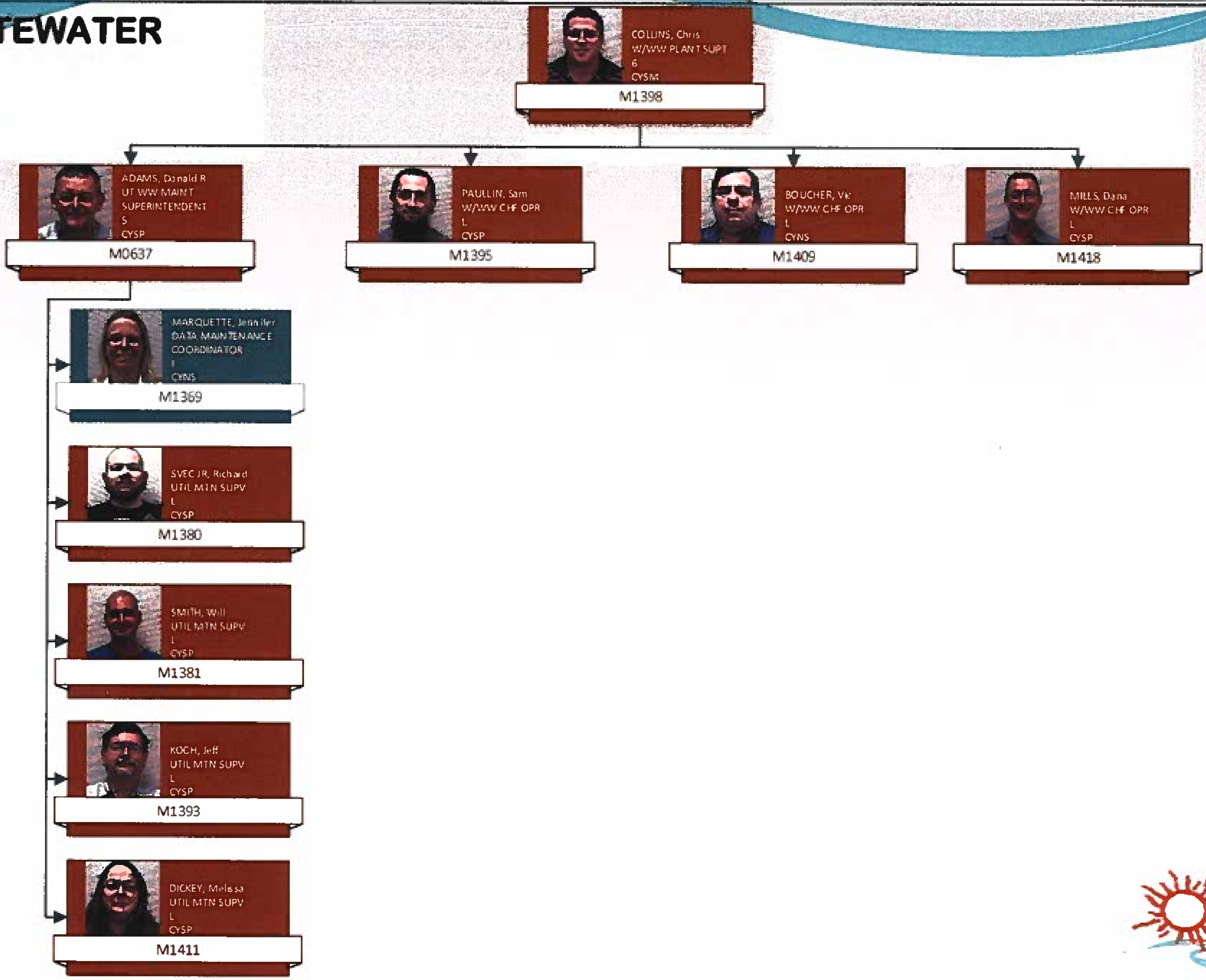
NEEDHAM, Shane
W/WW PLANT
OPERATOR III
I
CYNS
M1220

WILLIAMS, Roland
W/WW PLANT OPR I
F
CYNS
M1224

Manatee County
FLORIDA

UTILITIES

WASTEWATER



COLLINS, Chris
W/WW PLANT SUPT
6
CYSM
M1398

ADAMS, Donald R
UT WW MAINT SUPERINTENDENT
5
CYSP
M0637

PAULLIN, Sam
W/WW CHF OPR
L
CYSP
M1395

BOUCHER, Vic
W/WW CHF OPR
L
CYNS
M1409

MILLS, Dana
W/WW CHF OPR
L
CYSP
M1418

MARQUETTE, Jennifer
DATA MAINTENANCE COORDINATOR
I
CYNS
M1369

SVEC JR, Richard
UTIL MTN SUPV
L
CYSP
M1380

SMITH, Will
UTIL MTN SUPV
L
CYSP
M1381

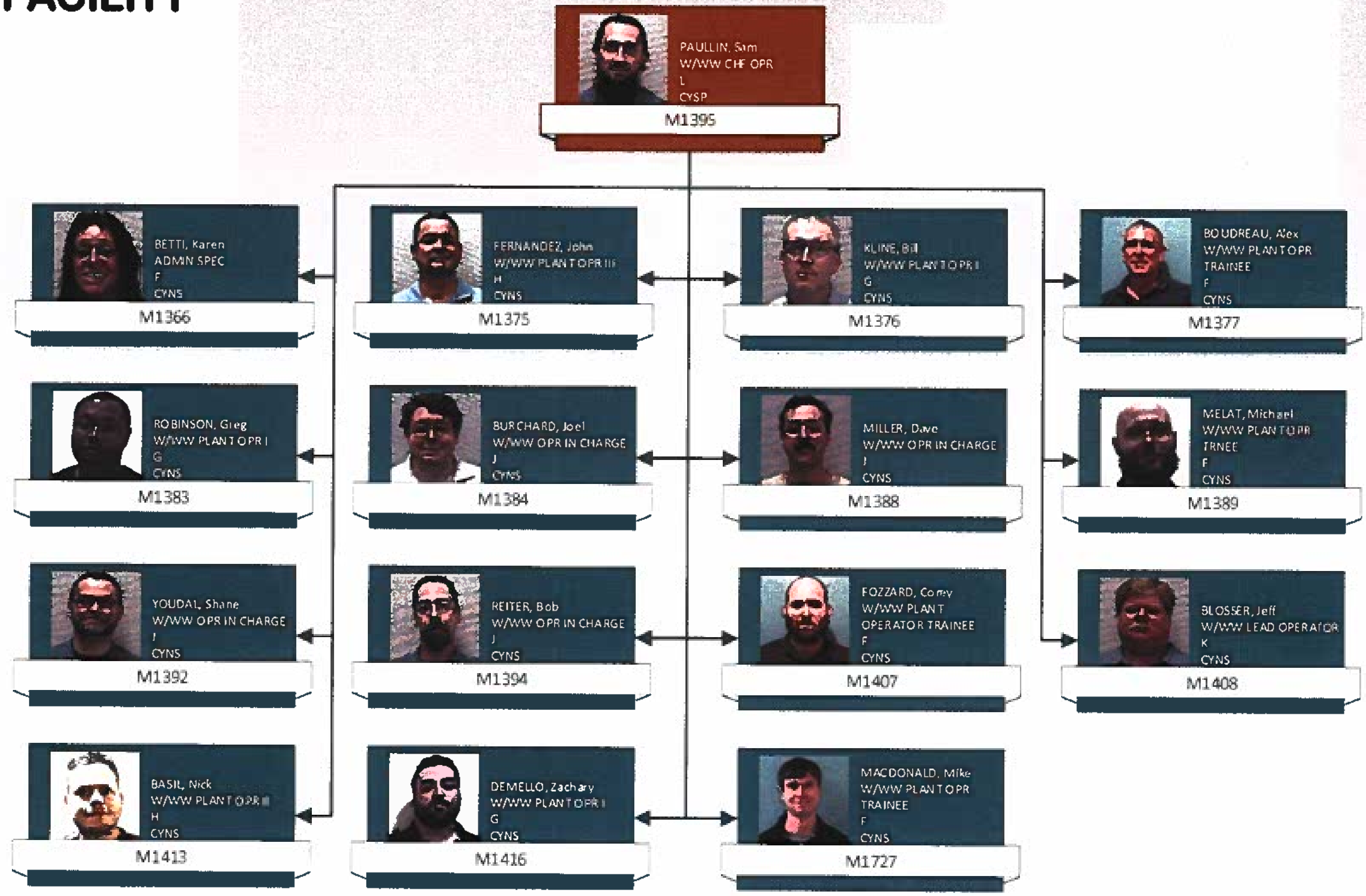
KOCH, Jeff
UTIL MTN SUPV
L
CYSP
M1393

DICKEY, Melissa
UTIL MTN SUPV
L
CYSP
M1411

Manatee County
FLORIDA

UTILITIES

SW WATER RECLAMATION FACILITY



PAULLIN, Sam
W/WW CHF OPR
L
CYSP
M1395

BETTI, Karen
ADMN SPEC
F
CYNS
M1366

ROBINSON, Greg
W/WW PLANT OPR I
G
CYNS
M1383

YOUDAL, Shane
W/WW OPR IN CHARGE
J
CYNS
M1392

BASIL, Nick
W/WW PLANT OPR II
H
CYNS
M1413

FERNANDEZ, John
W/WW PLANT OPR III
H
CYNS
M1375

BURCHARD, Joel
W/WW OPR IN CHARGE
J
CYNS
M1384

REITER, Bob
W/WW OPR IN CHARGE
J
CYNS
M1394

DEMELLO, Zachary
W/WW PLANT OPR I
G
CYNS
M1416

KLINE, Bill
W/WW PLANT OPR I
G
CYNS
M1376

MILLER, Dave
W/WW OPR IN CHARGE
J
CYNS
M1388

FOZZARD, Corey
W/WW PLANT
OPERATOR TRAINEE
F
CYNS
M1407

MACDONALD, Mike
W/WW PLANT OPR
TRAINEE
F
CYNS
M1727

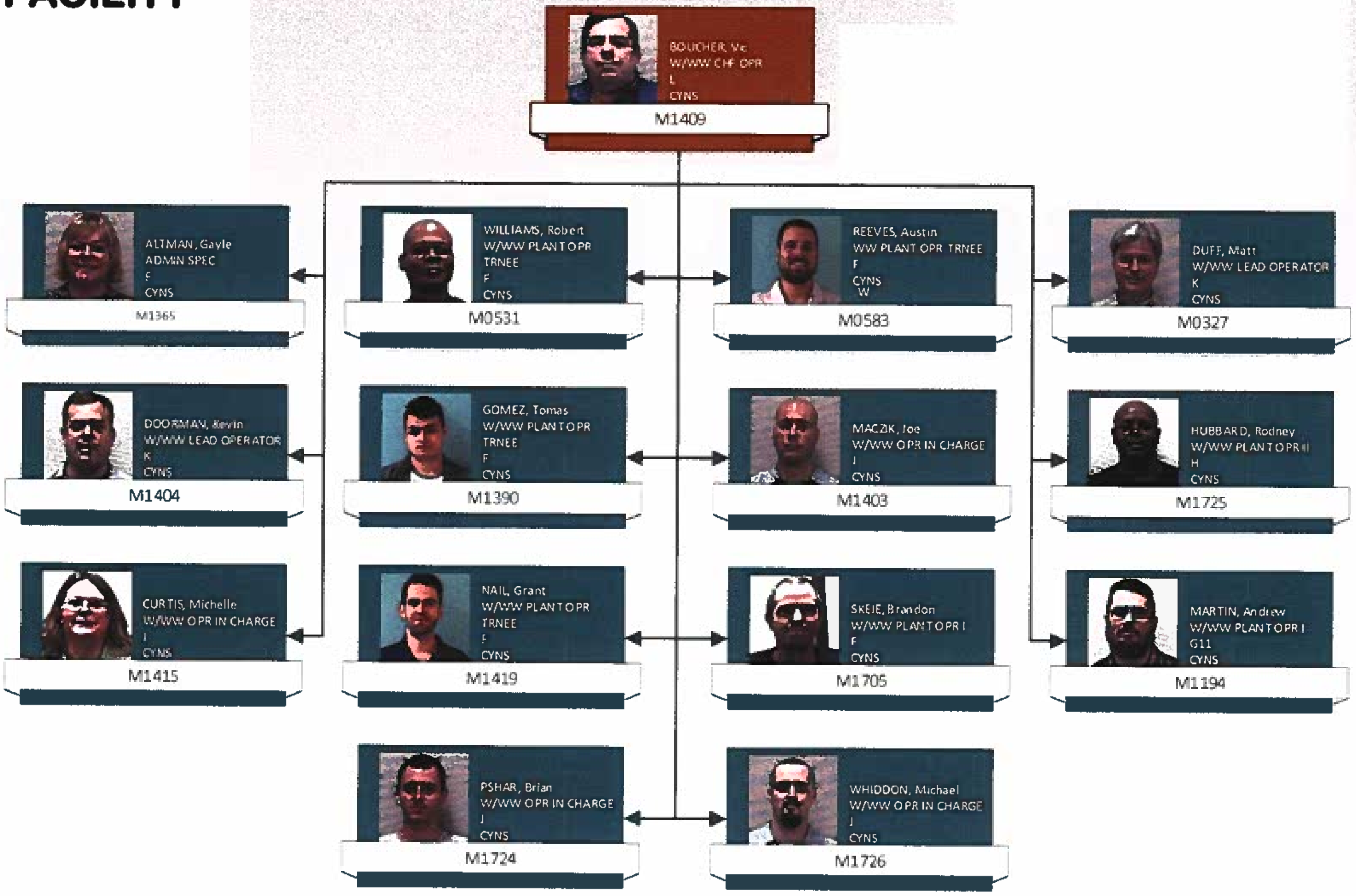
BOUDREAU, Alex
W/WW PLANT OPR
TRAINEE
F
CYNS
M1377

MELAT, Michael
W/WW PLANT OPR
TRNEE
F
CYNS
M1389

BLOSSER, Jeff
W/WW LEAD OPERATOR
K
CYNS
M1408

UTILITIES

SE WATER RECLAMATION FACILITY



BOUCHER, Vic
W/WW CHF OPR
L
CYNS
M1409

ALTMAN, Gayle
ADMIN SPEC
F
CYNS
M1365

WILLIAMS, Robert
W/WW PLANT OPR TRNEE
F
CYNS
M0531

REEVES, Austin
WW PLANT OPR TRNEE
F
CYNS
W
M0583

DUFF, Matt
W/WW LEAD OPERATOR
K
CYNS
M0327

DOORMAN, Kevin
W/WW LEAD OPERATOR
K
CYNS
M1404

GOMEZ, Tomas
W/WW PLANT OPR TRNEE
F
CYNS
M1390

MACZIK, Joe
W/WW OPR IN CHARGE
J
CYNS
M1403

HUBBARD, Rodney
W/WW PLANT OPR II
H
CYNS
M1725

CURTIS, Michelle
W/WW OPR IN CHARGE
J
CYNS
M1415

NAIL, Grant
W/WW PLANT OPR TRNEE
F
CYNS
M1419

SKEIE, Brandon
W/WW PLANT OPR I
F
CYNS
M1705

MARTIN, Andrew
W/WW PLANT OPR I
G11
CYNS
M1194

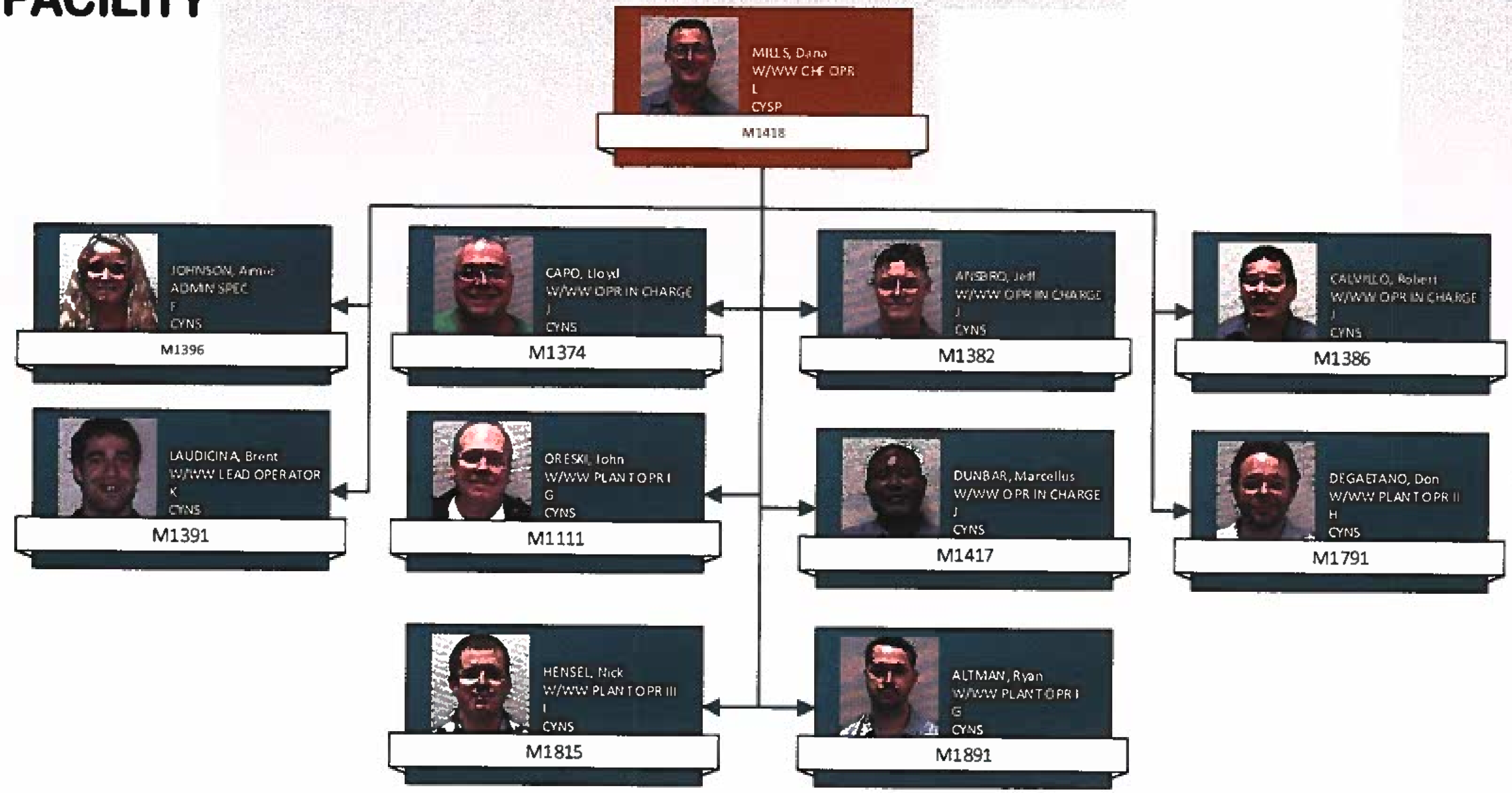
PSHAR, Brian
W/WW OPR IN CHARGE
J
CYNS
M1724

WHIDDON, Michael
W/WW OPR IN CHARGE
J
CYNS
M1726

Manatee County FLORIDA

UTILITIES

NORTH REGIONAL WATER RECLAMATION FACILITY



MILLS, Dana
W/WW CHF OPR
L
CYSP
M1418

JOHNSON, Amie
ADMIN SPEC
F
CYNS
M1396

LAUDICINA, Brent
W/WW LEAD OPERATOR
K
CYNS
M1391

CAPO, Lloyd
W/WW OPR IN CHARGE
J
CYNS
M1374

ORESKI, John
W/WW PLANT OPR I
G
CYNS
M1111

HENSEL, Nick
W/WW PLANT OPR III
I
CYNS
M1815

ANSBRO, Jeff
W/WW OPR IN CHARGE
J
CYNS
M1382

DUNBAR, Marcellus
W/WW OPR IN CHARGE
J
CYNS
M1417

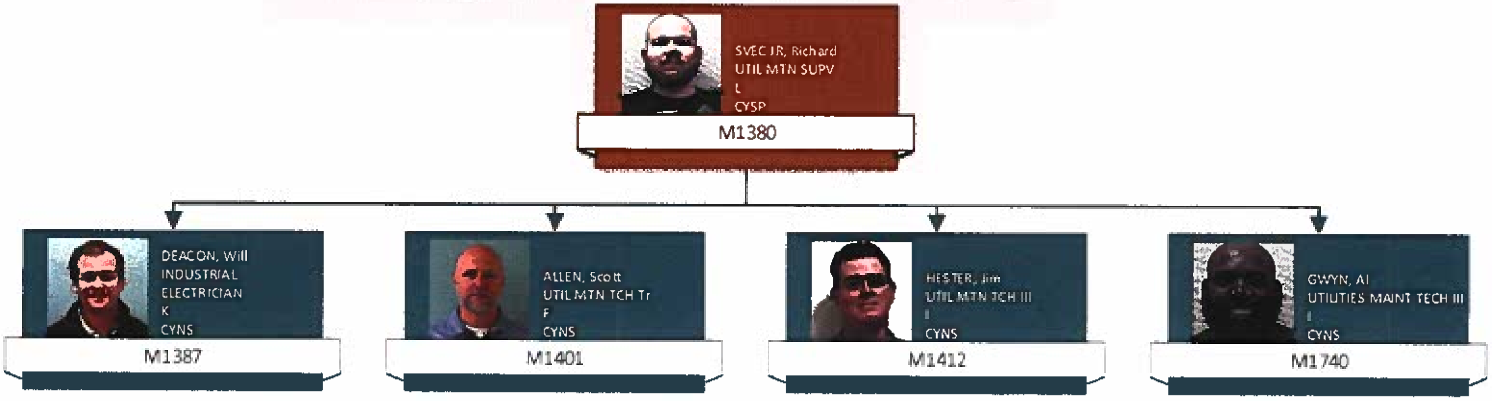
ALTMAN, Ryan
W/WW PLANT OPR I
G
CYNS
M1891

CALVILLO, Robert
W/WW OPR IN CHARGE
J
CYNS
M1386

DEGAETANO, Don
W/WW PLANT OPR II
H
CYNS
M1791

UTILITIES

NORTH RETIONAL WATER RECLAMATION FACILITY



SVEC JR, Richard
UTIL MTN SUPV
L
CYSP
M1380

DEACON, Will
INDUSTRIAL ELECTRICIAN
K
CYNS
M1387

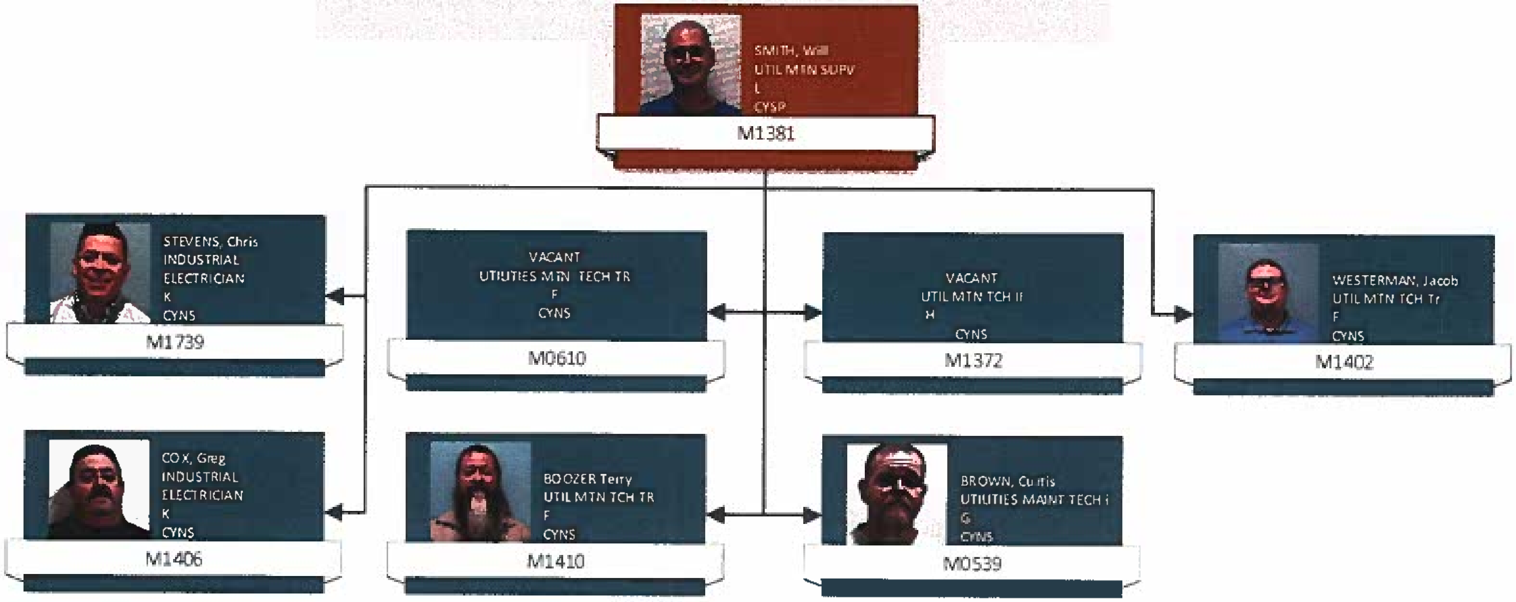
ALLEN, Scott
UTIL MTN TCH Tr
F
CYNS
M1401

HESTER, Jim
UTIL MTN TCH III
I
CYNS
M1412

GWYN, Al
UTIUTIES MAINT TECH III
I
CYNS
M1740

UTILITIES

SE WATER RECLAMATION FACILITY



SMITH, Will
UTIL MTN SUPV
L
CYSP
M1381

STEVENS, Chris
INDUSTRIAL ELECTRICIAN
K
CYNS
M1739

VACANT
UTIUTIES MTN TECH TR
F
CYNS
M0610

VACANT
UTIL MTN TCH II
H
CYNS
M1372

WESTERMAN, Jacob
UTIL MTN TCH Tr
F
CYNS
M1402

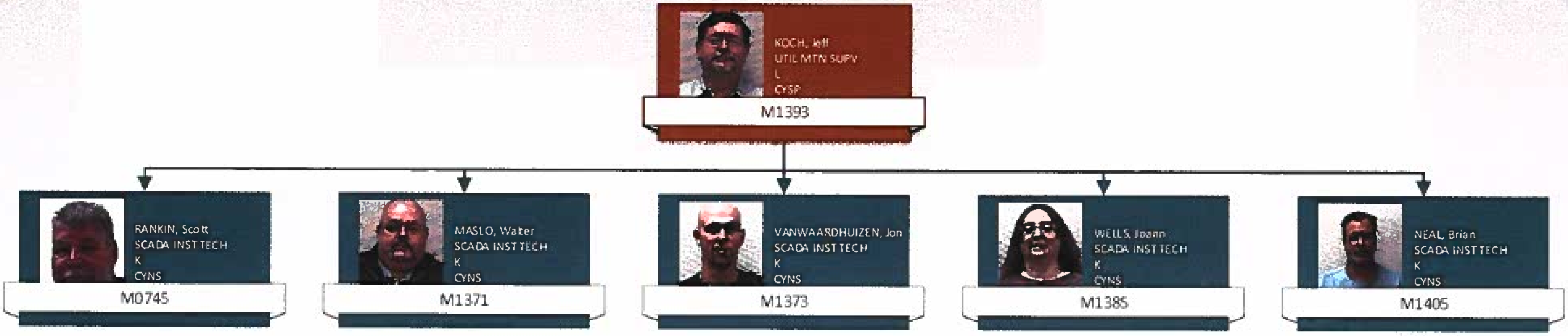
COX, Greg
INDUSTRIAL ELECTRICIAN
K
CYNS
M1406

BOOZER Terry
UTIL MTN TCH TR
F
CYNS
M1410

BROWN, Curtis
UTIUTIES MAINT TECH I
G
CYNS
M0539

UTILITIES

SW WATER RECLAMATION FACILITY



KOCH, Jeff
UTIL MTN SUPV
L
CYSP
M1393

RANKIN, Scott
SCADA INST TECH
K
CYNS
M0745

MASLO, Walter
SCADA INST TECH
K
CYNS
M1371

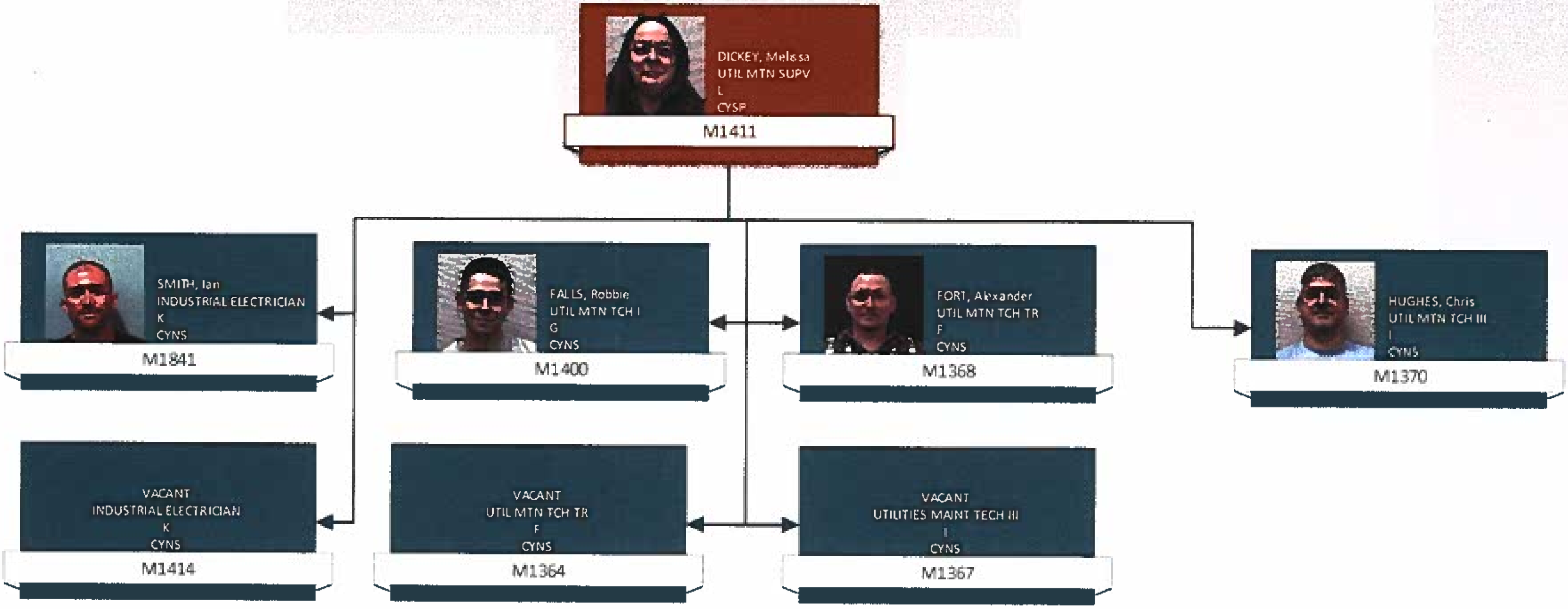
VANWAARDHUIZEN, Jon
SCADA INST TECH
K
CYNS
M1373

WELLS, Joann
SCADA INST TECH
K
CYNS
M1385

NEAL, Brian
SCADA INST TECH
K
CYNS
M1405

UTILITIES

SW WATER RECLAMATION FACILITY



DICKEY, Melissa
UTIL MTN SUPV
L
CYSP
M1411

SMITH, Ian
INDUSTRIAL ELECTRICIAN
K
CYNS
M1841

FALLS, Robbie
UTIL MTN TCH I
G
CYNS
M1400

FORT, Alexander
UTIL MTN TCH TR
F
CYNS
M1368

HUGHES, Chris
UTIL MTN TCH III
I
CYNS
M1370

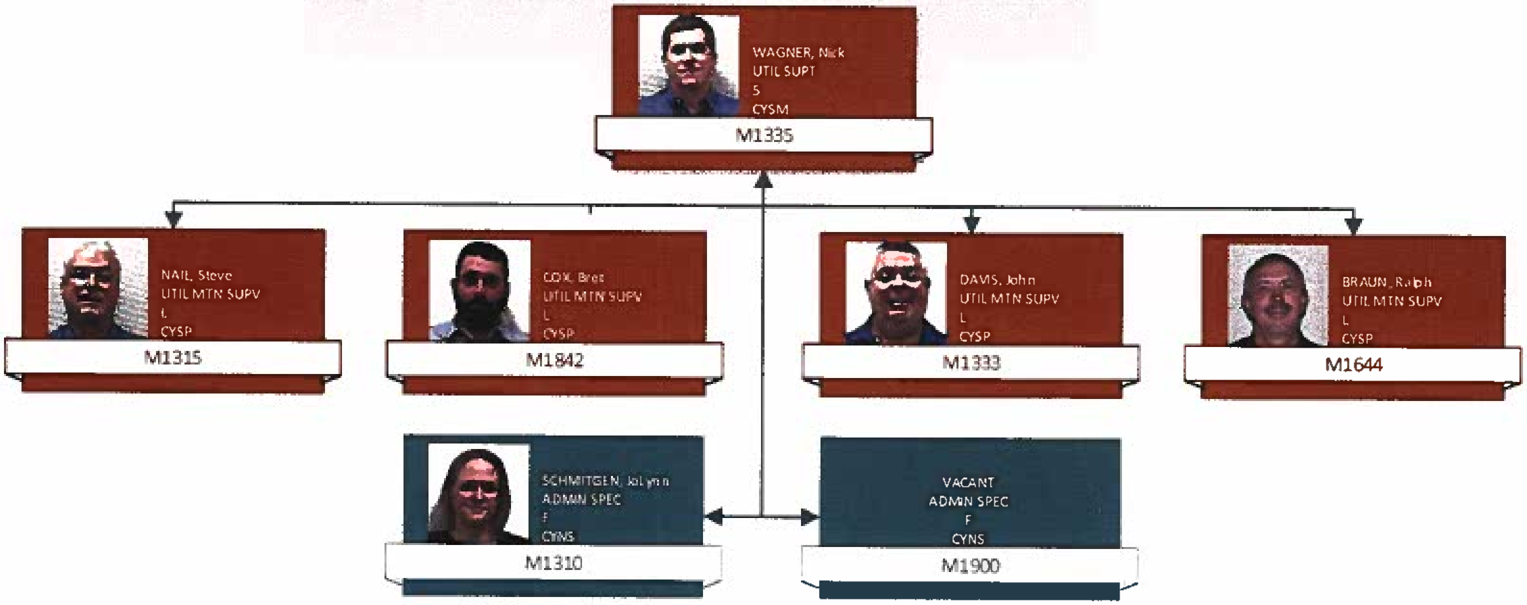
VACANT
INDUSTRIAL ELECTRICIAN
K
CYNS
M1414

VACANT
UTIL MTN TCH TR
F
CYNS
M1364

VACANT
UTILITIES MAINT TECH III
I
CYNS
M1367

UTILTIES

LIFT STATIONS



WAGNER, Nick
UTIL SUPT
S
CYSM
M1335

NAIL, Steve
UTIL MTN SUPV
L
CYSP
M1315

COX, Bret
UTIL MTN SUPV
L
CYSP
M1842

DAVIS, John
UTIL MTN SUPV
L
CYSP
M1333

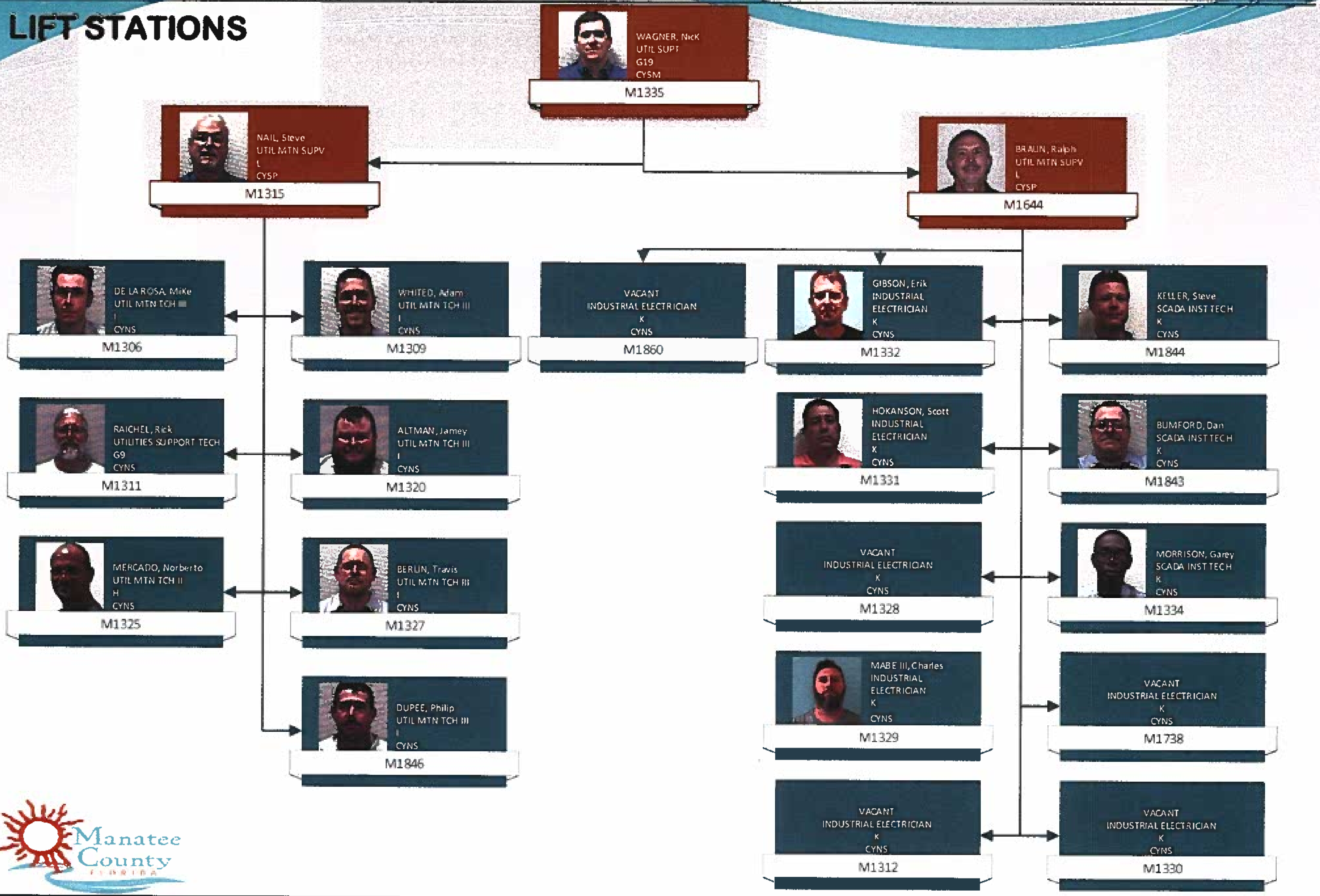
BRAUN, Ralph
UTIL MTN SUPV
L
CYSP
M1644

SCHMITGEN, JoLynn
ADMN SPEC
F
CYNS
M1310

VACANT
ADMN SPEC
F
CYNS
M1900

UTILITIES

LIFT STATIONS



WAGNER, Nick
UTIL SUPT
G19
CYSM
M1335

NAIL, Steve
UTIL MTN SUPV
L
CYSP
M1315

BRAUN, Ralph
UTIL MTN SUPV
L
CYSP
M1644

DE LA ROSA, Mike
UTIL MTN TCH [illegible]
I
CYNS
M1306

WHITED, Adam
UTIL MTN TCH III
I
CYNS
M1309

VACANT
INDUSTRIAL ELECTRICIAN
K
CYNS
M1860

GIBSON, Erik
INDUSTRIAL
ELECTRICIAN
K
CYNS
M1332

KELLER, Steve
SCADA INST TECH
K
CYNS
M1844

RAICHEL, Rick
UTILITIES SUPPORT TECH
G9
CYNS
M1311

ALTMAN, Jamey
UTIL MTN TCH III
I
CYNS
M1320

HOKANSON, Scott
INDUSTRIAL
ELECTRICIAN
K
CYNS
M1331

BUMFORD, Dan
SCADA INST TECH
K
CYNS
M1843

MERCADO, Norberto
UTIL MTN TCH II
H
CYNS
M1325

BERLIN, Travis
UTIL MTN TCH III
I
CYNS
M1327

VACANT
INDUSTRIAL ELECTRICIAN
K
CYNS
M1328

MORRISON, Garey
SCADA INST TECH
K
CYNS
M1334

DUPEE, Philip
UTIL MTN TCH III
I
CYNS
M1846

MABE III, Charles
INDUSTRIAL
ELECTRICIAN
K
CYNS
M1329

VACANT
INDUSTRIAL ELECTRICIAN
K
CYNS
M1738

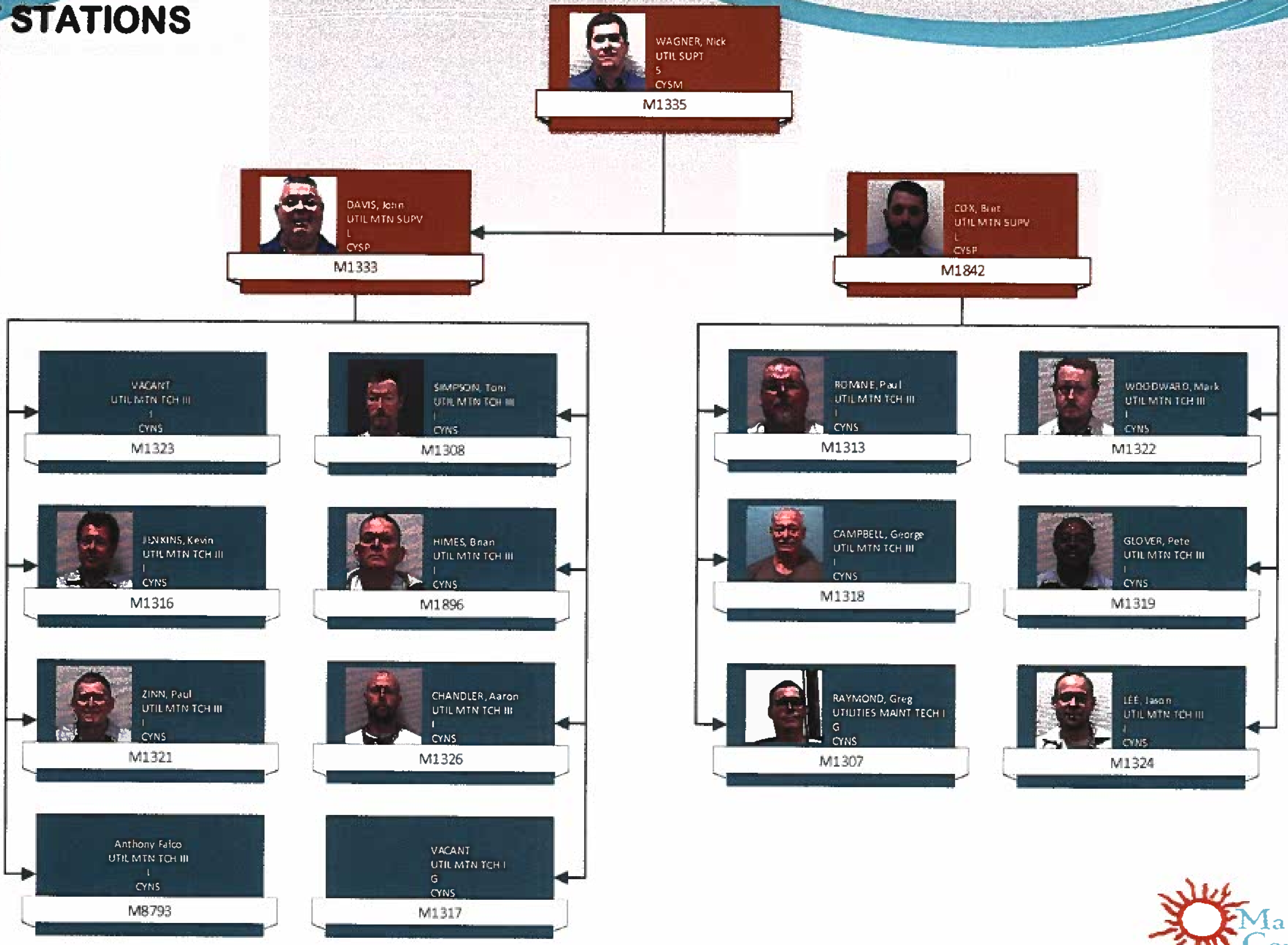
VACANT
INDUSTRIAL ELECTRICIAN
K
CYNS
M1312

VACANT
INDUSTRIAL ELECTRICIAN
K
CYNS
M1330

Manatee County
FLORIDA

UTILITIES

LIFT STATIONS



WAGNER, Nick
UTIL SUPT
5
CYSM
M1335

DAVIS, John
UTIL MTN SUPV
L
CYSP
M1333

COX, Bret
UTIL MTN SUPV
L
CYSP
M1842

VACANT
UTIL MTN TCH III
I
CYNS
M1323

SIMPSON, Toni
UTIL MTN TCH III
I
CYNS
M1308

JENKINS, Kevin
UTIL MTN TCH III
I
CYNS
M1316

HIMES, Brian
UTIL MTN TCH III
I
CYNS
M1896

ZINN, Paul
UTIL MTN TCH III
I
CYNS
M1321

CHANDLER, Aaron
UTIL MTN TCH III
I
CYNS
M1326

Anthony Falco
UTIL MTN TCH III
I
CYNS
M8793

VACANT
UTIL MTN TCH I
G
CYNS
M1317

ROMINE, Paul
UTIL MTN TCH III
I
CYNS
M1313

WOODWARD, Mark
UTIL MTN TCH III
I
CYNS
M1322

CAMPBELL, George
UTIL MTN TCH III
I
CYNS
M1318

GLOVER, Pete
UTIL MTN TCH III
I
CYNS
M1319

RAYMOND, Greg
UTILITIES MAINT TECH I
G
CYNS
M1307

LEE, Jason
UTIL MTN TCH III
I
CYNS
M1324

Appendix B

JOB DESCRIPTIONS

INSTRUMENT TECHNICIAN

Class Code:
232-100

Bargaining Unit: None Represented

MANATEE COUNTY GOVERNMENT
Established Date: Apr 11, 2009
Revision Date: Mar 2, 2011

SALARY RANGE

$16.44 - $25.50 Hourly
$34,195.20 - $53,040.00 Annually

GENERAL INFORMATION:

G12

This classification performs technical work in preventative and corrective maintenance and repair of electrical, electronic and pneumatic instrumentation in waste/water treatment plants or lift stations. Work also involves installation and modification of electronic instruments and control systems, including microprocessor/computer control systems and interfaces.

Working Conditions
Indoor/Outdoor situation; high noise environment while performing certain responsibilities. Lifting equipment up to 50 lbs. alone; up to 100 lbs. with assistance.

JOB DUTIES:

Essential Functions
These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position.

Performs preventative and corrective maintenance of instrumentation of waste/water treatment plants, lift stations, and related facilities.

Performs necessary adjustments and calibrations of instrumentation by using prepared chemical standards and portable electronic meters and related calibration equipment.

Installs new equipment and wires units according to electrical codes and schematics and diagrams provided; troubleshoots and makes repairs to all existing equipment.

Uses test equipment such as programmable logic controllers (PLCs), multimeters, digital voltmeters, digital calibrators, digital logic probes, oscilloscopes, frequency measuring meters and other pertinent electrical and electronic measuring devices. May be required to utilize Supervisory Control and Data Acquisition Systems (SCADA).

Calibrates all existing electrical equipment instruments with the use of calibration equipment mentioned above.

Services and repairs hydraulic, pneumatic, hydro-pneumatic and electro-pneumatic instrument/control systems.

Prepares necessary records and reports; prepares drawings, sketches and schematics.

Install, repair, maintain, and configure the radio telemetry system for all 533 manatee county lift stations.

Install, diagnose, repair lift station control panels as necessary when electricians need assistance.

Install, maintain, diagnose and repair field instrumentation used in control systems or for data acquisition in the telemetry system. These may be, but are not limited to flow meters, pressure transmitters, level sensors, rain gauges, vibration sensors.

Design new control systems and new data acquisition monitoring applications when necessary.

Bench test radio equipment to determine if it needs repair.

Perform any training that needs to be given to new instrument technicians, as well as training of electricians and mechanics on any equipment.

Performs other related work (including weather or other extreme emergency duties) as required.

Technical Requirements

Knowledge of principles and practices applied to preventative and corrective maintenance of electrical, electronic, pneumatic, microprocessor and other instrumentation of water treatment plants.

Knowledge of methods of operation of modern equipment and instrumentation of water treatment plants and related facilities and of work hazards and appropriate precautionary measures.

Knowledge of high and low voltage equipment and all types of flow meters, recorders and transmitters.

Knowledge of programmable logic controllers (PLCs), indicators, controllers, and other sensing equipment.

Knowledge of scientific electronic instrumentation of chemical monitoring systems repairs.

Knowledge and understanding of Supervisory Control and Data Acquisition Systems (SCADA).

Ability to read and understand programmable logic controllers (PLCs) ladder logic.

Ability to read and interpret electrical schematics, blueprints, piping layouts, and single line drawings.

Ability to read and understand specifications, instructions and recommendations.

Ability to distinguish colors.

Ability to apply theory, experience, and training in a logical and systematic fashion.

Ability to effectively deal with problems on a priority basis and investigate all possible causes before arriving at a conclusion.

Ability to establish and maintain effective working relationships with plant/field personnel, supervisor, and others.

Ability to work inside and outside in variable humidity and weather conditions, in noisy conditions, with solvents, on slippery and uneven surfaces, on or with moving objects, below ground level, in water, with odors and unusual fatigue factors; ability to perform strenuous work in adverse weather environments.

Ability to climb and descend ladders and stairs.

Ability to lift and move up to 50 pounds.

Ability to safely operate/drive a vehicle (car or pick up truck).

Ability to work emergency situations as required; ability to work after hours when needed and participate in a "standby" schedule.

MINIMUM QUALIFICATIONS:

High school diploma or equivalent certificate of competency. Prior courses or technical training in electronics, instrumentation and controls highly desired. Minimum of four (4) years experience in repair, inspection, adjustment, and calibration of electronic controls and instrumentation. Valid driver's license with valid Florida driver's license within 30 days of hire. Equivalent combinations of education and experience may be considered.

POSITION SPECIFIC:

ELECTRONICS, MAINTENANCE

INDUSTRIAL CONTROL TECHNICIAN

Class Code: 225-102

Bargaining Unit: None Represented

MANATEE COUNTY GOVERNMENT
Revision Date: Sep 20, 2017

SALARY RANGE

$18.48 - $28.65 Hourly
$38,438.40 - $59,592.00 Annually

GENERAL INFORMATION:

Paygrade: G14

Under general supervision, performs a variety of high level technical tasks relating to the maintenance, service, or installation of three phase electrical industrial plants. May work with high voltages when modifying, repairing, or installing electrical equipment and may be required to assume responsibility of controlling electrical emergencies. May initiate maintenance or repairs based on computerized radio telemetry reports or maintenance management system reports. Work is performed with considerable independence and reviewed for results obtained. Incumbent will be required to work after hours, weekends, and holidays when needed.

Working Conditions

Indoor/Outdoor situation; high noise environment while performing certain responsibilities. Lifting equipment up to 50 lbs. alone; up to 75 lbs. with assistance.

JOB DUTIES:

Essential Functions

These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position.

Performs maintenance, modification, repair, testing and installation of electrical fixtures and equipment in three phase industrial plants, including wiring, lighting, machinery, power appliances, overhead circuits, motors, relays, switches, and control boxes up to and including 4160-V, AC applications and, DC applications.

Performs emergency repair of industrial motor control centers.

Troubleshoots and repairs motors, appliances, heating and cooling equipment, and transformers. Works with single phase, split phase and three phase wiring.

Interprets and ensures compliance with existing electrical codes. Procures internal safety permits and wire numbers.

Works with electro-mechanical equipment and instrumentation motor control and process equipment; recommends replacement when necessary.

Maintains, repairs, adjusts, and installs electrical motors, generators, automatic power transfer switches, variable frequency drives,

radio telemetry systems, meters, timers and control centers in industrial applications.

Installs conduit, wall outlets, and fittings.

Detects causes of electrical failures; calculates line leads to determine wire and equipment size and capacity; prepares sketches for electrical layout and installations.

Performs other related work (including weather or other extreme emergency duties) as required.

MINIMUM QUALIFICATIONS:

High school diploma or equivalent certificate of competency.

Must have a minimum of six (6) years' experience as an Industrial (non-residential) Electrician
OR
a minimum of 3 years of experience as an Industrial (non-residential) Electrician with satisfactory completion of recognized training/certification program for electricians.

Valid driver's license with valid Florida driver's license within 30 days of hire.

Equivalent combinations of education and experience may be considered.

Desired - Licensed Master Industrial Electrician or State Electrical Contractor.

Knowledge/Skills/Abilities

Technical Requirements

Knowledge of the National Electrical Codes (NEC), use and care of advanced tools, equipment and testing devices of the electrical trade, and occupational hazards and safety precautions of the trade, including working with high voltages up to 4160-V, AC and DC circuits.

Knowledge of specialized testing equipment, high voltage safety equipment, and specialized high voltage material for repair of high voltage equipment; knowledge of high and low voltage equipment, knowledge of indicators, controllers and other process sensing equipment.

Knowledge of diesel engine controls with interface to electrical generator and automatic power transfer switches; knowledge of radio telemetry systems with interface to electro-mechanical controls.

Knowledge of manufacturers and their equipment for interfacing new technical equipment with old existing equipment.

Knowledge of CADD drawing programs.

Ability to analyze telemetry reports to predict failures of monitored equipment.

Ability to read and interpret intricate electrical control schematics, blue prints, piping layouts, single line drawings, with some knowledge of electronic schematics.

Ability to establish and maintain effective working relationships with others.

Ability to communicate clearly and effectively, orally, and in writing.

Ability to perform strenuous work tasks under adverse weather conditions.

Ability to work after-hours, weekends, and holidays when needed.

Ability to distinguish colors for various purposes, i.e., wiring, labels, etc.

Ability to climb and descend ladders.

Skill in the use of tools, materials and equipment used in the electrical trade.

Ability to understand ladder logic.

KEYWORDS:

Electronics, Facility Management, Maintenance, Professional, Trades, Water Treatment, Wastewater

CLASS SPEC TITLE 6:

03/23/2013
Entry pay for qualified applicant is $18.00/hour

INDUSTRIAL ELECTRICIAN

Class Code:
225-101

Bargaining Unit: None Represented

MANATEE COUNTY GOVERNMENT
Established Date: Apr 11, 2009
Revision Date: Mar 13, 2019

SALARY RANGE

$18.48 - $28.65 Hourly
$38,438.40 - $59,592.00 Annually

GENERAL INFORMATION:

Pay grade: G14
Under general supervision, performs a variety of high level technical tasks relating to the installation, maintenance or service of three phase electrical systems. May work with high voltages when installing, modifying or repairing electrical equipment and may be required to assume responsibility of controlling electrical emergencies. May initiate troubleshooting to motor controls or repairs based on computerized radio telemetry reports or maintenance management system reports. Oversees the work of lower level technical maintenance or laborer positions. Work is performed with considerable independence and reviewed for results obtained. Incumbent will be required to work after hours, weekends, and holidays when needed.

Working Conditions
Indoor/Outdoor situation; high noise environment while performing certain responsibilities. Lifting equipment up to 50 lbs. alone; up to 75 lbs. with assistance.

JOB DUTIES:

Essential Functions
These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position.

Oversees the work of lower level technical maintenance or laborer positions.

Oversees installation, maintenance, modification, and repair of electrical fixtures and equipment in three phase industrial plants, including wiring, lighting, machinery, power appliances, overhead circuits, motors, relays, switches, and control boxes up to and including 4160-V, AC application and DC voltages.

Performs emergency repair of industrial motor control centers.

Installs motors, appliances, heating and cooling equipment, and transformers. Works with single phase, split phase and three phase wiring.

Interprets and ensures compliance with existing electrical codes. Procures permits and layout numbers.

Works with electro-mechanical equipment and instrumentation motor control and process equipment; recommends replacement when necessary.

Installs, maintains, repairs and adjusts electrical motors, generators, automatic power transfer switches, variable frequency drives, eddy current drives, radio telemetry systems, meters, timers and control centers in industrial applications.

Installs conduit, wall outlets, and fittings.

Detects causes of electrical failures; calculates line leads to determine wire and equipment size and capacity; prepares sketches for electrical layout and installations.

Performs other related work (including weather or other extreme emergency duties) as required.

Technical Requirements

Knowledge of the National Electrical Codes (NEC), use and care of advanced tools, equipment and testing devices of the electrical trade, and occupational hazards and safety precautions of the trade, including working with high voltages up to 4160-V, AC and DC circuits.

Knowledge, or ability to obtain knowledge, of specialized testing equipment, high voltage safety equipment, and specialized high voltage material for repair of high voltage equipment; knowledge of high and low voltage equipment, knowledge of indicators, controllers and other process sensing equipment.

Knowledge of lathe and mill press operations.

Knowledge of diesel engine controls with interface to electrical generator and automatic power transfer switches; knowledge of radio telemetry systems with interface to electro-mechanical controls.
Knowledge of manufacturers and their equipment for interfacing new technical equipment with old existing equipment.

Knowledge of computer CADD drawing programs.

Ability to analyze telemetry reports to predict failures of monitored equipment.

Ability to read and interpret intricate electrical control schematics, blue prints, piping layouts, single line drawings, with some knowledge of electronic schematics.

Ability to effectively oversee and direct the work of others.

Ability to establish and maintain effective working relationships with others.

Ability to communicate clearly and effectively, orally, and in writing.

Ability to perform strenuous work tasks under adverse weather conditions.

Ability to work after-hours, weekends, and holidays when needed.

Ability to distinguish colors for various purposes, i.e., wiring, labels, etc.

Ability to climb and descend ladders.

Skill in the use of tools, materials and equipment used in the electrical trade.

MINIMUM QUALIFICATIONS:

High school diploma or equivalent certificate of competency.

Must have a minimum of six (6) years' experience as an Industrial (non-residential) Electrician or a minimum of 3 years of experience as an Industrial (non-residential) Electrician with satisfactory completion of recognized training/certification program for electricians.

Valid driver's license with valid Florida driver's license within 30 days of hire.

Equivalent combinations of education and experience may be considered.

Desired - Licensed Master Industrial Electrician or State Electrical Contractor.

POSITION SPECIFIC:

KEYWORDS:

Electronics, Facility Management, Maintenance, Professional, Trades, Water Treatment, Wastewater

CLASS SPEC TITLE 6:

03/23/2013
Entry pay for qualified applicant is $18.00/hour

SCADA INSTRUMENTATION TECHNICIAN

Class Code: 325-102

Bargaining Unit: None Represented

MANATEE COUNTY GOVERNMENT
Established Date: Jun 2, 2012
Revision Date: Oct 17, 2015

SALARY RANGE

$19.59 - $30.37 Hourly
$40,747.20 - $63,169.60 Annually

GENERAL INFORMATION:

PAY GRADE: G15

This classification performs a variety of advanced technical duties related to operating, maintaining, installing and troubleshooting instrumentation, process control and Supervisory Control and Data Acquisition (SCADA) systems for the County's waste/water treatment plants or wastewater lift stations system.

Working Conditions
Indoor/Outdoor situation; high noise environment while performing certain responsibilities. Lifting equipment up to 50 lbs. alone; up to 100 lbs. with assistance.

JOB DUTIES:

Essential Functions
These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position.

Facilitate/perform the implementation, coordination, supervision and maintenance of the SCADA Network.

Responsible for configuring, documenting and programming of the automation and control systems.

Responsible for all control aspects of in-house projects including design, programming, simulation, testing and start-up.

Perform general electrical work such as program VFDs, troubleshoot motor control panels and pull wire occasionally.

Perform preventative and corrective maintenance of instrumentation of waste/water treatment plants, lift stations, and related facilities.

Perform necessary adjustments and calibrations of instrumentation by using prepared chemical standards and portable electronic meters and related calibration equipment.

Install new equipment and wires units according to electrical codes and schematics and diagrams provided; troubleshoot and make repairs to all existing equipment.

Use test equipment such as multimeters, digital voltmeters, digital calibrators, digital logic probes, oscilloscopes, frequency measuring meters and other pertinent electrical and electronic measuring devices.

Calibrate all existing electrical equipment instruments with the use of calibration equipment mentioned above.

Service and repair hydraulic, pneumatic, hydro-pneumatic and electro-pneumatic instrument/control systems.

Prepare necessary records and reports; prepare drawings, sketches and schematics.

Install, repair, maintain, and configure the radio telemetry system for all 533 manatee county lift stations.
Install, diagnose, repair lift station control panels as necessary when electricians need assistance.

Install, maintain, diagnose and repair field instrumentation used in control systems or for data acquisition in the telemetry system. These may be, but are not limited to flow meters, pressure transmitters, level sensors, rain gauges, vibration sensors.

Design new control systems and new data acquisition monitoring applications when necessary.

Bench test radio equipment to determine if it needs repair.

Perform any training that needs to be given to new instrument technicians, as well as training of electricians and mechanics on any equipment.

Perform other related work (including weather or other extreme emergency duties) as required.

Technical Requirements
Knowledge of principles and practices of SCADA systems, specifically as applied to preventative and corrective maintenance of SCADA, including its electrical, electronic, pneumatic, microprocessor and other instrumentation components at water treatment plants.

Knowledge of methods of operation of modern equipment and instrumentation of water and wastewater treatment plants and related facilities and of work hazards and appropriate precautionary measures.

Knowledge of PLC and SCADA programming with Rockwell (RSLogix 500, Panelview, DeviceNet), Citect, Siemens and DFS.

Knowledge of antenna theory and related test equipment used to diagnose transmit/receive problems with radio telemetry systems.

Knowledge of tagging conventions, data logging and reporting, Boolean logic and symbol conventions.

Knowledge of external paging, alarming and reporting actions.

Knowledge of telemetry systems.

Knowledge of Autocad.

Knowledge of high and low voltage equipment and all types of flow meters, recorders and transmitters.

Knowledge of programmable logic controllers (PLCs), indicators, controllers, and other sensing equipment.

Knowledge of scientific, electronic instrumentation of chemical monitoring systems repairs.

Ability to read and understand programmable logic controllers (PLCs) ladder logic.

Ability to read, interpret, prepare and verify control schematics, diagrams, electrical schematics, blueprints, piping layouts, and single line drawings.

Ability to read and understand specifications, instructions and recommendations.

Ability to distinguish colors.

Ability to apply theory, experience, and training in a logical and systematic fashion.

Ability to effectively deal with problems on a priority basis and investigate all possible causes before arriving at a conclusion.

Ability to establish and maintain effective working relationships with plant/field personnel, supervisor, and others.

Ability to work inside and outside in variable humidity and weather conditions, in noisy conditions, with solvents, on slippery and uneven surfaces, on or with moving objects, below ground level, in water, with odors and unusual fatigue factors; ability to perform strenuous work in adverse weather environments.

Ability to climb and descend ladders and stairs.

Ability to work from aerial platform and perform repairs to antenna and coaxial cables.

Ability to lift and move up to 50 pounds.

Ability to safely operate/drive a vehicle (car or pickup truck).

Ability to work emergency situations as required; ability to work after hours when needed and participate in a "standby" schedule.

MINIMUM QUALIFICATIONS:

High school diploma or equivalent certificate of competency. Prior courses or technical training in electronics, instrumentation and controls highly desired. Minimum of Five (5) years experience in repair, inspection, adjustment, and calibration of electronic controls and instrumentation. Valid driver's license with valid Florida driver's license within 30 days of hire. Equivalent combinations of education and experience may be considered.

KEYWORDS:

ELECTRONICS, MAINTENANCE

SENIOR INDUSTRIAL ELECTRICIAN

Class Code:
138-100

Bargaining Unit: None Represented

MANATEE COUNTY GOVERNMENT
Established Date: Apr 11, 2009
Revision Date: Nov 7, 2011

SALARY RANGE

$20.46 - $31.72 Hourly
$42,556.80 - $65,977.60 Annually

GENERAL INFORMATION:

Pay grade: G16

This classification performs supervisory and skilled electrical, electronic air conditioning, and instrumentation maintenance work for water/wastewater facilities. Work involves establishing priorities on maintenance and repair work, scheduling and assigning work orders to electricians and technicians, and inspecting their work. Work also involves performing specialized repair and maintenance activities.

Working Conditions
Indoor/outdoor situation; high noise environment while performing certain responsibilities. Lifting equipment up to 25 lbs. alone; up to 50 lbs. with assistance.

JOB DUTIES:

Essential Functions
These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position.

Assists in planning work;establishes priorities.

Receives work orders or requests for repair or maintenance; prioritizes work; assigns, schedules, directs and evaluates work of assigned staff; conducts field inspections of work in process and upon completion to ensure that all work is performed according to code and safety regulations.

Directs and performs maintenance on electrical and electronic equipment, controls, air conditioning systems and other plant and lift station equipment; schedules preventative maintenance on equipment; modifies equipment as needed; installs new equipment up to and including 4160-V, AC application and DC voltages.

Maintains records on repair and maintenance activities and prepares reports. Confers with other supervisors and utility company representatives on projects involving electrical work; reviews plans and specifications; submits recommendations to improve the functioning of plant and lift station electrical equipment.

Troubleshoots electrical problems in plant and lift station equipment and takes corrective action.

Analyzes radio telemetry reports to predict problems with monitored equipment and issues work orders for corrective action; installs, configures, and maintains Radio Telemetry and Supervisory Control And Data Acquisition (SCADA) Systems.

Monitors computerized maintenance management work order system; establishes, maintains, and adjusts equipment maintenance schedules.

Participates in selection of new electricians and technicians; provides orientation to new hires; enforces safety regulations.

Additional Duties

Performs other related work (including weather or other extreme emergency duties) as required.

MINIMUM QUALIFICATIONS:

High school graduate/equivalent. Must be licensed as a Master Industrial Electrician or State Electrical Contractor, or may consider a minimum of eight (8) years experience as an industrial (non-residential) electrician with satisfactory completion of recognized training/certification program for electricians. Minimum of one (1) year of supervisory experience. Certified training in computerized maintenance management systems and radio telemetry desired. Valid Florida driver’s license. Equivalent combinations of education and experience may be considered.

Knowledge/Abilities/Skills

Knowledge of the National Electrical Codes (NEC), use and care of advanced tools, equipment and testing devices of the electrical trade, and occupational hazards and safety precautions of the trade, including working with high voltages up to 4160-V, AC and DC circuits.
Knowledge of the principles and practices applied to preventative and corrective maintenance of electronic, microprocessors, and other instrumentation of water and wastewater treatment plants.
Knowledge of components, software, and operation of radio telemetry systems.
Knowledge of components, operations and management of Supervisory Control and Data Acquisitions Systems (SCADA).
Knowledge of components, operation, and management of computerized maintenance management systems.
Ability to diagnose the seriousness of electrical and electronic failures and take appropriate corrective action.
Ability to schedule, assign, prioritize and evaluate work of assigned staff.
Ability to establish and maintain effective working relationships with others.
Ability to analyze vibration analysis reports and telemetry reports.
Ability to make estimates of time and materials accurately.
Ability to work from drawings, schematics and specifications, and to carry out oral and written instructions.
Ability to operate and maintain a computerized maintenance management system.
Ability to perform strenuous work tasks under adverse weather conditions.
Ability to work after hours, weekends and holidays when needed.
Ability to distinguish colors for various purposes, i. e., wiring, labels, etc.
Ability to climb and descend ladders.
Ability to work emergency situations as required.
Skill in locating and adjusting defects in electrical and electronic systems and equipment.
Skill in the use of tools, materials and equipment used in the electrical trade.
Skill in the use of advanced computer systems.

KEYWORDS:

Building Maintenance, Construction Maintenance, Construction Trades, Electronics, Trades, Maintenance

Appendix C
CAREER LADDER ELECTRICAL

ELECTRICIAN LADDER REQUIREMENTS

EMPLOYEE:	John Doe	**ID#**	M0000XX	**Section**	401	**Pos #**		**DOH**	

TITLE	REQUIREMENT	DATE ACHIEVED	DATE HIRED /PROMOTED
Prerequisite to be hired as a trainee:	Must have HS Diploma or GED with electrical aptitude and pass a one year in an electrical apprenticeship or technical school.		
Industrial Electrician Trainee	Apprenticeship		**01/01/2016**
Must complete trainee requirements in the first year of County Employment.	Possession of " Confined Space Training" Certification		
	Possession of " Blood Borne and Water Borne Pathogen Safety Course" Certification - County		
	Possession of " Electrical Safety" course -- cost and class unknown possible given by County		
	Possession of " Blood Borne and Water Borne Pathogen Safety Course" Certification County		
	Possession of "Electrical troubleshooting and Preventive Maintenance" course completion. (American Trainco $1980.00 +3 day hotel/travel- offered in Tampa)		
	Possession of "UDEMY PLC Programming From Scratch" course completion. ($15.00 online)		
	Possession of "AM1956 Electrical Schematics" course completion. (Polk State $498.00 +2 day hotel/travel)		
	Possession of "Drives- VFD online course" -- cost and class?		
	Prerequisite to be promoted to an Electrician I: Must demonstrate proficiency and complete Electrician I requirements with two years County employment as a trainee.		
Industrial Electrician I	Electrician		**01/01/2016**
Prerequisite to be hired: Must have HS Diploma or GED with six years' experience in Industrial Motor Controls, 480 VAC switchgear, VFD, PLC troubleshooting, and 4-20 analog controls. Must complete trainee requirements in the first year of County Employment and the Electrician I requirements in the second year of County Employment.	Possession of "Arc Flash Electrical Safety" Certification ($2000.00? + 1 day hotel/travel)		
	Possession of "Conductors, Terminators & Splices AM1958" (Polk State $498.00 + 1 day hotel/travel)		
	Possession of "Electrical Theory AM1952" (Polk State $498.00 +2 day hotel/travel)		
	Possession of "ControlLogix System Fundamentals. CCP146 (Polk State) (Polk State $798.00 ?+2 day hotel/travel)		
	Possession of "Water & Wastewater Treatment" AMI2080 (Polk State $1520.00 +3 d day hotel/travel)		
	Prerequisite to be promoted to an Electrician II: Must demonstrate proficiency and complete Trainee, Electrician I, and Electrician II requirements and have a minimum of five years County employment as an Electrician I and/or Electrician Trainee.		

ELECTRICIAN LADDER REQUIREMENTS

Industrial Electrician II	Equivalent to a Journeyman Electrician		**01/01/2016**
Prerequisite to be hired: Must have HS Diploma or GED and a Journeyman's license with six years' experience in Industrial Motor Controls, 480 VAC switchgear, VFD, PLC troubleshooting, and 4-20 analog controls. Must complete trainee requirements in the first year of County Employment and Electrician I requirements by the third year of County Employment.	Possession of "Generators & Emergency Power" (American Trainco $990.00 +2 day hotel/travel) Possession of "DFS - TAC PACK TCU Certification" (DFS $498.00? + 2 day hotel/travel??) Possession of "Motors, Drives and Control Circuits" (American Trainco $990.00 +2 d day hotel/travel) Possession of "System Problem Solving and Troubleshooting - Rockwell GEN-003" (Polk State (40 Hours) EM-206: Electrical Troubleshooting -- $2520.00? +4 day hotel/travel) Possession of "Modular Programming for Machine Applications: 9393-MODPROG" for Studio 5000 ControlLogix® ($399.00 ROCKWELL AUTOMATION CD) Prerequisite to be promoted to an Electrician II : Must demonstrate proficiency and complete Trainee, Electrician I, and Electrician II requirements and have a minimum of five years County employment as an Electrician I and/or trainee.		
Industrial Electrician III	Equivalent to a Master Electrician's License		**01/01/2016**
Prerequisite to be hired: Must have HS Diploma or GED and a Master Electrician license with six years' experience in Industrial Motor Controls, 480 VAC switchgear, VFD, PLC troubleshooting, and 4-20 analog controls. Must complete trainee requirements in the first year of County Employment and	Possession of "PowerFlex 700 vector control communications over Devicenet" (Polk State $1520.00 +4 day hotel CCA12/travel) Possession of "EM204 Advanced Motor Control" (Polk State $1520.00 +4 day hotel CCA12/travel) Possession of "CCP153 Studio 5000⍰ Logix Designer Level 2: ControlLogix® Maintenance and Troubleshooting" (Polk State $1520.00 + 4 day hotel/travel) Possession of "CitectSCADA / Vijeo Citect Architecture and Redundancy Virtual Training" ($1000.00? Citect/BCI Online training) Prerequisite: Must demonstrate proficiency and complete Industrial Electrician II requirements and have minimum three years County employment as an Electrician II.		

ELECTRICIAN LADDER REQUIREMENTS

Electrician I requirements by the third year of County Employment.			
Electrical Supervisor			**01/01/2016**
Must complete Electrical Supervisor requirements in the first four years of County Employment.	Possession of " "EPE Supervisor Training" Certification by County		
	Possession of "Microsoft Word office" Certification by County		
	Possession of "Microsoft Excel office" Certification by County		
	Possession of "Effective Team Building" Certification by County		
	Possession of "Workplace Sensitivity" Certification by County		
	Possession of " Leadership Academy" Certification by County		
	Possession of "Employment Law 101" Certification by County		
	Possession of "Advanced supervisory Development Program" Certification by County		
	Prerequisite: Must demonstrate proficiency and complete Electrical/SCADA Supervisor requirements and have minimum one year County employment as an Electrician III or SCADA III and be interviewed and be offered the open position.		

Appendix D
EQUIPMENT LIST

Facility	Tag Number	Control Panel	Description	Manufacturer	Platform	Model #	CPU	Comm	QTY	DI	QTY	DO	QTY	AI	QTY	AO	QTY	RTD	QTY	Thermocouple	QTY	Relay	QTY	Notes:
MCMRS		63rd Street PLC Panel	63rd Street MARS PLC	Allen-Bradley	SLC	SLC5/05				IA16	3	OA16	1	INI4i	3									
MCMRS		Rye Road PLC Panel	Rye Road MARS PLC	Allen-Bradley	SLC	SLC5/05				IA16	4	OA16	1	INI4i	3									
MCMRS		Spencer Parish PLC Panel	Spencer Parish MARS PLC	Allen-Bradley	SLC	SLC5/05				IA16	3	OA16	1	INI4i	3									
North WRF		MARS_NE	SLC 5/05	Allen-Bradley	SLC	1747-L553C				IB16	1	OB16	1	NI8	1	NO4I	1							
North WRF		SP-1	SLC 5/05	Allen-Bradley	SLC	1747-L553C				IB16	2	OB16	1	NI8	1	NO4I	1							
North WRF		SP-2	SLC 5/05	Allen-Bradley	SLC	1747-L553C				IB16	1	OB16	1	NI8	1	NO4I	1							
North WRF		SP-3	SLC 5/05	Allen-Bradley	SLC	1747-L553C				IB16	4	OB16	1	NI8	2									
North WRF		SP4_N	SLC 5/05	Allen-Bradley	SLC	1747-L553C				IB16	6	OB16	1	NI8	3	NO4I	2							
North WRF		NE_Everfilt	SLC 5/05	Allen-Bradley	SLC	1747-L553C				I*16	5	O*8	6	NI4	1									
North WRF		Lake Filter North	SLC 5/05	Allen-Bradley	SLC	1747-L541C				I*16	5	O*8	6	NI4	1									
North WRF		ADF12PLC	SLC 5/05	Allen-Bradley	SLC	1747-L542C				IA16	5	OW16	3	NI8	1									
North WRF		Micro Clarifier Pump West	Micrologix 1100	Allen-Bradley	MicroLogix	1763																		
North WRF		Sludge Pump #1	Micrologix 1100	Allen-Bradley	MicroLogix	1763																		
North WRF		Sludge Pump #2	Micrologix 1100	Allen-Bradley	MicroLogix	1763																		
SE WRF		Headworks MCC	SP2-A Rack 0	Allen-Bradley	SLC	SLC5/05				IA16	3	OW16	2	NI8	4	NO4I	2							
SE WRF		Headworks MCC	SP2-B Rack 1	Allen-Bradley	SLC	SLC5/05				IA16	3			NI8	1									
SE WRF		Headworks MCC	SP2-B Rack 2	Allen-Bradley	SLC					IA16	3	OW16	3	NI8	1									
SE WRF		Headworks	Spiragrit Control Panel- Micrologix	Allen-Bradley	MicroLogix	1400 (X 2)																		
SE WRF		Beltpress Office	SP-4	Allen-Bradley	SLC	SLC5/05				IB16	1	OW16	2	NI8	4	NO4I	1							
SE WRF		Bio-Solids Building	RTO	Allen-Bradley	SLC	SLC5/05				IA16	4	OW16	2	NI4	2	NO4I	2	NR4	1	NT8	1			
SE WRF		Bio-Solids Building	R10-10 (PLC 10)	Allen-Bradley	SLC	SLC5/05				IA16	1	OW16	2							NT8	1			
SE WRF		Bio-Solids Building	Micrologix-Burner Mgmt Panel	Allen-Bradley	MicroLogix	1500				IA16	1			IF4	1	OF2	1	IT6	1					
SE WRF		Blower Building	SP-3	Allen-Bradley	SLC	SLC5/05				IA16	4	OW16	1	NI8	2	NO4I	3							
SE WRF		Main MCC	SP1-A	Allen-Bradley	SLC	SLC5/05				IA16	3	OW16	2	NI8	2	NO4I	2							
SE WRF		Main MCC	SP1-B Rack 1	Allen-Bradley	SLC					IA16	2	OW16	1	NI8	2	NO4I	3							
SE WRF		Main MCC	SP1-B Rack 2	Allen-Bradley	SLC					IA16	4			NI8	3									
SE WRF		In front of Nova filters	SP5	Allen-Bradley	SLC	SLC5/05				IB16	4													
SE WRF		Main MCC High Service Room	SP6	Allen-Bradley	CompactLogix	Compact Logix L33ER				IQ16	2	OW16	1	IF41	2									
SE WRF		GBT Panel	GBT1	Allen-Bradley	SLC	SLC5/05				IA16	3	OW16	2	NI8	1	NO4I	1							
SE WRF		GBT2 Panel	GBT2	Allen-Bradley	CompactLogix	Compact Logix L30ER				IA16	3	OW16	3	IF8	1	OF4	1							
SE WRF		Main MCC back room	RTD HSP1	Allen-Bradley	MicroLogix	Micrologix 1100																		
SE WRF		Main MCC back room	RTD HSP2	Allen-Bradley	MicroLogix	Micrologix 1100																		
SE WRF		Main MCC back room	RTD HSP3	Allen-Bradley	MicroLogix	Micrologix 1100																		
SE WRF		Main MCC back room	RTD HSP4	Allen-Bradley	MicroLogix	Micrologix 1100																		
SE WRF		Main MCC back room	RTD Jockey P1	Allen-Bradley	MicroLogix	Micrologix 1100																		
SE WRF		Main MCC back room	RTD Jockey P2	Allen-Bradley	MicroLogix	Micrologix 1100																		
SE WRF		Poly Room	Polyomer Mixing Management Panel	Allen-Bradley	MicroLogix	Micrologix 1000																		
SE WRF		Main MCC	Generator Controller	GE	Other	90-30																		
SE WRF		Landfill Gas Panel	Landfill flame station	GE	Other	Versamax																		
SW WRF		Operations Room	Operations Room SW_RU SLC-5/05	Allen-Bradley	SLC	1747-L553C		1747-SDN	1	1746-IA16	1	1746-OA16	1	1746-NI8	1	1746-NO4I	1							
SW WRF		LSPS SP-1	Low Service PS (LSPS) SP-1 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IB16	6	1746-OB16	1	1746-NI8	5	1746-NO4I	2							
SW WRF		Chemical Bldg SP-2	Chemical Bldg SP-2 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IB16	3	1746-OB16	1	1746-NI8	4	1746-NO4I	3							
SW WRF		DAF Bldg SP-3	DAF Bldg SP-3 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IB16	3	1746-OB16	1	1746-NI8	1	1746-NO4I	1							
SW WRF		Headworks Bldg SP-4	Headworks Bldg SP-4 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IB16	6	1746-OB16	2	1746-NI8	4	1746-NO4I	4							
SW WRF		Sludge Transfer Pump Bldg SP-5	Digester Bldg SP-5 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IB16	4	1746-OB16	1	1746-NI8	4	1746-NO4I	1							
SW WRF		Dewatering Bldg SP-6	Dewatering Bldg SP-6 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IB16	1	1746-OB16	1	1746-NI8	1	1746-NO4I	1							
SW WRF		?	Electric South Bldg	Allen-Bradley	Other																			
SW WRF		Blower Bldg SP-8	Blower Bldg SP-8 SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IA16	6			1746-NI8	2	1746-NO4I	3					1748-OX8	2	
SW WRF		Sludge Pump Bldg SP-17	Sludge Pump Bldg SLC-5/05	Allen-Bradley	SLC	1747-L553C				1746-IA16	4	1746-OB16	1	1746-NI8	2									
SW WRF		ASR Well SP-10	ASR Well SP-10 Micrologix	Allen-Bradley	MicroLogix	1500 LRP Ser. C								1769-IF4	3	1769-OF8C	1							
SW WRF		North Lake Level SP-11	North Lake Level SP-11 Micrologix	Allen-Bradley	MicroLogix	1100 Ser. A																		
SW WRF		North Lake Reject PS SP-12	North Lake Reject PS SP-12 Micrologix	Allen-Bradley	MicroLogix	1100 Ser. A				1762-IQ16	1													
SW WRF		Reuse PS SP-13	Plant Reuse PS SP-13 Micrologix	Allen-Bradley	MicroLogix	1100 Ser. A																		
SW WRF		ABW #1	ABW SLC-5/05	Allen-Bradley	SLC	1747-L552C		1747-SN	1	1746-IA16	2	1746-OW16	1	1746-NI8	1	1746-NO4I	1							
SW WRF		North Lake PS SP-14	North Lake PS SP-14 SLC-5/05	Allen-Bradley	SLC	1747-L552C				1746-IB16	2	1746-OW16	2	1746-NI8	1									
SW WRF		Nova Filters SP-15	Nova Filters SP-15 SLC-5/05	Allen-Bradley	SLC	1747-L552C				1746-IB16	4	1746-OW16	1	1746-NI8	1	1746-NO8I	1							
SW WRF		HSPS SP-16	High Service SP (HSPS) SP-16 SLC-5/05	Allen-Bradley	SLC	1747-L552C				1746-IB16	3	1746-OA8	1	1746-NI8	1									
SW WRF		HSPS SP-16B	High Service PS (HSPS) CompactLogix 5370	Allen-Bradley	CompactLogix	1769-L18ER-BB1B																		
SW WRF		LSPS SP-1B	Low Service PS (LSPS) CompactLogix 5370	Allen-Bradley	CompactLogix	1769-L18ER-BB1B																		
SW WRF		HSPS 1 VFD	HSPS 1 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B								1762-IF2OF2	1			1762-IR4	2					

SW WRF	HSPS 2 VFD	HSPS 2 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	HSPS 3 VFD	HSPS 3 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	HSPS 4VFD	HSPS 4 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	HSPS 5 VFD	HSPS 5 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	LSPS 1 VFD	LSPS 1 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B				1762-IR4	2	
SW WRF	LSPS 2 VFD	LSPS 2 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B				1762-IR4	2	
SW WRF	LSPS 3 VFD	LSPS 3 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	LSPS 4 VFD	LSPS 4 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	LSPS 5 VFD	LSPS 5 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	LSPS 6 VFD	LSPS 6 VFD Micrologix	Allen-Bradley	MicroLogix	1100 Ser. B		1762-IF2OF2	1	1762-IR4	2	
SW WRF	South Elec. Buildnig SP-18	South Electrical Bldg SLC	Allen-Bradley	SLC	SLC-5/05						
SW WRF	Turbo Blower Bldg Blower 1	Turbo Blower No. 1 Compact Logix	Allen-Bradley	CompactLogix	CompactLogix L33ER						
SW WRF	Turbo Blower Bldg Blower 2	Turbo Blower No. 2 Compact Logix	Allen-Bradley	CompactLogix	CompactLogix L33ER						
SW WRF	Turbo Blower Bldg SP-19	New Blower Bldg CompactLogix	Allen-Bradley	CompactLogix	CompactLogix L33ER	1	1	2	1		
SW WRF	Dewatering Bldg	Dewatering Bldg Polymer Feed Pumps 5 & 6 SLC	Allen-Bradley	SLC	SLC-5/05						
SW WRF	Dewatering Bldg	Dewatering Bldge Polymer Mixing System SLC	Allen-Bradley	SLC	SLC-5/05						
SW WRF	Headwork Bldg	Grit Classifier Micrologix	Allen-Bradley	MicroLogix	1400 Ser. B						1762-OW8

Controller	**QTY**	**Percentage**
SLC	39	50.6%
CompactLogix	7	9.1%
MicroLogix	28	36.4%
Other	3	3.9%
Total	**77**	

Facility	Tag Number	Control Panel	Description	Manufacturer	Model #	Notes:
MCMRS		63rd Street PLC Panel	63rd Street MARS PLC Copper Switch	Phoenix Contact		
MCMRS		63rd Street PLC Panel	63rd Street MARS FOC Switch	Phoenix Contact		
MCMRS		63rd Street Radio Panel	63rd Street MARS FOC Switch	Phoenix Contact		
MCMRS		Rye Road PLC Panel	Rye Road MARS PLC Copper Switch	Phoenix Contact		
MCMRS		Rye Road PLC Panel	Rye Road MARS FOC Switch	Phoenix Contact		
MCMRS		Rye Road Radio Panel	Rye Road MARS FOC Switch	Phoenix Contact		
MCMRS		Spencer Parish PLC Panel	Spencer Parish MARS PLC Copper Switch	Phoenix Contact		
MCMRS		Spencer Parish PLC Panel	Spencer Parish MARS FOC Switch	Phoenix Contact		
MCMRS		Spencer Parish Radio Panel	Spencer Parish MARS FOC Switch	Phoenix Contact		
North WRF		Operations Room	Baseline Switch	3COM	2916-SFP Plus	
North WRF		Operations Room	Ethernet\Fiber Optic Switch	3COM	5500-E1 28-Port FX	
North WRF		Operations Room - DFS Encl.	Ethernet Switch	Netgear	Auto 10/100	
North WRF		Operations Room - DFS Encl.	Ethernet/Fiber Optic Switch	Phoenix Contact	FL MC 10/100 Base - T/FO G1300	
North WRF		Headworks SP-1	Ethernet/Fiber Optic Switch	Phoenix Contact	SFN 6TX-2FX	
North WRF		NWRF PLC Clarifiers SP-2	Ethernet/Fiber Optic Switch	Phoenix Contact	SFN 6TX-2FX	
North WRF		Sludge Pump # 1	Ethernet Switch	Phoenix Contact	SFNB 5TX	
North WRF		Sludge Pump # 2	Ethernet Switch	Phoenix Contact	SFNB 5TX	
North WRF		ABW # 1	Ethernet/Fiber Optic Switch	Phoenix Contact	SFN 6TX-2FX	
SE WRF		Headworks	Ethernet\Fiber Optic Switch	Phoenix Contact	LM4TX/2FX ST-E	
SE WRF		Spiragrit Control Panel	Ethernet Switch	Lanolinx	LNX-500A	
SE WRF		Belt Press Office SP-4	Ethernet\Fiber Optic Switch	Phoenix Contact	LM4TX/2FX ST-E	
SE WRF		RTO	Ethernet Switch	Netgear	FS105	
SE WRF		SE Dryer Bldg.	Ethernet Switch (10.215.24/4)			
SE WRF		SP-3	Ethernet\Fiber Optic Switch	Phoenix Contact	LM4TX/2FX ST-E	
SE WRF		SP5	Ethernet	Phoenix Contact	LM4TX/2FX	
SE WRF		SP6	Ethernet\Fiber Optic Switch	Phoenix Contact	LM4TX/2FX ST-E	
SE WRF		SP6	Ethernet\Fiber Optic Switch	Phoenix Contact	LM4TX/2FX ST-E	
SE WRF		SP6	Ethernet	Phoenix Contact	SFN8 STX	
SE WRF		GBT1	Ethernet\Fiber Optic Switch	Phoenix Contact	LM4TX/2FX ST-E	
SE WRF		GBT2	Ethernet\Fiber Optic Switch	N-Tron	508 FX2	
SE WRF		Dryer	(Panel on East wall) Ethernet to RS-232	Allen Bradley	1761-NET-ENI	Serial to IP converter
SW WRF		LSPS 3 VFD	Ethernet Switch	Phoenix Contact	SFN 5TX	
SW WRF		LSPS 4 VFD	Ethernet/Fiber Optic Switch	Phoenix Contact	SFN 4TX-1FX	
SW WRF		LSPS 5 VFD	Ethernet/Fiber Optic Switch	Phoenix Contact	SFN 4TX-1FX	
SW WRF		LSPS 6 VFD	Ethernet/Fiber Optic Switch	Phoenix Contact	SFN 4TX-1FX	
SW WRF		Operations Room	AB - DFS Digi One Module	Digi One	IAP	Serial to IP converter
SW WRF		Sludge Pump Bldg SP-17	Sludge Tank Pump Bldg SP-17 Digi One Module	Digi One	IAP	Serial to IP converter
SW WRF		Turbo Blower Bldg	Turbo Blower Bldg Digi One Module	Digi One	IAP	Serial to IP converter
SW WRF		South Electrical Bldg	South Electrical Bldg Dig One Module	Digi One	IAP	Serial to IP converter
					Percentage	
			Phoenix Contact	27	69%	
			Other	12		

Facility	Tag Number	Control Panel	Description	Manufacturer	Model #	Operating System	HMI Software	Notes:
MCMRS		63rd Street PLC Panel	63rd Street MARS OIT	Xycom	3115T	Windows 7	Citect 6.0	
MCMRS		Rye Road PLC Panel	Rye Road MARS OIT	Xycom	3115T	Windows 7	Citect 6.0	
MCMRS		Spencer Parish PLC Panel	Spencer Parish MARS OIT	Xycom	3115T	Windows 7	Citect 6.0	
North WRF		Clarifiers Bldg SP-2	Citect Touch Screen Workstation	Proface	PS4700-V1-1P-AN-A-2G-XP-SHD-DVD	Windows 7	Citect 7.5	
North WRF		Dewatering Bldg	Citect Touchscreen SP-3	Proface	PS4700-V1-1P-AN-A-2G-W732-SSD-DVD	Windows 7	Citect 7.5	
North WRF		Electrical Bldg	Citect Touchscreen SP-4	Proface	PS4700-V1-1P-AN-A-2G-XP-SHD-DVD	windows 7	Citect 7.5	
North WRF		Rye Mars Booster Station	Citect Touchscreen Rye				Citect	
North WRF		Spencer Mars	Citect Touchscreen Spencer				Citect	
SE WRF		RTO	Allen Bradley Panelview 1000	AB	Panel View 1000			
SE WRF		Dryer (East Wall)	East Well	AB	Panel View Plus 400			
SE WRF		Bio-Solids Operations Room	New RTO Panel View	AB	Panel View Plus 1250			
SE WRF		SP-1	View only	Proface	PS4700-1S-N270	Windows 7	Citect 7.5	
SE WRF		GBT1	View only	Proface	PS4700-1S-N270	Windows 7	Citect 7.5	
SE WRF		Poly Room	Poly HMI Panel	Total Control Products	QPKSTDN000-A			
SW WRF		Admin Bldg Operations Room	BCPC056169.bcc.ad.mymanatee.org Citect Primary SCADA Server	HP		Windows 7	Citect 7.5	
SW WRF		Admin Bldg Operations Room	BCPC056167.bcc.ad.mymanatee.org Citect Backup SCADA Server	HP		Windows 7	Citect 7.5	
SW WRF		Admin Bldg Operations Room	BCPC056245.bcc.ad.mymanatee.org Citect Workstation	HP		Windows 7	Citect 7.5	
SW WRF		Electrical Bldg SP-1	Electrical Bldg Citect Touch Screen Workstation	Proface	PS4700-VI-IP-AN-A-2G-W732-SSD-DV	Windows 7	Citect 7.5	
SW WRF		Headworks Bldg SP-4	Headworks Bldg Citect Touch Screen Workstation	Proface		Windows 7	Citect 7.5	
SW WRF		Sludge Transfer Bldg SP-5	Digester Bldg Citect Touch Screen Workstation	Proface		Windows 7	Citect 7.5	
SW WRF		Dewatering Bldg Office	BCPC013632.bcc.ad.mymanatee.org Citect Workstation	HP		Windows 7	Citect 7.5	
SW WRF		Blower Buidling SP-8	Blower Bldg Total Control QuickPanel	Total Control	QuickPanel	N/A		
SW WRF		ABW #1	ABW #1 OPI PanelView 600	Allen-Bradley	PanelView 600	N/A	PanelBuilder 32 or FactoryTalkME	
SW WRF		North Lake PS SP-14	North Lake PS OPI Maple System HMI	Maple Systems	HMI5070TH	NA	NA	
SW WRF		High Service PS SP-16	High Service Bldg Citect Touch Screen Workstation	Proface		Windows 7	Citect 7.5	
SW WRF		Sludge Pump Bldg SP-17	Sludge Tank Pump Bldg SP-17 Citect Touch Screen Workstation	Proface		Windows 7	Citect 7.5	
SW WRF		South Electrical Bldg SP-18	South Electrical Bldg Citect Touch Screen Workstation	Proface		Windows 7	Citect 7.5	
SW WRF		Turbo Blower Bldg SP-19	New Blower Bldg Touch Screen Workstation	Allen-Bradley	PanelView 1000			
SW WRF		Turbo Blower Bldg	New Turbo Blower No. 1 PanelView 600	Allen-Bradley	PanelView 600	N/A	PanelBuilder 32 or FactoryTalkME	
SW WRF		Turbo Blower Bldg	New Turbo Blower No. 2 PanelView 600	Allen-Bradley	PanelView 600	N/A	PanelBuilder 32 or FactoryTalkME	
SW WRF		Dewatering Bldg	Dewatering Bldg Polymer Feed Pumps 5 & 6 PanelView 600	Allen-Bradley	PanelView 600	N/A	PanelBuilder 32 or FactoryTalkME	
SW WRF		Dewatering Bldg	Dewatering Bldge Polymer Mixing System PanelView 600	Allen-Bradley	PanelView 600	N/A	PanelBuilder 32 or FactoryTalkME	

Facility	Tag Number	Location	Description	Manufacturer	Model #	Comm	Notes:
SW WRF		Sludge Tank Pump Bldg	Sludge Tank Power Monitoring 1	Square D	PM 800	DeviceNet	
SW WRF		Sludge Tank Pump Bldg	Sludge Tank Power Monitoring 2	Square D	PM 800	DeviceNet	
SW WRF		Turbo Blower Bldg	Turbo Blower Bldg Power Monitoring 1	Square D	PM 800	DeviceNet	
SW WRF		Turbo Blower Bldg	Turbo Blower Bldg Power Monitoring 2	Square D	PM 800	DeviceNet	
SW WRF		South Electrical Bldg	South Electrical Bldg Power Monitoring 1	Square D	PM 800	DeviceNet	
SW WRF		South Electrical Bldg	South Electrical Bldg Power Monitoring 2	Square D	PM 800	DeviceNet	

Facility	Tag Number	Control Panel	Description	Manufacturer	Model #	Frequency
MCMRS		63rd Street Radio Panel	63rd Street Ethernet Radio	MDS	iNET 900	
MCMRS		Rye Road Radio Panel	Rye Road Ethernet Radio	MDS	iNET 900	
MCMRS		Spencer Parish Radio Panel	Spencer Parish Ethernet Radio	MDS	iNET 900	
SW WRF		Chemical Bldg SP-2	Chemical Bldg Ethernet Radio	Engenius	ENH500	
SW WRF		North Lake Level SP-11	North Lake Level Ethernet Radio	Engenius	ENH500	
SW WRF		Reuse PS SP-13	Plant Reuse PS Ethernet Radio	Engenius	ENH500	
SW WRF		ABW #1 Bridge	ABW #1 Bridge Ethernet Radio	Engenius	ENH500	
SW WRF		Reject Lake PS SP-12	North Lake Reject PS Ethernet Radio	Engenius	ENH500	

Facility	Tag Number	Control Panel / Location	Description	Manufacturer	Model #	Notes:
MCMRS		63rd Street PLC Panel	UPS	Eaton	5S 700	
MCMRS		63rd Street Radio Panel	UPS	Tripp-Lite		
MCMRS		Rye Road PLC Panel	UPS	Eaton	5S 700	
MCMRS		Rye Road Radio Panel	UPS	Tripp-Lite		
MCMRS		Spencer Parish PLC Panel	UPS	APC	5S 700	
MCMRS		Spencer Parish Radio Panel	UPS	Tripp-Lite		
North WRF		Admin. Bldg		KW Controls	510028104	
North WRF		Admin Bldg.	under console	Eaton	PW9120 2000	
North WRF		Dana's Office		APC	Backups 750	
North WRF		Operators' Console	under console	APC	Smart-UPS750	
North WRF		Electrical Bldg.		APC	Smart-UPS750	
North WRF		Lake Gravity Filters SP-9		APC	Smart-UPS750	
North WRF		Clarifier Bldg. SP-2		APC	Smart-UPS750	
North WRF		Dewatering Bldg.		APC	Smart-UPS750	
SE WRF		SP-1		Tripp-Lite	OMNIVS1500XL	
SE WRF		SP-2	Headworks MCC	Tripp-Lite	OMNIVS1500XL	
SE WRF		SP-3		Tripp-Lite	OMNIVS1500XL	
SE WRF		SP-4	Belt Press Bldg. (Office)	Tripp-Lite	OMNIVS1500XL	
SE WRF		SP-5	Nova Filters	APC	1500	
SE WRF		SP-6	HSPS	APC	RT 1500	
SE WRF		GBT1	GBT	Tripp-Lite	OMNIVS1500XL	
SE WRF		GBT2	GBT2	Liebert	GXT3	
SE WRF		BCPC013441	Dryer Bldg. (Upstairs PC)	APC	Backup-UPS 750	
SE WRF		Dryer Office Network		APC	Smart UPS 750	
SE WRF		Dryer Office Network BCPC58375		APC	Backup-UPS 1500	
SE WRF		Dryer Office Network BCPC58372		APC	Backup-UPS 1500	
SE WRF		Dryer Office Network Switch Gear		Eaton	9PX6000	
SE WRF		Dryer Office Network Switch Gear		Eaton	9PX6000 EBM	
SE WRF		Dryer Office Network Switch Gear		Eaton	9PX6000 PPDM	
SE WRF		Dryer Office BCPC15004		APC	Backup-UPS 750	
SW WRF		63rd ave		APC	Pro 700	
SW WRF		Chlorine Bldg	PH and Chlorine meters	APC	Pro 700	
SW WRF		RU-SW	Admin Electrical room	APC	Pro 700	

SW WRF	SP-1	Electric Building	APC	Pro 700
SW WRF	SP-2	Chemical Building	APC	Pro 700
SW WRF	SP-3	DAF building	APC	Pro 700
SW WRF	SP-4	Head works building	APC	Pro 700
SW WRF	SP-5	Sludge Transfer Building	APC	Pro 700
SW WRF	SP-6	Dewatering	APC	Pro 700
SW WRF	SP-17	Sludge Tank Pump Bldg	Eaton	9130
SW WRF	SP-8	Blower building	APC	Pro 1500
SW WRF	SP-15	Nova Lake Filter	APC	Smart1500
SW WRF	SP-16	High Service	APC	Smart UPS 1500
SW WRF	NA	norht wall of headworks	APC	LS-500
SW WRF	ABW panel	south end of ABW 1	APC	Pro 700
SW WRF	ABW panel	on bridge of ABW 1	APC	Pro 700
SW WRF	NA	Dewatering Office PC	APC	Pro 700
SW WRF	Admin Console	Ops north pc		Backup UPS 750
SW WRF	Admin Console	Ops middle pc	APC	SMT2200
SW WRF	Admin Console	Ops south pc		
SW WRF	Office	Jeff koch office	APC	Pro 700
SW WRF	Office	scada office pc	APC	Pro 700
SW WRF	Office	scada office plc board	APC	Pro 700
SW WRF	Office	Ops room lab	APC	SMT2200
SW WRF	SP-18	South Electrical Bldg	Eaton	9130
SW WRF	SP-19	Turbo Blower Bldg SP-19	Cyber Power	625VA
SW WRF	P.P. 25	Turbo Blower Bldg patch p	Eaton	35 750

Eaton	**9**
APC	**29**
Tripp-Lite	**8**
Other	**11**

Appendix E

SLCMIGRATION

Migration Solutions

SLC 500 to CompactLogix 5380 and 5069 Compact I/O

Overview

In today's economy it is necessary to have migration solutions that help you to achieve increased productivity and lessen your risk of maintaining your legacy equipment. You need to work with a supplier that has the product, service, and industry knowledge to partner with you on an upgrade strategy that will help you maximize your competitive advantage.

Rockwell Automation® and its partners will work with you to outline a plan that fits your application needs and long-term goals. We can help you migrate all at once or in phases, at the pace that is comfortable for you and fits your budget.

With your goals in mind, Rockwell Automation has developed a migration strategy that will allow you to quickly and easily migrate from SLC-based control to Logix-based control and Integrated Architecture, while maintaining the existing field wiring. This approach will:

- Lower conversion time and labor costs
- Reduce risk by preserving existing field wiring connections
- Lower engineering costs
- Minimize production downtime

Simplifying SLC™ Migrations

- Minimizes risk and reduces labor time
  - convert I/O without disturbing field wiring connections
  - code conversion tools reduce time to rewrite controller program
- Improves migration and planning using Integrated Architecture Builder tool
- Supports various network topologies with the proven technology of EtherNet/IP

New Control System Benefits

- Increased flexibility with new open architecture
- Reduced development time and costs through re-use of engineering practices
- Maximized returns on existing assets through improved control and monitoring
- Increased access to plant and production information
- One programming environment for discrete, motion, process, drive, batch, and safety control

Choosing a Partner for your Project

When planning your migration, there are several resources available to help you develop a proactive lifecycle plan:

Migration Services from Rockwell Automation

Reduce lifecycle risks before, during and after the migration process with migration services that are tailored to your specific needs. Our modernization services and support are available to help you realize the benefits of CompactLogix System and a modern control architecture. Our factory-trained Field Service Professionals are experienced and prepared to provide onsite assessments, migration planning services, start-up and commissioning of your modernized control architecture. From project management to start-up, we will help define and implement an effective modernization strategy for your facility that goes beyond simply addressing your legacy equipment to truly optimizing your operation.

Recognized System Integrator or Solution Provider

Our **PartnerNetwork**™ provides an integrated team of engineering specialists and suppliers that are leaders in the automation and manufacturing industry who have experience delivering products or services that are designed to work with Rockwell Automation® solutions.

Do It Yourself

If you prefer to migrate from SLC-based control system and 1746 I/O to CompactLogix system without assistance, Rockwell Automation provides a number of tools free of charge to help you plan and migrate with as little disruption as possible.

Tools to Plan and Execute your Migration

Rockwell Automation provides migration tools for hardware selection, code conversion and hardware conversion that practically eliminate the need to modify any field device wiring. All tools are available regardless of who performs the migration: Rockwell Automation, System Integrator, or Do It Yourself

Product Lifecycle Status

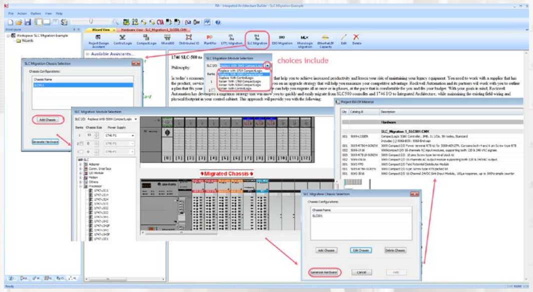
The online Product Lifecycle Status tool can help you determine the lifecycle of your existing equipment and identify the most contemporary Rockwell Automation products, bringing you advancements in performance, flexibility and security. Having this knowledge makes it easier to plan and manage the transition from legacy or obsolete equipment to leading-edge technologies.

Installed Base Evaluation

An Installed Base Evaluation provides a thorough analysis of your critical plant assets and their condition. This site-delivered service provides detailed reports by site, area, line, machine and panel.

Integrated Architecture Builder

The Integrated Architecture Builder (IAB) is a graphical, user-friendly software tool that allows you to automatically define and configure a contemporary CompactLogix-based architecture including a detailed bill of materials based on your current SLC-based control system.



Popular Configuration Drawings for CompactLogix 5380

Use these system configuration the following system drawings as examples of how to build a scalable integrated architecture for your industrial application and understand the basic performance, capacity, and configurations the controllers can use.

ProposalWorks Proposal Builder

This tool helps you create bill of materials, RFQs, and proposals for your automation projects directly from your computer. The tool has 1,500 wizards and an easy-to-use search capability to find the right products to meet your application requirements.

RSLogix 5000 or Studio 5000 Project Migrator

The Project Migrator tool allows you to save time and engineering resources when converting your SLC 500 application code. After exporting your RSLogix 500 project file, you can use the using the embedded conversion utilities to import your code into RSLogix 5000 or Studio 5000 software.

Network Adaptor Module

The 1747-AENTR Ethernet adaptor module enables communication and data transfer between a CompactLogix controller and remote 1746 I/O via ethernet communications. It can be used to upgrade an existing SLC™ system to a CompactLogix system. The advantages of using the 1747-AENTR module in a phased modernization include allowing the existing Remote I/O network to remain in place and allows the new application to be tested before switch over and to switch back to the old application in minutes.

Controller and I/O Wiring Conversion Systems (Coming in 2019)

I/O Conversion Modules provide a fast and efficient method for converting from legacy I/O to contemporary I/O. The I/O conversion is accomplished without removing any field wires from the existing 1746 Swing Arm, virtually eliminating the risk of wiring errors. The existing 1746 Swing Arms fit directly onto the edge connector of the Conversion Modules.

Getting Started

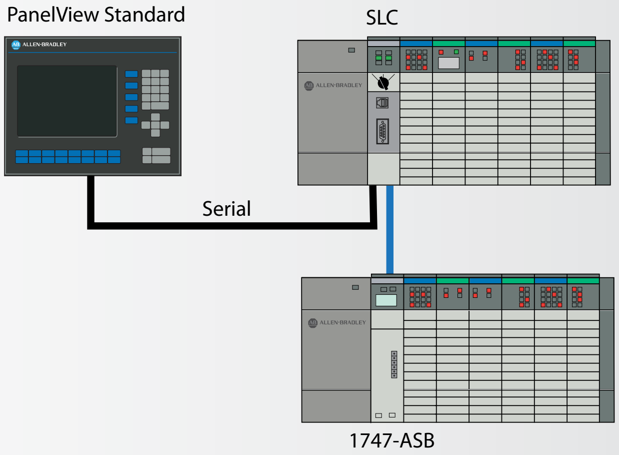
With industry knowledge and worldwide services support, Rockwell Automation will partner with you to ensure a smooth transition from your SLC controllers to the flexible, scalable Integrated Architecture.

STEP 1

Document your Current System Layout and Define your Future System Requirements

Begin planning your migration by documenting your existing system as a reference point. This will enable you to consider the available options and find a solution that best meets your existing and future requirements.

Tools: Installed Base Evaluation

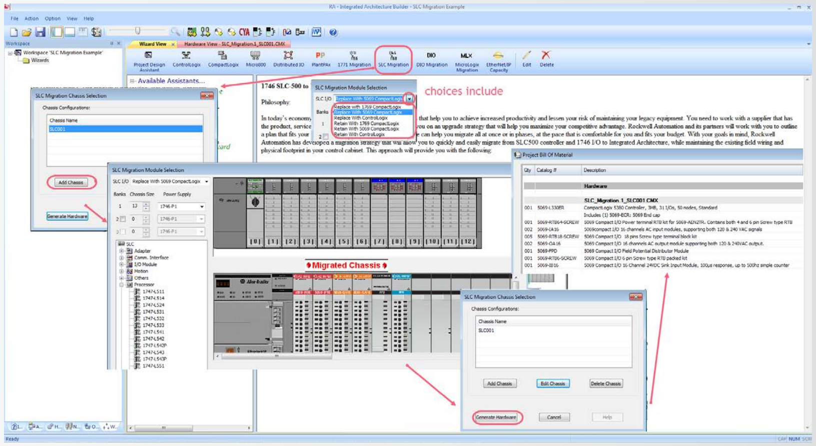


STEP 2

Plan your Migration

Once you have planned your overall migration approach, let Integrated Architecture Builder (IAB) help plan the details. The SLC migration wizard embedded in IAB will step you through the system configuration process, allowing to you make the decisions on which components you prefer to keep and reuse and which components you prefer to replace. If you choose to reuse the SLC I/O, IAB will verify module support and power supply loading and help you layout the new EtherNet/IP network.

Tools: Integrated Architecture Builder (IAB), Popular Configuration Drawings



1746 SLC-500 to

Philosophy:

In today's economy ... that help you to achieve increased productivity and lessen your risk of maintaining your legacy equipment. You need to work with a supplier that has the product, service ... you on an upgrade strategy that will help you maximize your competitive advantage. Rockwell Automation and its partners will work with you to outline a plan that fits your ... can help you migrate all at once or in phases, at the pace that is comfortable for you and fits your budget. With your goals in mind, Rockwell Automation has developed a migration strategy that will allow you to quickly and easily migrate from SLC500 controller and 1746 I/O to Integrated Architecture, while maintaining the existing field wiring and physical footprint in your control cabinet. This approach will provide you with the following:

SLC Migration Module Selection

SLC I/O: Replace With 5069 CompactLogix

- Replace with 1769 CompactLogix
- Replace With 5069 CompactLogix
- Replace With ControlLogix
- Retain With 1769 CompactLogix
- Retain With 5069 CompactLogix
- Retain With ControlLogix

Banks	Chassis Size	Power Supply
1	13	1746-P1
2 □	0	1746-P1
3 □	0	1746-P1

SLC: Adapter, Comm. Interface, I/O Module, Motion, Others, Processor: 1747-L511, 1747-L514, 1747-L524, 1747-L531, 1747-L532, 1747-L533, 1747-L541, 1747-L542, 1747-L542P, 1747-L543, 1747-L543P, 1747-L551

SLC Migration Chassis Selection

Chassis Configurations:

Chassis Name: SLC001

Add Chassis | Edit Chassis | Delete Chassis

Generate Hardware | Cancel | Help

Project Bill Of Material

Qty	Catalog #	Description
		Hardware
		SLC_Migration.1_SLC001.CMX
001	5069-L330ER	CompactLogix 5380 Controller, 3MB, 31 I/Os, 50 nodes, Standard
		Includes (1) 5069-ECR: 5069 End cap
001	5069-RTB64-SCREW	5069 Compact I/O Power terminal RTB kit for 5069-AEN2TR. Contains both 4 and 6 pin Screw type RTB
002	5069-IA16	5069compact I/O 16 channels AC input modules, supporting both 120 & 240 VAC signals
005	5069-RTB18-SCREW	5069 Compact I/O 18 pins Screw type terminal block kit
002	5069-OA16	5069 Compact I/O 16 channels AC output module supporting both 120 & 240VAC output.
001	5069-FPD	5069 Compact I/O Field Potential Distributor Module
001	5069-RTB6-SCREW	5069 Compact I/O 6 pin Screw type RTB packed kit
001	5069-IB16	5069 Compact I/O 16 Channel 24VDC Sink Input Module, 100µs response, up to 500hz simple counter

Moving Forward: Executing Your Project

Whether you choose to migrate all at once or in phases, we have the tools and experience to guide you through the transition. Our approach to modular automation coupled with backward compatibility allows you to maintain productivity as you upgrade portions of your automation system. Migrate in phases at a pace that's right for you.

PHASE 1

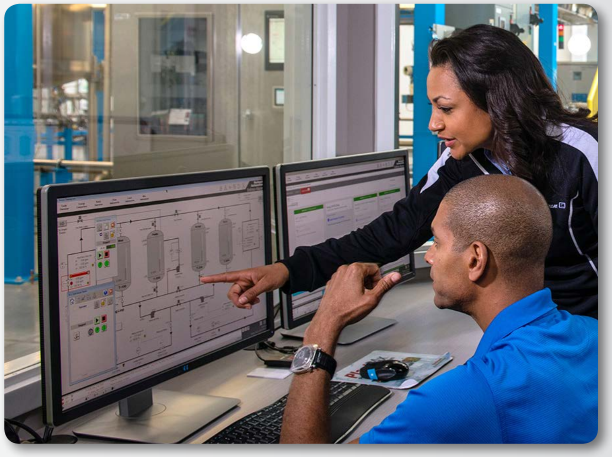
Application Code Conversion

Save time and engineering resources when converting your SLC 500 application code by using the embedded conversion utilities in either RSLogix 5000 or Studio 5000 software. And, converting your PanelView Standard project to PanelView Plus is as simple as importing the existing project into FactoryTalk View Studio.

Tools: RSLogix 5000 and Studio 5000 software, FactoryTalk View Studio Software

Benefits (application code):
- Convert 80-100% of code using automated code conversion
- Take advantage of powerful constructs and features that you can leverage to improve the application

Benefits (HMI application):
- 80% of the time no further modification is required for HMI application
- Utility generates conversion log identifying features not supported by new hardware selected
- Option to take advantage of enhanced features and graphics
- Better integration with controllers



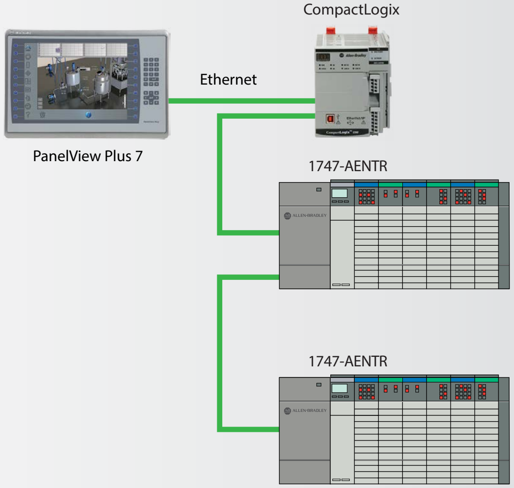
PHASE 2

Replace the SLC Processor and/or Adaptor Modules

Mount and wire the CompactLogix™ system and replace the SLC first slot modules (SLC processor or communication adaptor module) with the SLC Ethernet adaptor (1747-AENTR). Utilizing this module allows you to retain your existing SLC I/O and preserve existing field wiring, while allowing your SLC I/O chassis to be controlled from your new CompactLogix controller. This approach simplifies the migrations process, reduces risks associated with rewiring the I/O, and saves valuable time allowing you to quickly get your application into production.

Tools: 1747-AENTR Ethernet adaptor, CompactLogix User Manual

Benefits:
- Maintain existing field wiring
- Minimize commissioning time and effort
- Ability to return to SLC control, if needed



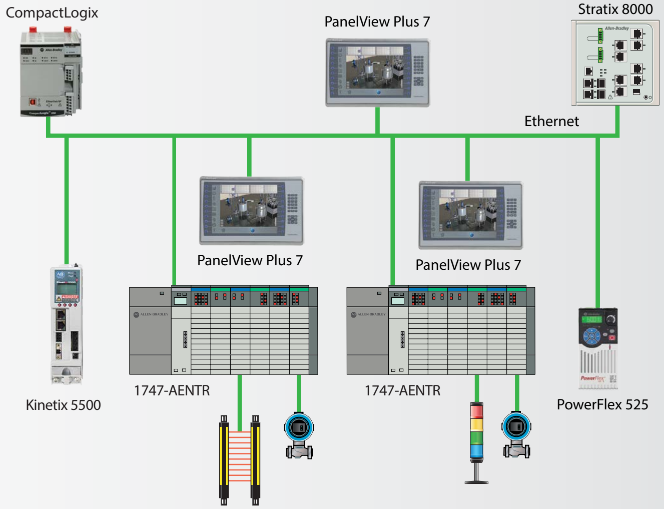
Moving Forward: Executing Your Project

PHASE 3

Replace other System Components

Because Rockwell Automation is a comprehensive supplier, we can help with other products and services. If your control system has legacy or competitive variable speed drives, motion control, sensors or motor control centers we can discuss how we can help migrate those products as well. But it doesn't stop there. We have a worldwide service group that can do the migration work, assist and train operators or provide the maintenance services once it's complete. We can also review your network needs and review asset management for your entire facility.

Tools: Popular Configuration Drawings for CompactLogix 5380

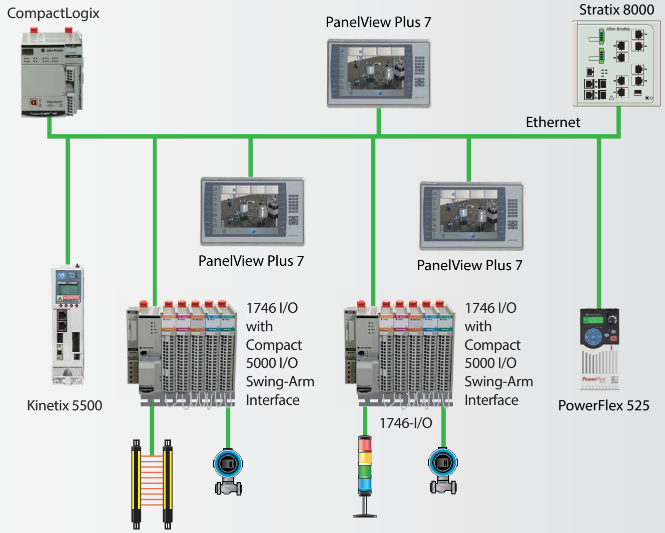


PHASE 4

I/O Replacement (FUTURE STATE)

In the final phase of the migration process, the I/O Wiring Conversion System is used to replace the 1746 I/O with the CompactLogix I/O. Because I/O replacement represents a large investment, we provide an approach that's right for your schedule and budget. The I/O Wiring Conversion System provides a method to connect the existing 1746 I/O wiring to the 5069 I/O modules without disturbing the field wiring connections, dramatically reducing labor time and eliminating the potential for downtime that could result from wiring mistakes during the migration. Planning your migration is more manageable as I/O can be swapped one rack at a time or all at once based on your schedule and budget. In either case, you can run both new and old I/O networks simultaneously. Additionally, I/O cross reference documentation assures correctness and provides historical back-up for future troubleshooting or diagnostics.

Tools: I/O Wiring Conversion System (Coming in 2019), ProposalWorks Selection Software



Complete Conversion Services

In any phase of your conversion project, Rockwell Automation can provide you with technical, industry and project management expertise to help make a migration project easier. We will help you design a plan to account for your short- and long-term goals. You will be assigned a primary engineer who will be responsible for coordinating and scheduling implementation activities and resources, and who will also be the primary communications contact.

On-site Assessment

Using standardized checklists and processes, a job site visit will be perfromed to confirm the project scope, validate risks, review testing and acceptance criteria, and gather the required information and software to convert existing screens and configurations.

You will receive:

- Completed risk assessment form
- Bill of materials
- Conversion acceptance criteria
- Project schedule and timeline
- Required information sent to conversion engineer team

To request a migration quote, please contact your local authorized Allen-Bradley distributor or Rockwell Automation sales office.

If you need additional help, Rockwell Automation can provide:
Application level phone support during the start-up and debugging phase of the project

Consultation on system re-engineering, operator interface, architecture and communication strategies, training, and on-site start-up is available through our local Rockwell Automation office.

Application Conversion Engineering Services

Using custom-developed proprietary software applications designed to convert existing configurations, our engineers will complete and test the screen conversion process and any required PLC code changes necessary.

We can help you:

- Decrease turn-around time
- Save money
- Minimize errors that can occur in a manual conversion

Deliverables include:

- The existing console and configurations converted to the appropriate Logix controller and FactoryTalk products
- Conversion of the documentation database
- Correct and convert any instruction and/or addressing errors to the new processor family
- Multilingual database conversion offered

Start-up and Acceptance

Prior to installation, comprehensive functional testing will be performed including pre-loading of all applicable software and firmware. Once installation is complete, our engineer, working closely with your plant staff, will conduct an operational compliance review. Comprehensive system documentation will be provided upon project acceptance.

Deliverables include:

- Pre-operational checklist
- Operational test performed and validated by customer
- Customer acceptance
- Necessary documentation, including product sheets and software files

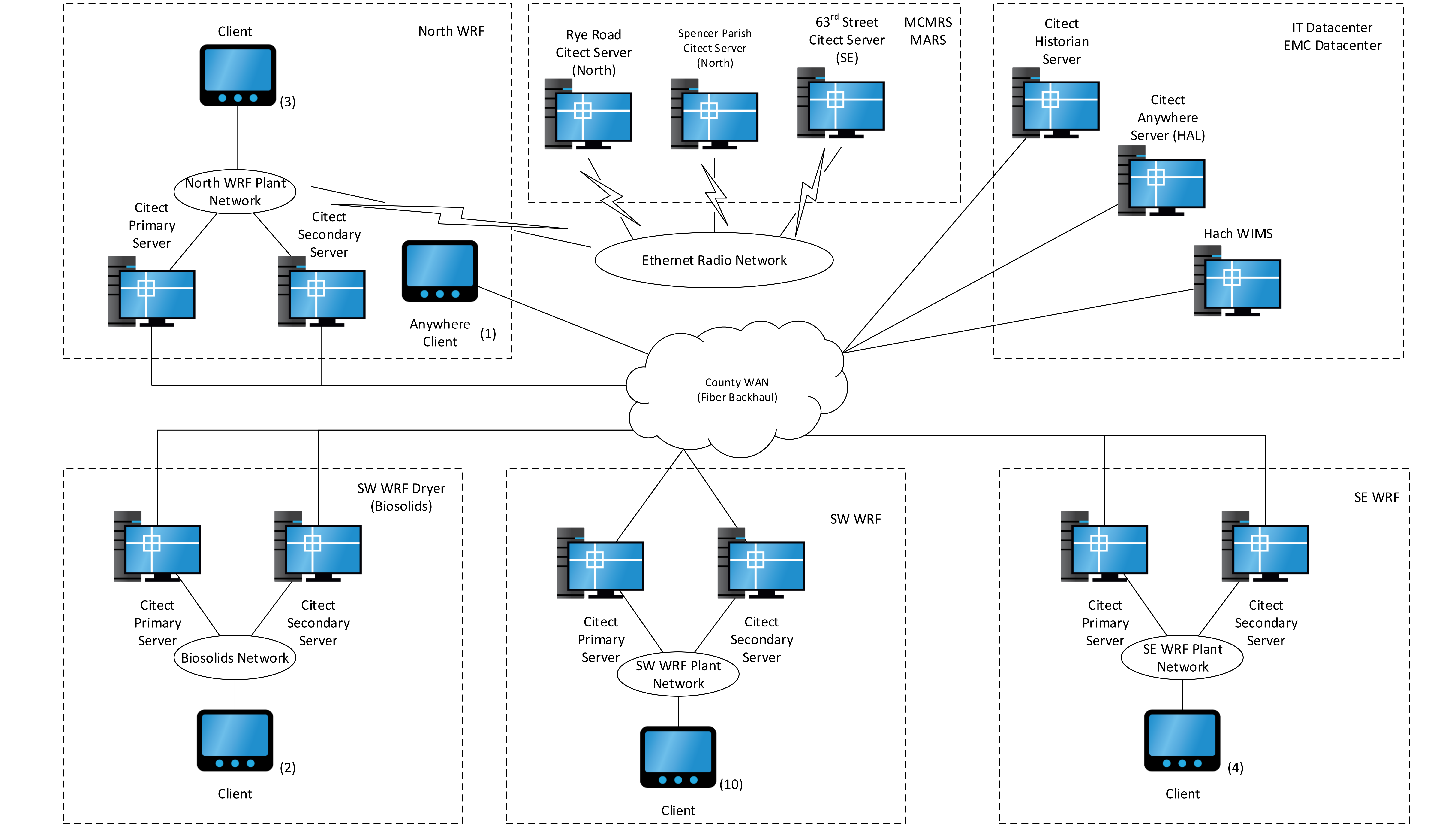
www.rockwellautomation.com

Power, Control and Information Solutions Headquarters
Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication MIGRAT-PP004B-EN-E – February 2019
Supersedes MIGRAT-PP004A-EN-E – September 2011

Appendix F

HMI TOPOLOGY



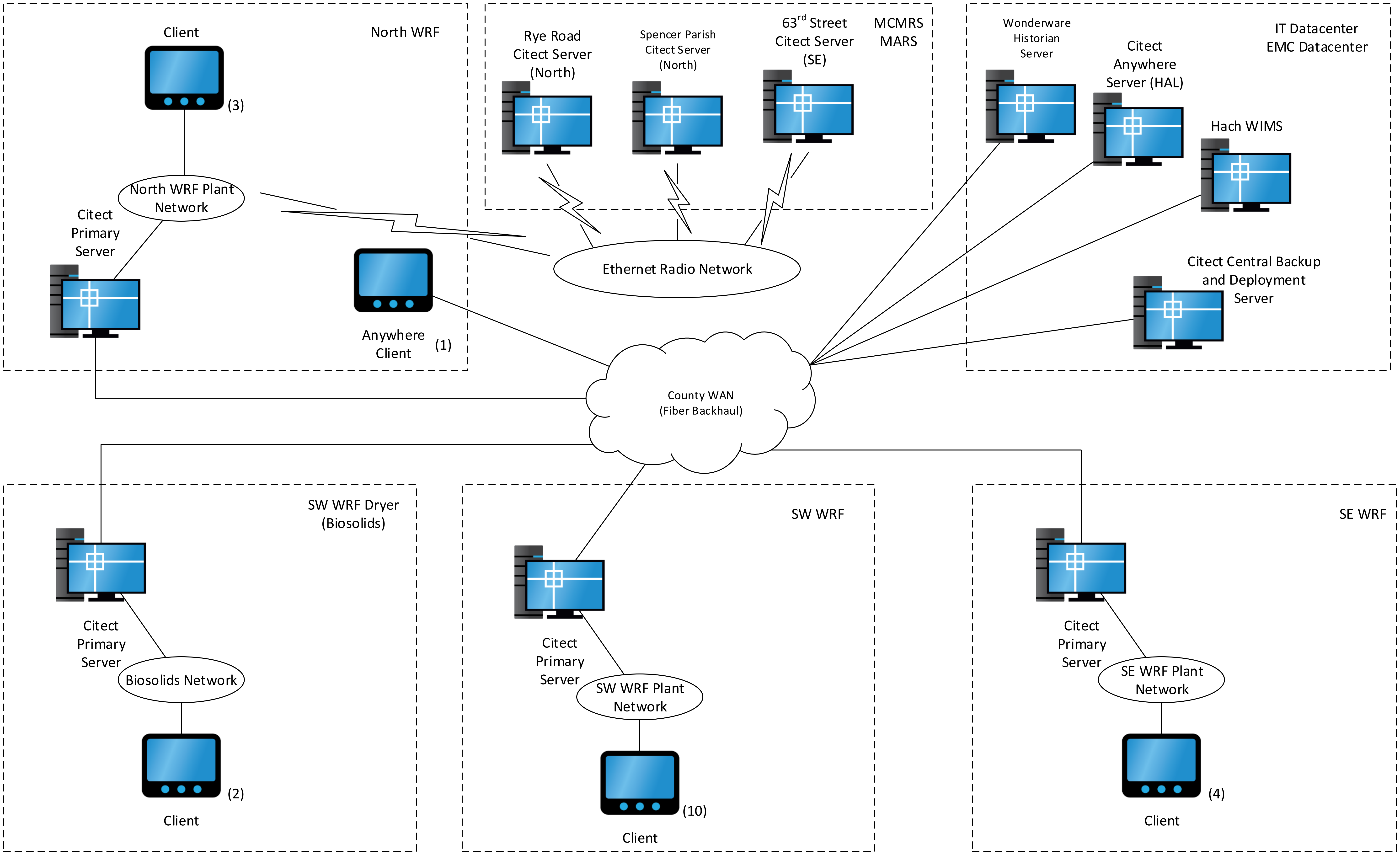
MANATEE COUNTY UTILITIES
4410 66TH ST W, BRADENTON, FL

SCADA SOFTWARE ARCHITECTURE OVERVIEW

INSTRUMENTATION & CONTROL

DRAFT

	DATE	DWG NO	REV
	3/20/2019	I-XX	0
SCALE: NTS		SHEET 1 OF 2	



INSTRUMENTATION & CONTROL	MANATEE COUNTY UTILITIES 4410 66TH ST W, BRADENTON, FL		
	CENTRAL BACKUP SERVER ARCHITECTURE		
	DATE 3/20/2019	DWG NO I-XX	REV 0
DRAFT	SCALE: NTS	SHEET 2 OF 2	

Appendix G
SCADA ARCH

MANATEE COUNTY
SCADA SYSTEM DOCUMENTATION
9/12/2017

DRAWING LISTING

DRAWING NUMBER	SHEET DESCRIPTION	REVISON DATE
	SOUTHWEST WRF SCADA SYSTEM ARCHITECTURE DRAWING	9/1/2016
	SOUTHWEST WRF TCP/IP ADDRESS LISTING	9/1/2016
	SOUTHWEST WRF PLC LISTING	9/1/2016
	SOUTHWEST WRF MISC. LISTING	9/1/2016
	SOUTHWEST PLC MESSAGE LISTING	9/1/2016
	SOUTWEST PLC DEVICE NET MESSAGES	9/1/2016
	SOUTHEAST WRF SCADA SYSTEM ARCHITECTURE DRAWINGS	9/12/2017
	SOUTHEAST WRF TCP/IP ADDRESS LISTING	9/1/2016
	SOUTHEAST WRF PLC LISTING	9/1/2016
	SOUTHEAST WRF MISC. LISTING	9/1/2016
	SOUTHEAST WRF PLC MESSAGE LISTING	9/1/2016
	SOUTHEAST WRF PLC DEVICENET MESSAGE	9/1/2016
	NORTH WRF SCADA SYSTEM ARCHITECTURE DRAWING	9/1/2016
	NORTH WRF TCP/IP ADDRESS AND PLC LISTING	9/1/2016
	NORTH WRF MISC. LISTING	9/1/2016
	NORTH WRF PLC MESSAGE LISTING	9/1/2016
	MCMRS SCADA SYSTEM ARCHITECTURE DRAWING	9/1/2016
	MCMRS TCP/IP ADDRESS AND PLC LISTING	9/1/2016
	MCMRS MISC. LISTING	9/1/2016
	SOUTHWEST WRF DRYER SCADA SYSTEM ARCHITECTURE DRAWING	9/1/2016

REV	DATE	BY	DESCRIPTION

DESIGNED
YOCUM
DRAWN
YOCUM
CHECKED
YOCUM
DATE
SETP 2017

carollo®

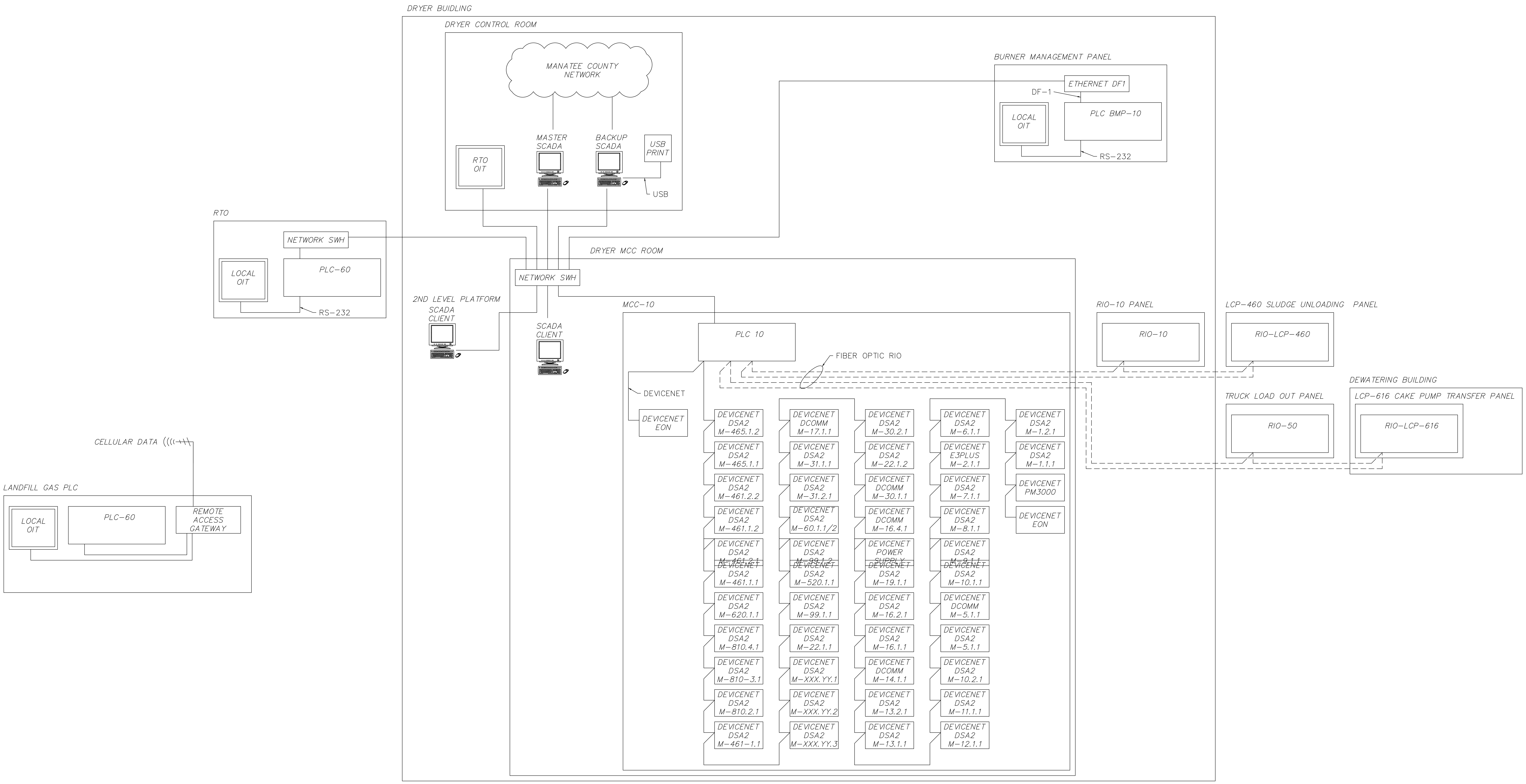
Manatee County
FLORIDA

MANATEE COUNTY
WRF SCADA EVALUATION

MANATEE COUNTY WRF
SCADA SYSTEM DOCUMENTATION

VERIFY SCALES
BAR IS ONE INCH ON ORIGINAL DRAWING
0 1"
IF NOT ONE INCH ON THIS SHEET, ADJUST SCALES ACCORDINGLY

JOB NO.
10096H.00
DRAWING NO.



REV	DATE	BY	DESCRIPTION

DESIGNED
YOCUM
DRAWN
YOCUM
CHECKED
YOCUM
DATE
SEPTEMBER 2016

carollo®

Manatee County
FLORIDA

MANATEE COUNTY

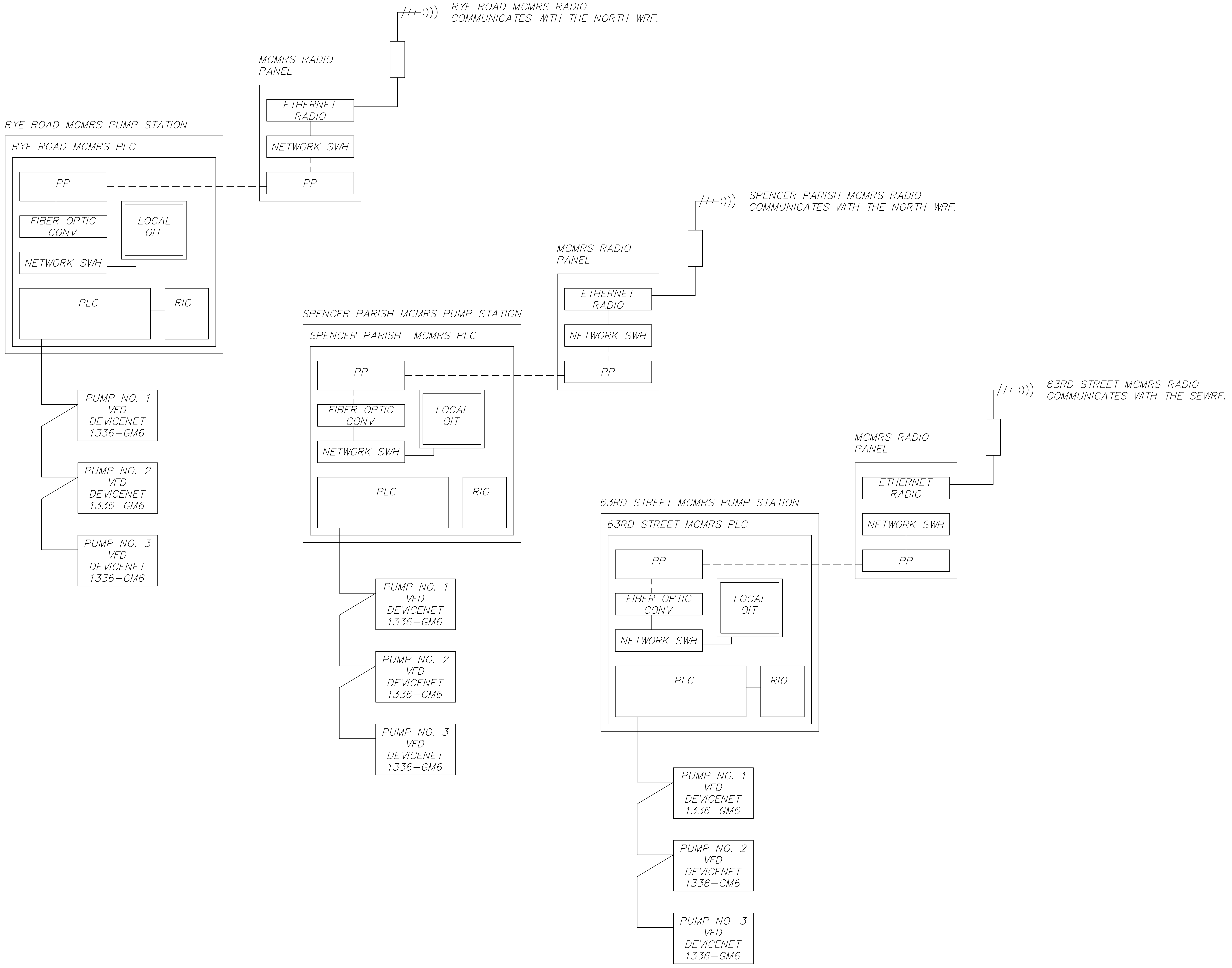
WRF SCADA EVALUATION

SOUTHWEST WRF DRYER
SCADA SYSTEM ARCHITECTURE DRAWING

VERIFY SCALES
BAR IS ONE INCH ON ORIGINAL DRAWING
0 1"
IF NOT ONE INCH ON THIS SHEET, ADJUST SCALES ACCORDINGLY

JOB NO.
10096H.00

DRAWING NO.


RYE ROAD MCMRS RADIO
COMMUNICATES WITH THE NORTH WRF.
MCMRS RADIO PANEL
ETHERNET RADIO
NETWORK SWH
PP
RYE ROAD MCMRS PUMP STATION
RYE ROAD MCMRS PLC
PP
FIBER OPTIC CONV
LOCAL OIT
NETWORK SWH
PLC
RIO
PUMP NO. 1 VFD DEVICENET 1336-GM6
PUMP NO. 2 VFD DEVICENET 1336-GM6
PUMP NO. 3 VFD DEVICENET 1336-GM6
SPENCER PARISH MCMRS RADIO
COMMUNICATES WITH THE NORTH WRF.
MCMRS RADIO PANEL
ETHERNET RADIO
NETWORK SWH
PP
SPENCER PARISH MCMRS PUMP STATION
SPENCER PARISH MCMRS PLC
PP
FIBER OPTIC CONV
LOCAL OIT
NETWORK SWH
PLC
RIO
PUMP NO. 1 VFD DEVICENET 1336-GM6
PUMP NO. 2 VFD DEVICENET 1336-GM6
PUMP NO. 3 VFD DEVICENET 1336-GM6
63RD STREET MCMRS RADIO
COMMUNICATES WITH THE SEWRF.
MCMRS RADIO PANEL
ETHERNET RADIO
NETWORK SWH
PP
63RD STREET MCMRS PUMP STATION
63RD STREET MCMRS PLC
PP
FIBER OPTIC CONV
LOCAL OIT
NETWORK SWH
PLC
RIO
PUMP NO. 1 VFD DEVICENET 1336-GM6
PUMP NO. 2 VFD DEVICENET 1336-GM6
PUMP NO. 3 VFD DEVICENET 1336-GM6

REV	DATE	BY	DESCRIPTION

DESIGNED
YOCUM
DRAWN
YOCUM
CHECKED
YOCUM
DATE
SEPTEMBER 2016

carollo®

Manatee County
FLORIDA

MANATEE COUNTY

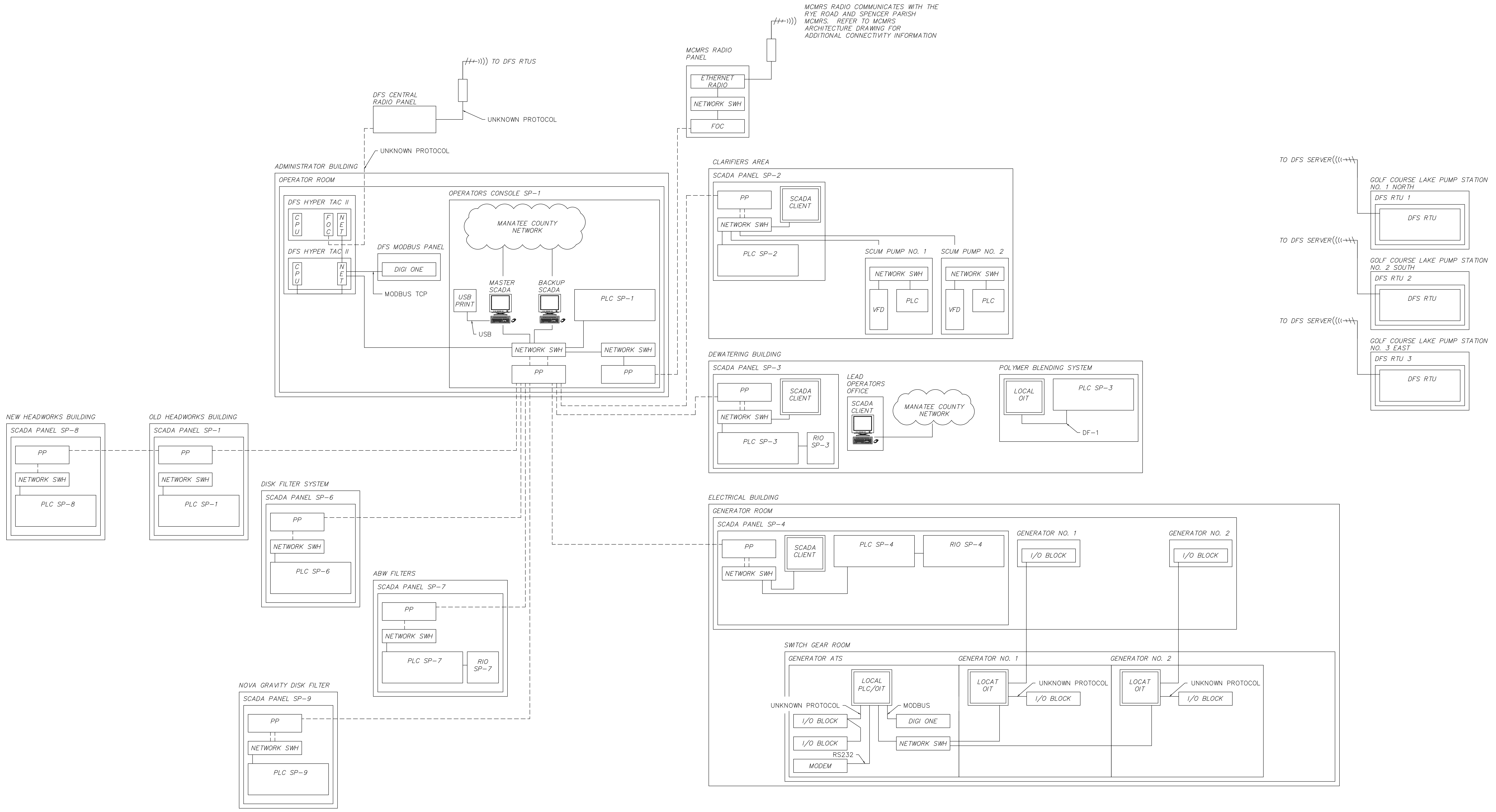
WRF SCADA EVALUATION

MCMRS
SCADA SYSTEM ARCHITECTURE DRAWING

VERIFY SCALES
BAR IS ONE INCH ON ORIGINAL DRAWING
0 1"
IF NOT ONE INCH ON THIS SHEET, ADJUST SCALES ACCORDINGLY

JOB NO.
10096H.00

DRAWING NO.



REV	DATE	BY	DESCRIPTION

DESIGNED
YOCUM

DRAWN
YOCUM

CHECKED
YOCUM

DATE
SEPTEMBER 2016

carollo®

Manatee County
FLORIDA

MANATEE COUNTY

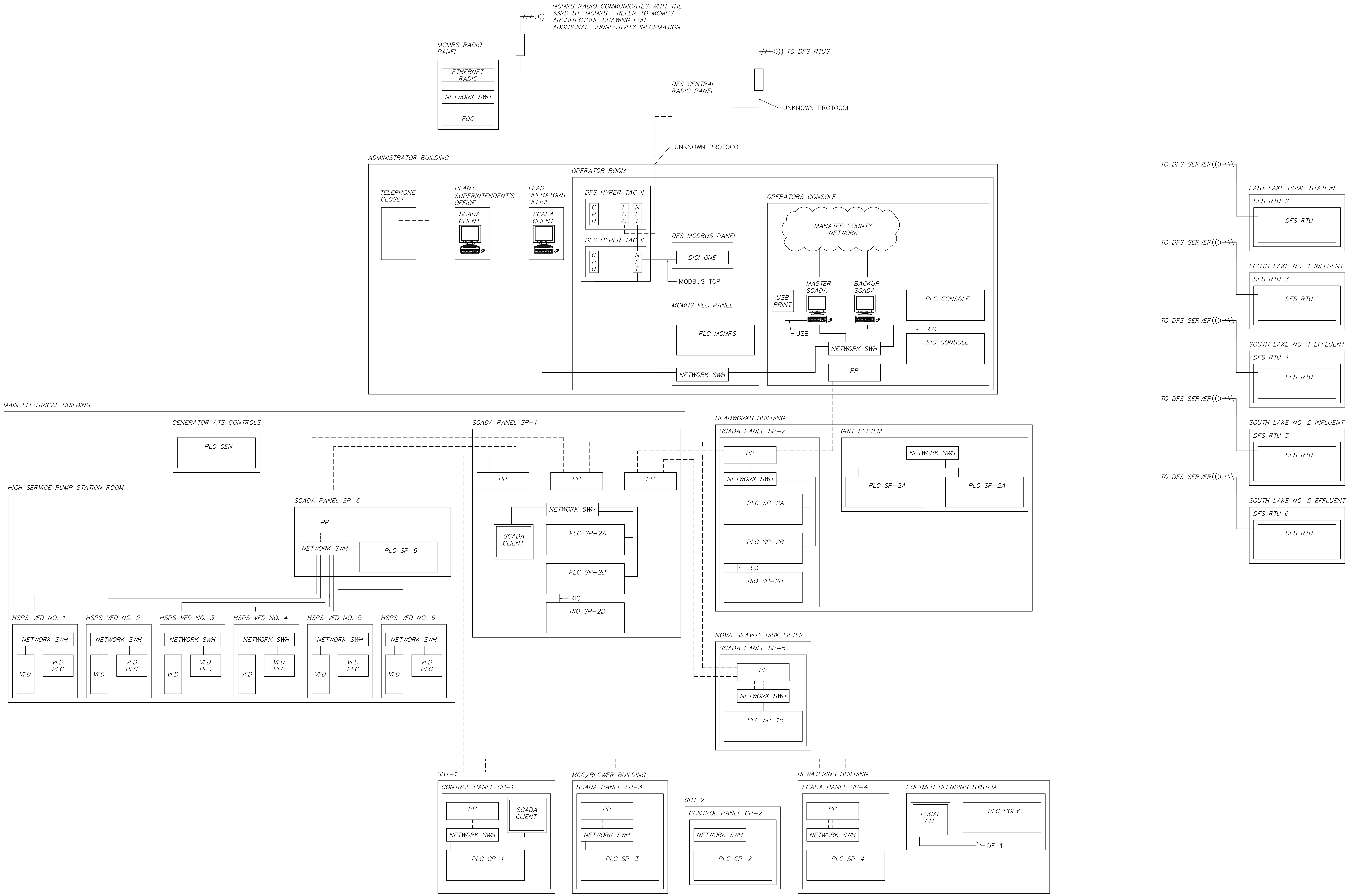
WRF SCADA EVALUATION

NORTH WRF
SCADA SYSTEM ARCHITECTURE DRAWING

VERIFY SCALES
BAR IS ONE INCH ON ORIGINAL DRAWING
0 1"
IF NOT ONE INCH ON THIS SHEET, ADJUST SCALES ACCORDINGLY

JOB NO.
10096H.00

DRAWING NO.



REV	DATE	BY	DESCRIPTION

DESIGNED
YOCUM
DRAWN
YOCUM
CHECKED
YOCUM
DATE
SEPTEMBER 2016

carollo®

Manatee County
FLORIDA

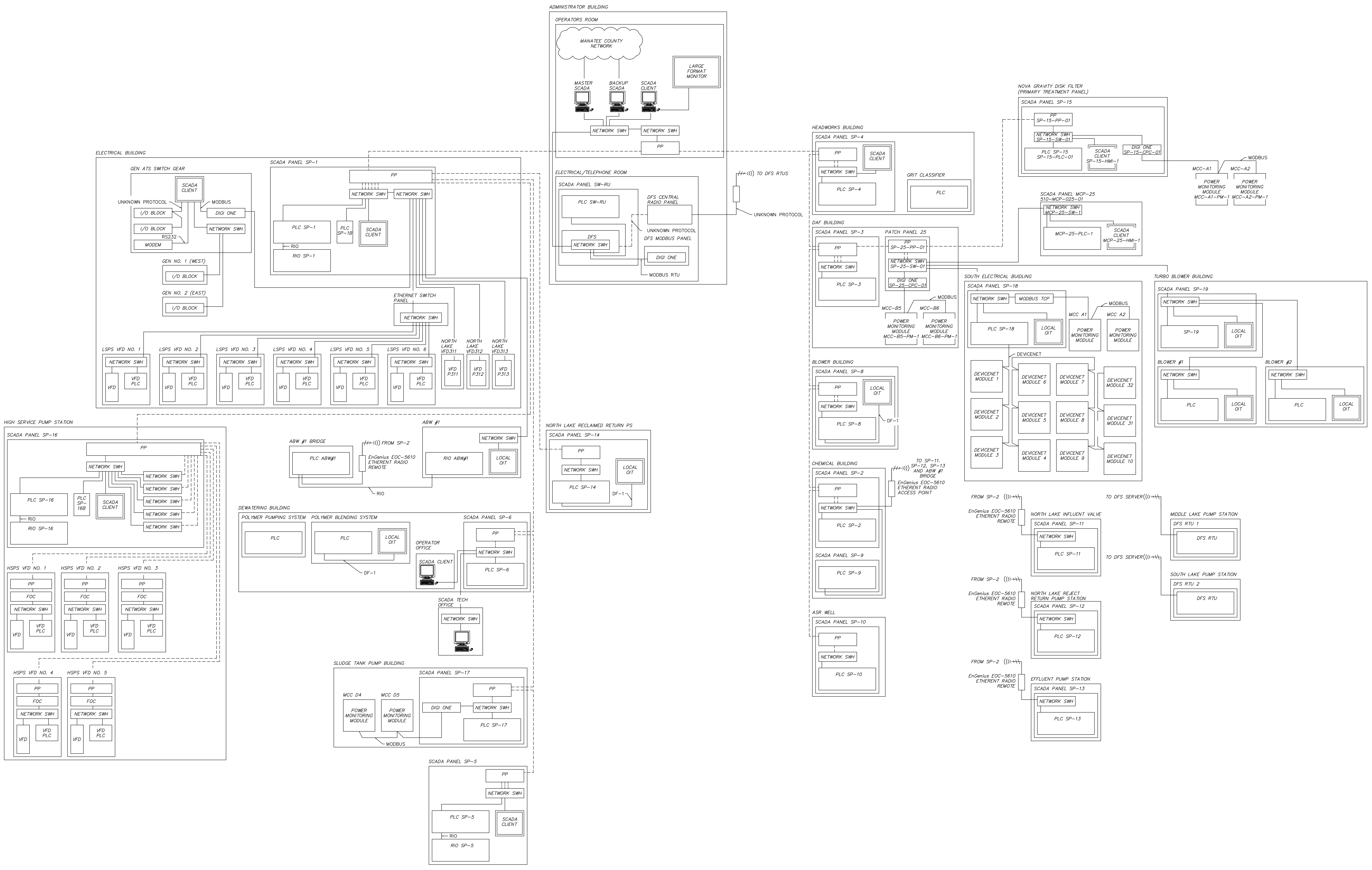
MANATEE COUNTY

WRF SCADA EVALUATION

SOUTHEAST WRF
SCADA SYSTEM ARCHITECTURE DRAWING

VERIFY SCALES
BAR IS ONE INCH ON ORIGINAL DRAWING
0 1"
IF NOT ONE INCH ON THIS SHEET, ADJUST SCALES ACCORDINGLY

JOB NO.
10096H.00
DRAWING NO.



REV	DATE	BY	DESCRIPTION

DESIGNED
YOCUM

DRAWN
YOCUM

CHECKED
YOCUM

DATE
SETP 2017

carollo®

Manatee County
FLORIDA

MANATEE COUNTY

WRF SCADA EVALUATION

SOUTHWEST WRF
SCADA SYSTEM ARCHITECTURE DRAWING

VERIFY SCALES
BAR IS ONE INCH ON ORIGINAL DRAWING
0 1"
IF NOT ONE INCH ON THIS SHEET, ADJUST SCALES ACCORDINGLY

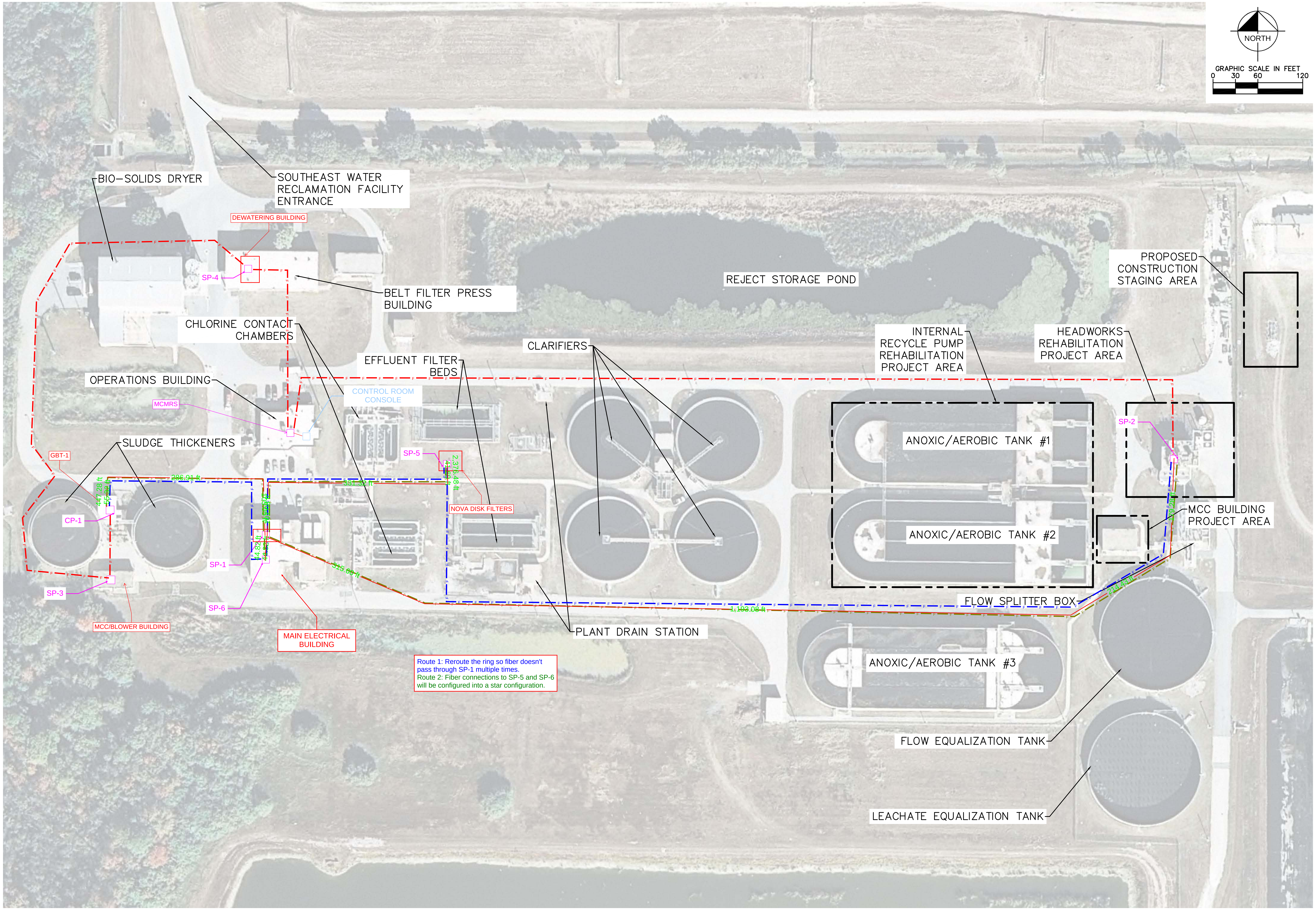
JOB NO.
10096H.00

DRAWING NO.

Appendix H

FIBER OPTIC CABLE MODIFICATIONS

Drawing name: K:\TAM_Civil\148400 – Manatee County\001 – SEWRF Headworks Rehab\CADD\PlanSheets\G-03 PROJECT LOCATION MAP.dwg PROJECT LOCATION MAP Dec 02, 2013 5:02pm by: jordan.walker



Route 1: Reroute the ring so fiber doesn't pass through SP-1 multiple times.
Route 2: Fiber connections to SP-5 and SP-6 will be configured into a star configuration.

No.	REVISIONS	DATE	BY

Kimley-Horn and Associates, Inc.

© 2013 KIMLEY-HORN AND ASSOCIATES, INC.
655 NORTH FRANKLIN STREET, SUITE 150, TAMPA, FL 33602
PHONE: 813-620-1460
WWW.KIMLEY-HORN.COM CA 00000696

DESIGN ENGINEER: WAYNE E. WHITE, P.E.
FLORIDA REGISTRATION NUMBER: 53232
DATE:

SCALE	AS NOTED
DESIGNED BY	JWW
DRAWN BY	JRT
CHECKED BY	WEW

PROJECT LOCATION MAP

MANATEE COUNTY SEWRF
MANATEE COUNTY FLORIDA

DATE
DECEMBER 2013

PROJECT NO.
148400001

SHEET NUMBER
G-0.3

BIO–SOLIDS DRYER
SOUTHEAST WATER RECLAMATION FACILITY ENTRANCE
DEWATERING BUILDING
SP-4
BELT FILTER PRESS BUILDING
REJECT STORAGE POND
PROPOSED CONSTRUCTION STAGING AREA
CHLORINE CONTACT CHAMBERS
EFFLUENT FILTER BEDS
CLARIFIERS
INTERNAL RECYCLE PUMP REHABILITATION PROJECT AREA
HEADWORKS REHABILITATION PROJECT AREA
OPERATIONS BUILDING
CONTROL ROOM CONSOLE
MCMRS
SP-2
SLUDGE THICKENERS
ANOXIC/AEROBIC TANK #1
GBT-1
SP-5
NOVA DISK FILTERS
MCC B
PROJE
CP-1
ANOXIC/AEROBIC TANK #2
SP-1
SP-3
SP-6
FLOW SPLITTER BOX
MCC/BLOWER BUILDING
PLANT DRAIN STATION
MAIN ELECTRICAL BUILDING
ANOXIC/AEROBIC TANK #3

NORTH
100' 0 100' 200'
SCALE: 1"=100' (Horiz.)
FLOATING TURBITITY BARRIER (TYP.)
ADDITIONAL SILT FENCE IN FRONT OF ALL CULVERTS THAT TO DRAIN INTO WETLANDS
SILT FENCE (TYP.)
NEW HEADWORKS BUILDING
SP-8
557.39 ft
DISK FILTER SYSTEM
ABW FILTERS
CLARIFIERS AREA
SP-2
SP-7
SP-6
OLD HEADWORKS BUILDING
SP-1
159.34 ft
SP-3
SP-9
ADMINISTRATION BUILDING
DEWATERING BUILDING
NOVA GRAVITY DISK FILTERS
158.36 ft
SP-4
ELECTRICAL BUILDING

NOTES

1. PRIOR TO THE COMMENCEMENT OF ANY CONSTRUCTION OR DEMOLITION ACTIVITIES, ALL SOIL EROSION AND SEDIMENTATION CONTROL MEASURES SHALL BE IN PLACE AND REMAIN THROUGHOUT CONSTRUCTION.

2. CONTRACTOR SHALL FOLLOW BEST MANAGEMENT PRACTICES THROUGHOUT CONSTRUCTION.

3. CONTRACTOR SHALL PREPARE AND SUBMIT A STORM WATER POLLUTION PLAN (SWPPP) FOR REVIEW AND APPROVAL PRIOR TO COMMENCEMENT OF ANY CONSTRUCTION ACTIVITIES. APPROVAL DOES NOT OBSOLVE CONTRACTOR OF RESPONSIBILITY FOR THE IMPLEMENTATION AND COMPLIANCE OF THE SWPPP. THE CONTRACTOR SHALL BE RESPONSIBLE FOR OBTAINING PERMITS ASSOCIATED WITH THE SWPPP.

4. SEE DWG NO. C-0.2.2 FOR DETAILS.

5. CARE SHALL BE EXERCISED TO PREVENT DISTURBANCE TO THE NATURAL VEGETATION IN AREAS NOT PROPOSED FOR IMMEDIATE CONSTRUCTION.

6. AS SOON AS PRACTICAL, ALL DRESSED SLOPES AND DISTURBED AREAS SHALL BE SODDED OR SEEDED AND MULCHED TO PREVENT EROSION.

7. CONTRACTOR SHALL PREPARE AND SUBMIT A DEWATERING PLAN SHOWING APPLICABLE BEST MANAGEMENT PRACTICES FOR REVIEW AND APPROVAL BY THE OWNER PRIOR TO ANY DEWATERING ACTIVITIES. APPROVAL DOES NOT OBSOLVE CONTRACTOR OF RESPONSIBILITY FOR DEWATERING ACTIVITIES.

8. CONTRACTOR SHALL BE RESPONSIBLE FOR OBTAINING PERMITS ASSOCIATED WITH DEWATERING ACTIVITIES.

9. DEWATERING WATER SHALL BE FILTERED AND TREATED WITH SILTATION SUMP AND/OR FILTER SOCKS OR OTHER FDEP APPROVED METHOD PRIOR TO DISCHARGE ONTO THE GROUND IN A MANNER IN WHICH THE WATER DOES NOT LEAVE THE PREMESIS OR CAUSE A NUISANSE TO PLANT OPERATIONS.

S:\1024\0143\80-Drawings\General\G-0.5.dwg, 7/15/2011 9:01:02 AM, Brian Nought

REV.NO.	DESCRIPTIONS	DATE

REVISIONS

SEAL

DAVID C. WEHNER, P.E.
No. 59541

SEAL

McKIM&CREED
1365 Hamlet Avenue
Clearwater, Florida 33756
Phone: (727)442-7196, Fax: (727)461-3827
EB0006691
www.mckimcreed.com

MANATEE COUNTY, FLORIDA

NWRF EXPANSION PHASE 1

SOIL EROSION AND SEDIMENTATION CONTROL PLAN

DATE:	JULY 2011
MCE PROJ. #	1024-0143
DRAWN	BFN
DESIGNED	DCW
CHECKED	JSL
PROJ. MGR.	DCW

SCALE
HORIZONTAL: 1" = 100'
VERTICAL: NA

DRAWING NUMBER
G-0.5

STATUS: ISSUED FOR BID
REVISION

NEW HEADWORKS BUILDING
SP-8
DISK FILTER SYSTEM
CLARIFIERS AREA
ABW FILTERS
SP-2
SP-7
SP-6
OLD HEADWORKS BUILDING
SP-1
ADMINISTRATION BUILDING
SP-3
SP-9
SILT FENCE (TYP.)
DEWATERING BUILDING
NOVA GRAVITY DISK FILTERS
SP-4
ELECTRICAL BUILDING
F

NEW HEADWORK S BUILDING
SP-8
ABW FILTERS
DISK FILTER SYSTEM
CLARIFIERS AREA
SP-7
SP-6
SP-2
OLD HEADWORKS BUILDING
SP-1
SP-3
SP-9
ADMINISTRATION BUILDING
SILT FENCE (TYP.)
SP-4
DEWATERING BUILDING
NOVA GRAVITY DISK FILTERS
ELECTRICAL BUILDING
F

LAB
10 MG RCW GROUND STORAGE TANK
EXIST. POND
EXIST. SWALE
HIGH SERVICE PUMP STATION
SP-16
NORTH
100' 0 100' 200'
SCALE: 1"=100' (Horiz.)
DISCHARGE STRUCTURE
METER VAULT
EFFLUENT PUMP STATION
PRESERVE AND PROTECT UTILITY POLES (TYP)
PRESERVE AND PROTECT METER ASSEMBLY
LAKE FILTERS
NORTH LAKE RETURN PUMP STATION
RETURN P.S. #4
SP-14
SP-15
NOVA DISK FILTERS
CHLORINE CONTACT CHAMBER
FINAL CLARIFIER No. 5
SP-10
SP-2
Blower Building
FINAL CLARIFIER NO. 1
DAF
SP-8
ABW #1
FINAL CLARIFIER NO. 2
SP-19
TURBO BLOWER BUILDING
SP-18
SOUTH ELETRICAL BUILDING
SP-3
DAF BUILDING
SP-1
NORTH POND 27.7 AC
AUTOMATIC BACKWASH FILTERS
ELECTRICAL BUILDING
VALVE VAULT
MECHANICAL BUILDING
FLOW EQUALIZATION TANK
HEADWORKS
SP-4
OPERATORS ROOM SW-RU
ADMINISTRATION BUILDING
AERATION BASINS
66TH STREET
FINAL CLARIFIER NO. 3
PRIMARY CLARIFIERS
THICKENERS
RAS/WAS PUMP STATION
FINAL CLARIFIER NO. 4
MAINTENANCE BUILDING
Sludge Tank Pump Building
SP-17
ANAEROBIC DIGESTERS
SP-5
SP-6
METER VAULT
OUTLET STRUCTURE
DEWATERING BUILDING
CHEMICAL STORAGE

S:\1024\0147\80-Drawings\Civil\C-0.1-CX-101.dwg, 2/15/2012 3:24:38 PM, Brian Naught

REV.NO.	DESCRIPTIONS	DATE

REVISIONS

SEAL

NORMAN J. SCALLY, P.E.
No. 41338

SEAL

MᶜKIM&CREED
1365 Hamlet Avenue
Clearwater, Florida 33756
Phone: (727)442-7196, Fax: (727)461-3827
EB0006691
www.mckimcreed.com

MANATEE COUNTY FLORIDA

MANATEE COUNTY, FLORIDA

SWWRF LAKE FILTRATION AND NORTH POND IMPROVEMENTS

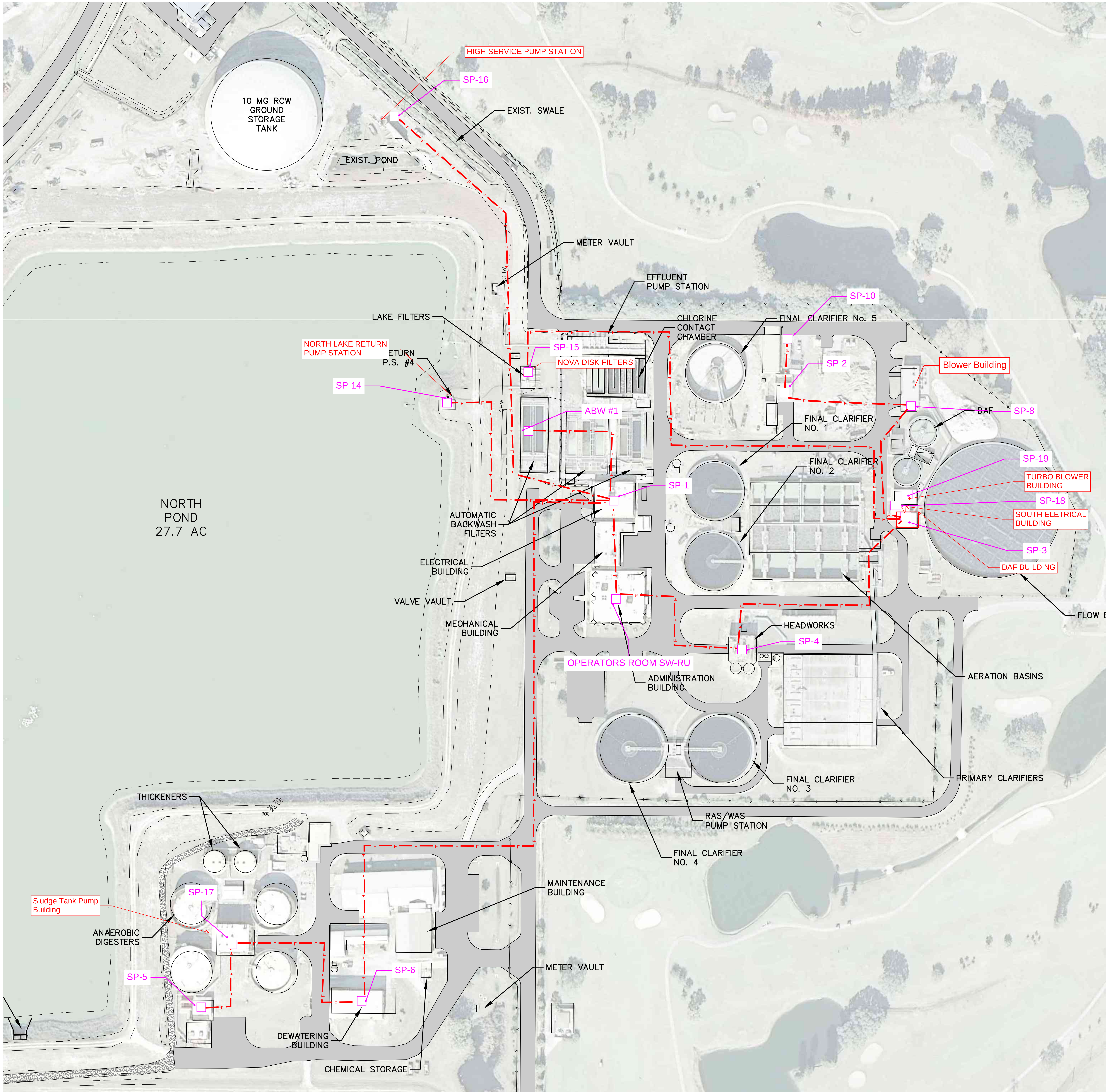
EXISTING SITE PLAN

DATE:	FEBRUARY 2012
MCE PROJ. #	1024-0147
DRAWN	BFN
DESIGNED	MSL
CHECKED	JSL
PROJ. MGR.	MSL

SCALE
HORIZONTAL: 1" = 100'
VERTICAL: NA

DRAWING NUMBER
C-0.1

STATUS: ISSUE FOR BID
REVISION


HIGH SERVICE PUMP STATION
SP-16
10 MG RCW
GROUND
STORAGE
TANK
EXIST. SWALE
EXIST. POND
METER VAULT
EFFLUENT
PUMP STATION
SP-10
LAKE FILTERS
CHLORINE
CONTACT
CHAMBER
FINAL CLARIFIER No. 5
NORTH LAKE RETURN
PUMP STATION
ETURN
P.S. #4
SP-15
NOVA DISK FILTERS
SP-2
Blower Building
SP-14
ABW #1
DAF
SP-8
FINAL CLARIFIER
NO. 1
SP-19
FINAL CLARIFIER
NO. 2
TURBO BLOWER
BUILDING
SP-1
SP-18
SOUTH ELETRICAL
BUILDING
NORTH
POND
27.7 AC
AUTOMATIC
BACKWASH
FILTERS
SP-3
DAF BUILDING
ELECTRICAL
BUILDING
VALVE VAULT
FLOW E
MECHANICAL
BUILDING
HEADWORKS
SP-4
OPERATORS ROOM SW-RU
ADMINISTRATION
BUILDING
AERATION BASINS
FINAL CLARIFIER
NO. 3
PRIMARY CLARIFIERS
THICKENERS
RAS/WAS
PUMP STATION
FINAL CLARIFIER
NO. 4
MAINTENANCE
BUILDING
SP-17
Sludge Tank Pump
Building
ANAEROBIC
DIGESTERS
SP-6
METER VAULT
SP-5
DEWATERING
BUILDING
CHEMICAL STORAGE

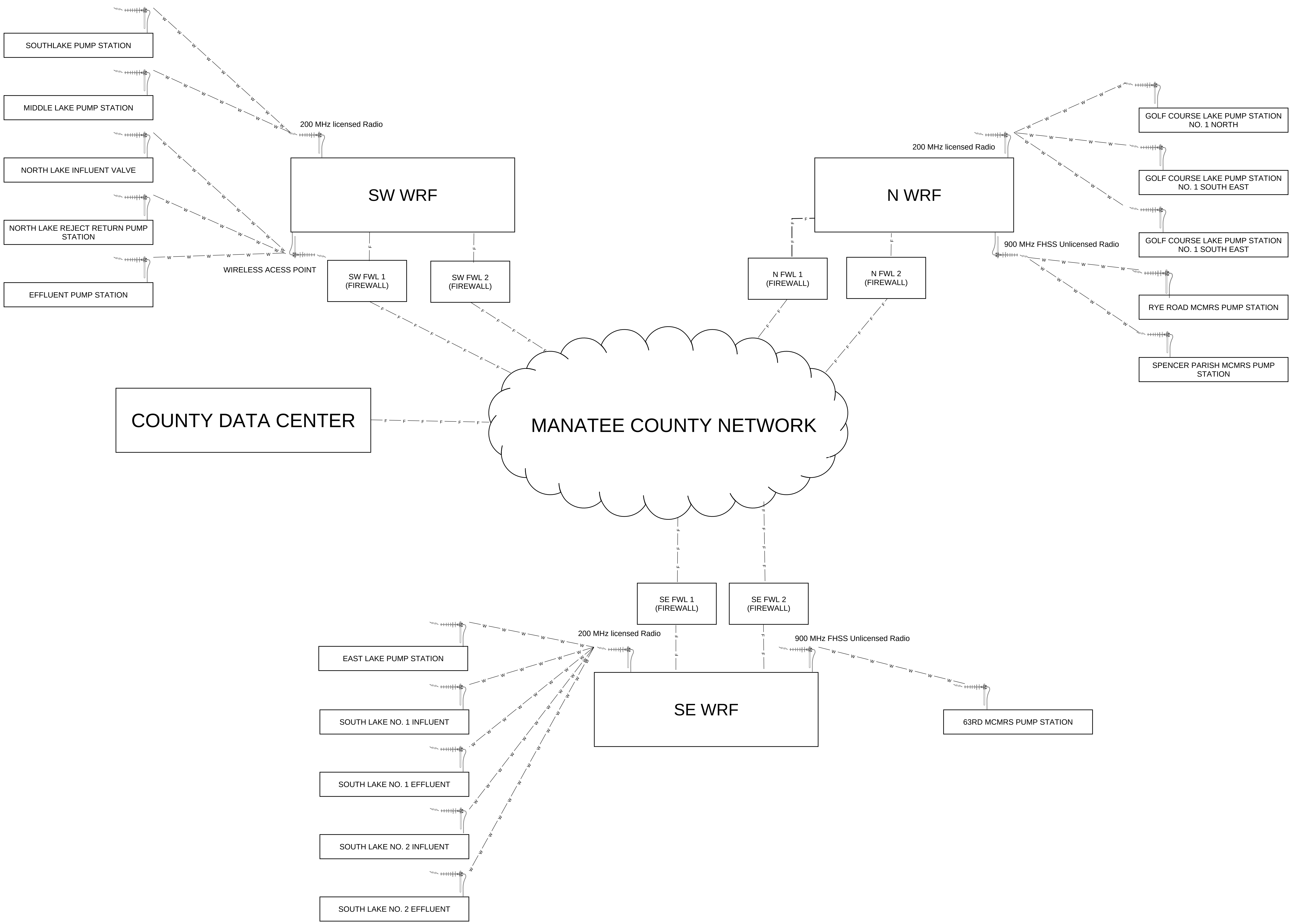

SOUTHLAKE PUMP STATION
MIDDLE LAKE PUMP STATION
NORTH LAKE INFLUENT VALVE
NORTH LAKE REJECT RETURN PUMP STATION
EFFLUENT PUMP STATION
200 MHz licensed Radio
WIRELESS ACESS POINT
SW WRF
SW FWL 1 (FIREWALL)
SW FWL 2 (FIREWALL)
COUNTY DATA CENTER
MANATEE COUNTY NETWORK
200 MHz licensed Radio
N WRF
N FWL 1 (FIREWALL)
N FWL 2 (FIREWALL)
900 MHz FHSS Unlicensed Radio
GOLF COURSE LAKE PUMP STATION NO. 1 NORTH
GOLF COURSE LAKE PUMP STATION NO. 1 SOUTH EAST
GOLF COURSE LAKE PUMP STATION NO. 1 SOUTH EAST
RYE ROAD MCMRS PUMP STATION
SPENCER PARISH MCMRS PUMP STATION
SE FWL 1 (FIREWALL)
SE FWL 2 (FIREWALL)
200 MHz licensed Radio
900 MHz FHSS Unlicensed Radio
SE WRF
EAST LAKE PUMP STATION
SOUTH LAKE NO. 1 INFLUENT
SOUTH LAKE NO. 1 EFFLUENT
SOUTH LAKE NO. 2 INFLUENT
SOUTH LAKE NO. 2 EFFLUENT
63RD MCMRS PUMP STATION
W
F

FIGURE - OVERALL COUNTY BACKBONE NETWORK

Appendix I

EUM PRIMER

Effective Utility Management

A Primer for Water and Wastewater Utilities

January 2017

EPA United States Environmental Protection Agency
Association of Metropolitan Water Agencies
ACWA Association of Clean Water Administrators
ASDWA Association of State Drinking Water Administrators
APWA
American Water Works Association
NACWA
NAWC National Association of Water Companies
Water Environment Federation the water quality people®
Water Environment & Reuse Foundation WE&RF
Water Research Foundation®

MESSAGE FROM THE EUM UTILITY LEADERSHIP GROUP

Dear Water Leader:

Every day you provide the leadership to deliver vital services that protect public health and support the vitality of your communities, natural environment, and economy; your organizations are truly anchor institutions in your communities. Today's water sector utilities also face a broad range of complex challenges, including rising costs and affordability, aging infrastructure, on-going regulatory requirements, enhanced customer expectations, and rapidly evolving technology. Utilities need a common sense, replicable, and proactive set of approaches to meet these current and future challenges.

Since 2008, a unique coalition representing the "Collaborating Organizations," which include the U.S. Environmental Protection Agency and a growing number of major water sector associations, has supported an approach developed by water sector leaders for water utility management. The approach is based around the Ten Attributes of an Effectively Managed Utility and Five Keys to Management Success—known as Effective Utility Management (EUM). EUM is now the most widely recognized water sector utility management program in the country, and this *Primer* is the foundation of EUM. The *Primer* will help your utility comprehensively assess current operations and identify a path to improving in key areas that are the highest priorities.

EUM, as embodied in this *Primer*, is more relevant than ever before to help meet the challenges that we face. EUM is a starting point for any utility's path to effective and sustainable operations. It can help your utility to respond to and plan for current and future challenges, supporting your mission of being a successful 21st century service provider. The *Primer* allows you to address these challenges in a step-wise process, at a pace that you control based on the capacity of your utility.

Key Messages to the Water Sector

EUM and this *Primer* are the keys to unlock the potential of your utility to protect public health and the environment in the 21st century:

- EUM helps you take a 360-degree look at your utility and then set priorities that work for you and your community.
- It helps you protect your current infrastructure investments and ensure that your workforce is motivated and able to address the challenges that they face every day.
- It moves you from reacting only to the "hot priorities" of the day to proactively planning for the future.
- It helps you engage your staff in the process of assessing and charting your own course for the future.
- It is simple, actionable, affordable, and scalable to meet the needs of all utilities.
- Finally, YOU CAN DO THIS. Staff across all levels of your utility can use the *Primer*, helping them collaborate internally and work with the community to provide affordable and sustainable services.

In closing, thank you for all you do every day. Please consider using the EUM *Primer* and chart a sustainable course for the future. We encourage you to join the growing group of utility leaders implementing EUM!

Sincerely,

The EUM Utility Leadership Group

EUM UTILITY LEADERSHIP GROUP

Colleen Arnold
Aqua America

Shellie Chard
Oklahoma Department of Environmental Quality

Barry Gullet
Charlotte Water

Dan Hartman
City of Golden Public Works

Patrick Kerr
Baton Rouge Water

Ed McCormick
McCormick Strategic Water Management, LLC
(Formerly with East Bay Municipal Utility District)

Tyler Richards
Gwinnett County Department of Water Resources

Frank Roth
Albuquerque Bernalillo County Water Utility Authority

Tom Sigmund
NEW Water

Kathryn Sorensen
Phoenix Water

John Sullivan
Boston Water and Sewer Commission

Diane Taniguchi-Dennis
Clean Water Services

Donna Wies
Donna Wies Consulting
(Formerly with Union Sanitary District)

Tim Wilson
Marshalltown Water

EUM COLLABORATING ORGANIZATIONS

Julia Anastasio
Association of Clean Water Administrators

Adam Carpenter
American Water Works Association

Alison Deines
Water Environment & Reuse Foundation

Chris Hornback
National Association of Clean Water Agencies

Jim Horne
Office of Water
U.S. Environmental Protection Agency

Anne Jackson
American Public Works Association

Carolyn Peterson
Association of Metropolitan Water Agencies

Linda Reekie
Water Research Foundation

Matt Ries
Water Environment Federation

Petra Smeltzer
National Association of Water Companies

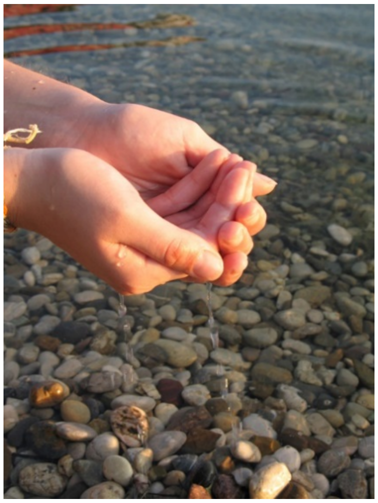
Jim Taft
Association of State Drinking Water Administrators

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

This product was developed with assistance from Rob Greenwood, Morgan Torres, and Sarah Shadid with Ross Strategic (www.rossstrategic.com), under contract EP-C-11-009 with the Office of Wastewater Management at U.S. EPA.

TABLE OF CONTENTS

I. Effective Utility Management



The *Effective Utility Management: A Primer for Water and Wastewater Utilities* (“*Primer*”) is the foundation of Effective Utility Management (EUM). It is designed to help water and wastewater utility managers make informed decisions and practical, systematic changes to achieve excellence in utility performance in the face of everyday challenges and long-term needs for the utility and the community it serves. It was produced by utility leaders who are committed to helping other utilities improve water and wastewater management. The *Primer* distills the expertise and experience of these utility leaders into a framework intended to help utilities identify and address their most pressing needs through an incremental, continual improvement management approach.

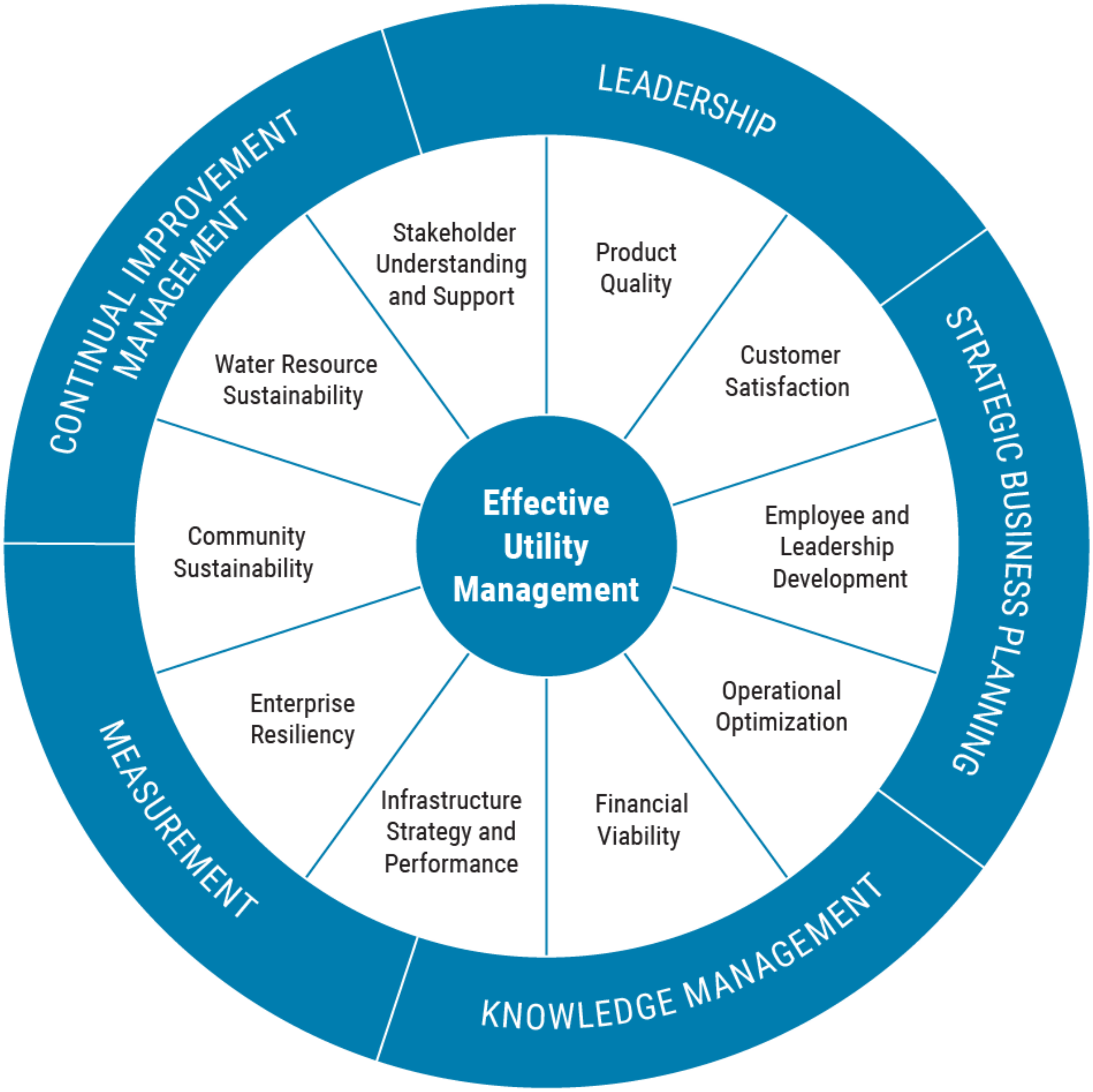
All water and wastewater utilities can benefit from applying this *Primer*. Each utility has unique management opportunities and challenges, and this *Primer* provides a common sense way of assessing, managing, and measuring a utility’s performance to address these opportunities and challenges. The steps described in the document and associated resources are relevant to any water or wastewater utility, regardless of size, budget, or other capacity.

The *Primer* has four primary components which, when taken together, form the basis for a complete cycle of effective and sustainable utility management:

- **The Ten Attributes of Effectively Managed Water Sector Utilities (Attributes).** These Attributes provide a clear set of reference points and are intended to help utilities maintain a balanced focus on all important operational areas rather than reactively moving from one problem to the next or focusing on the “problem of the day.”
- **Five Keys to Management Success.** These proven approaches help utilities maximize their resources and improve performance. By embedding the Five Keys to Management Success into their workplace culture, utilities create a robust foundation for strong, ongoing performance in the Ten Attribute areas.
- **Where to Begin – A Self-Assessment Tool**. The rigorous and systematic self-assessment tool described in the *Primer* helps utility managers and staff evaluate their operations and identify where to begin improvement efforts. By assessing how a utility performs relative to the Attributes, utility managers can gain a more balanced and comprehensive picture of their organization.
- **Getting to Work – Implementation of Effective Utility Management.** The Implementation section is a central connecting point between multiple elements of Effective Utility Management. It focuses on an overall continual improvement cycle (the “EUM cycle”), and describes how a utility’s self-assessment results can lead into a cycle of planning, implementation of effective practices, measuring performance, and making adjustments over time. It includes the following components:
  1. A description of the essential components of the EUM cycle;
  2. A guide for measuring performance;
  3. Resources to support Effective Utility Management implementation; and
  4. Steps for creating an Improvement Plan.

Throughout the *Primer,* utilities will learn about the Ten Attributes of Effectively Managed Utilities and the Five Keys to Management Success, and how these important elements work in tandem to support successful utilities in today's challenging operating contexts.

The Ten Attributes of Effectively Managed Utilities and Five Keys to Management Success


LEADERSHIP
STRATEGIC BUSINESS PLANNING
KNOWLEDGE MANAGEMENT
MEASUREMENT
CONTINUAL IMPROVEMENT MANAGEMENT
Product Quality
Customer Satisfaction
Employee and Leadership Development
Operational Optimization
Financial Viability
Infrastructure Strategy and Performance
Enterprise Resiliency
Community Sustainability
Water Resource Sustainability
Stakeholder Understanding and Support
Effective Utility Management

This *Primer* is the product of a decade-long collaboration between the Collaborating Organizations and group of respected water and wastewater utility leaders from across the nation. Originally released in 2008, and updated in 2017 to reflect changes to the context in which water sector utilities operate, the *Primer* is a powerful tool for water sector utilities of all sizes, types, and geographies. A brief history of Effective Utility Management is included on the following page.

A Brief History of Effective Utility Management

MAY 2006

Seven Collaborating Organizations sign a Statement of Intent to establish a framework for working together to advance understanding of the principles and practices of effective utility management, and to encourage and promote their wider application.

MAY 2007

Findings and Recommendations report delivered from a utility Steering Committee to the seven collaborating organizations. The report recommends a variety of activities be initiated, including the development of a stand-alone primer that outlines a strategy for effective utility management.

JUNE 2008

Effective Utility Management: A Primer for Water and Wastewater Utilities is released.

2009 - 2015

The Collaborating Organizations develop and sponsor a wide range of EUM-based workshops, webinars, case examples, and award programs to promote and support EUM implementation by the water sector.

APRIL 2015

The Association of Clean Water Agencies and the Association of State Drinking Water Administrators join as new EUM Collaborating Organization partners.

Collaborating Organizations convene a group of utility leaders to explore how the operating context of water sector utilities has changed since the *Primer* was released in 2008, and to consider refinements to the EUM framework.

FEB 2016

Taking the Next Step: Findings of the Effective Utility Management Review Steering Group report released. The report outlines key operating shifts in the water sector since 2008, and recommends a series of updates to the *Primer.*

JULY–DEC 2016

Collaborating Organizations convene a group of utility leaders to update the *Primer.*

OCT 2016

The Water Research Foundation and the Water Environment & Reuse Foundation join as new EUM Collaborating Organization partners.

JAN 2017

The Collaborating Organizations release the newly updated *Primer.*

2017 & BEYOND

The Collaborating Organizations sponsor ongoing education and promotional efforts to support implementation of EUM by the water sector, including webinars, workshops, and the development of other learning resources.

II. Ten Attributes of an Effectively Managed Utility

The Ten Attributes of an Effectively Managed Utility provide useful and concise goals for water sector utility managers seeking to improve organization-wide performance. The Attributes describe desired outcomes that are applicable to all water and wastewater utilities. They comprise a comprehensive framework related to operations, infrastructure, customer satisfaction, community sustainability, natural resource stewardship, and financial performance.

Water and wastewater utilities can use the Attributes to select priorities for improvement, based on each organization's strategic objectives and the needs of the community it serves. The Attributes are not presented in a particular order, but rather can be viewed as a set of opportunities for improving utility management and operations. **Section IV** provides a basic self-assessment tool to help utilities easily identify their priorities and opportunities based on the Attributes. Over time, utilities will be able to deliver increasingly efficient, high-quality service by addressing more, and eventually all, of the Attributes. **Section V** provides several example performance measures for each of the Attributes.

Ten Attributes of an Effectively Managed Utility

Product Quality

Produces “fit for purpose” water and other recovered resources (e.g., energy, nutrients, biosolids) that meet or exceed full compliance with regulatory and reliability requirements and consistent with customer, public health, ecological, and economic needs. Products include treated drinking water, treated wastewater effluent, recycled water, stormwater discharge, and recovered resources.

Customer Satisfaction

Provides reliable, responsive, and affordable services in line with explicit, customer-derived service levels. Utilizes a mix of evolving communication technologies to understand and respond to customer needs and expectations, including receiving timely customer feedback and communicating during emergencies. Provides tailored customer service and outreach to traditional residential, commercial, and industrial customers, and understands and exercises as appropriate the opportunities presented by emergent customer groups (e.g., high strength waste producers, power companies).

Stakeholder Understanding and Support

Engenders understanding and support from stakeholders (anyone who can affect or be affected by the utility), including customers, oversight bodies, community and watershed interests, and regulatory bodies for service levels, rate structures, operating budgets, capital improvement programs, and risk management decisions. Actively promotes an appreciation of the true value of water and water services, and water’s role in the social, economic, public and environmental health of the community. Actively engages in partnerships, involves stakeholders in the decisions that will affect them, understands what it takes to operate as a “good neighbor,” and positions the utility as a critical asset (anchor institution) to the community.

Financial Viability

Understands and plans for the full life-cycle cost of utility operations and value of water resources. Establishes and maintains an effective balance between long-term debt, asset values, operations and maintenance expenditures, and operating revenues. Establishes predictable rates—consistent with community expectations and acceptability—adequate to recover costs, provide for reserves, maintain support from bond rating agencies, plan and invest for future needs, and taking into account affordability and the needs of disadvantaged households. Implements sound strategies for collecting customer payments. Understands the opportunities available to diversify revenues and raise capital through adoption of new business models, including revenues from resource recovery.

Operational Optimization

Ensures ongoing, timely, cost-effective, reliable, and sustainable performance improvements in all facets of its operations in service to public health and environmental protection. Makes effective use of data from automated and smart systems, and learns from performance monitoring. Minimizes resource use, loss, and impacts from day-to-day operations, and reduces all forms of waste. Maintains awareness of information and operational technology developments to anticipate and support timely adoption of improvements.

Employee and Leadership Development

Recruits, develops, and retains a workforce that is competent, motivated, adaptive, and safety-focused. Establishes a participatory, collaborative organization dedicated to continual learning, improvement, and innovation. Ensures employee institutional knowledge is retained, transferred, and improved upon over time. Emphasizes and invests in opportunities for professional and leadership development, taking into account the differing needs and expectations of a multi-generational workforce and for resource recovery operations. Establishes an integrated and well-coordinated senior leadership team.

Enterprise Resiliency

Ensures utility leadership and staff work together internally, and coordinate with external partners, to anticipate, respond to, and avoid problems. Proactively identifies, assesses, establishes tolerance levels for, and effectively manages a full range of business risks (including interdependencies with other services and utilities, legal, regulatory, financial, environmental, safety, physical and cyber security, knowledge loss, talent, and natural disaster-related) consistent with industry trends and system reliability goals. Plans for and actively manages around business continuity.

Infrastructure Strategy and Performance

Understands the condition of and costs associated with critical infrastructure assets. Plans infrastructure investments consistent with community needs, anticipated growth, system reliability goals, and relevant community priorities, building in a robust set of adaptation strategies (e.g., for changing weather patterns, customer base). Maintains and enhances the condition of all assets over the long-term at the lowest possible life-cycle cost and acceptable risk consistent with customer, community, and regulator-supported service levels. Assures asset repair, rehabilitation, and replacement efforts are coordinated within the community to minimize disruptions and other negative consequences.

Community Sustainability

Takes an active leadership role in promoting and organizing community sustainability improvements through collaboration with local partners (e.g., transportation departments, electrical utilities, planning departments, economic development organizations, watershed and source water protection groups). Manages operations, infrastructure, and investments to support the economic, environmental, and social health of its community. Integrates water resource management with other critical community infrastructure, social and economic development planning to support community-wide resilience, support for disadvantaged households, community sustainability, and livability.

Water Resource Sustainability

Ensures the availability and sustainable management of water for its community and watershed, including water resource recovery. Understands its role in the complete water cycle, understands fit for purpose water reuse options, and integrates utility objectives and activities with other watershed managers and partners. Understands and plans for the potential for water resource variability (e.g., changing weather patterns, including extreme events, such as drought and flooding), and utilizes as appropriate a full range of watershed investment and engagement strategies (e.g., Integrated Planning). Engages in long-term integrated water resource management, and ensures that current and future customer, community, and ecological water-related needs are met.

III. Keys to Management Success

The Keys to Management Success represent frequently used management approaches and systems that experience indicates help water and wastewater utilities manage more effectively. They create a supportive context for a utility as it works towards the outcomes outlined in the Attributes, and they can help integrate the utility's improvement efforts across the Attributes. The Keys to Management Success are listed below.

Leadership

Leadership must respond to both internal organizational and broader external community imperatives. It is critical to effective utility management, particularly in the context of leading and inspiring change within an organization and in its surrounding community.

"Leadership" refers both to individuals who can be effective champions for improvement, and to teams that provide resilient, day-to-day management continuity and direction. Effective leadership establishes and communicates a long-term vision for the organization and embodies a commitment to cultivating the organization's culture, helping to ingrain methods to achieve the utility's vision into the organization's day-to-day operations.

Leaders have an important responsibility to engage proactively with stakeholders and community decision makers, promote the utility as a valued, competent, and trustworthy environmental steward and community asset, and collaborate with external partners (including new and nontraditional partners, like the agricultural sector). Leaders should drive an awareness and commitment to workplace safety, organizational diversity, ethical conduct, and positive morale. Leadership further reflects a commitment to organizational excellence, leading by example to establish and reinforce an organizational culture that embraces positive change, providing new opportunities for emerging leaders, and planning for and assuring a seamless transition to new leadership when required. Organizational improvement efforts require a commitment to continual improvement from the utility's leadership, including the celebration of small and large victories for the utility.

Strategic Business Planning

Strategic business planning directs and helps to achieve balance and cohesion across the Ten Attributes. A strategic business plan provides a framework for decision making by:

- Assessing current conditions and conducting a strengths, weaknesses, opportunities, and threats (SWOT analysis);
- Characterizing a continuum of possible and likely future conditions;
- Assessing underlying causes and effects of future conditions; and
- Establishing vision, objectives, strategies, and underlying organizational values.

A successful strategic business plan is dynamic and adaptable, allowing the utility to capitalize on new and emerging opportunities. It is made more robust by engaging with staff and external stakeholders, and by utilizing planning methods that can accommodate and address a variety of future operating scenarios (e.g., managing for uncertainty through "stress testing" a plan's ability to hold up during extreme events, such as extended drought).

A strong plan reflects specific implementation steps that will move a utility from its current level of performance to achieving its vision. Preparation of a strategic business plan involves taking a longer-term view of utility goals and operations and establishing a clear vision and mission. The plan, through engagement with external stakeholders, should reflect key community values, needs, and interests. When developed, the strategic business plan should drive and guide utility objectives, measurement efforts, investments, and operations. A strategic business plan can also help explain the utility's conditions, goals, and plans to staff and stakeholders, stimulate change, and increase engagement and support for improvement efforts. After developing a strategic business plan, it is important that the utility integrates tracking of progress and clear accountability into its management framework, and revisits the plan on a regular basis.

Knowledge Management

Knowledge management is another cornerstone of effective utility management, and is critical to ensuring reliable utility operations. It spans standard operating procedures, human resource management, and business systems and operating systems data integration and utilization to support dependable operations and continual improvement across the Ten Attributes.

By ensuring that processes are well documented through writing down "this is how we do things" and regularly updating standard operating procedures and creating shared knowledge among various employee categories, a utility is able to respond effectively to the inevitable knowledge loss brought on by employee turnover or unexpected absences. An effective knowledge management system is flexible to the use of new and evolving technologies, and should be updated on an ongoing basis. Automated "smart" systems and data integration/management capabilities are an increasingly important aspect of efficient and effective continual improvement management. These systems and capabilities are available across all areas of utility management, and can substantially improve the ability of utilities to track performance in real time, identify variability, and manage performance more effectively and precisely.

Measurement

Measurement is critical to management improvement efforts associated with the Attributes and is the backbone of successful continual improvement management and strategic business planning. A measurement system serves many vital purposes, including focusing attention on key issues, clarifying

> "If you can't measure it, you can't improve it."
>
> *Peter Drucker*

expectations, facilitating decision making, supporting learning and improving, establishing and maintaining accountability, and, most importantly, communicating effectively internally and externally. Always keep in mind the management adage, “If you can’t measure it, you can’t improve it.” Successful measurement efforts should be:

- Carefully select a limited number of performance measures that are used to focus the organization on the achievement of the Strategic Business Plan goals;
- Viewed as a continuum starting with basic internal tracking, and moving to more sophisticated baselining and trend analysis as necessary, with development of key performance indicators, and inclusion of externally oriented measures which address community sustainability interests;
- Informed by staff input, driven by and focused on answering questions critical to effective internal management and external stakeholder needs, including information needed to allow governing bodies to comfortably support large capital investments; and
- Supported by a well-defined decision framework assuring results are evaluated, communicated, and addressed in a timely manner.

Continual Improvement Management

Continual improvement management is usually implemented through a complete, start-to-finish management system, also referred to as a “Plan-Do-Check-Act” framework. Continual improvement plays a central role in effective utility management and is critical to making progress on the Attributes. Continual improvement management includes:

- Conducting an honest and comprehensive self- assessment – informed through staff engagement – to identify management strengths, areas for improvement, priority needs, etc.;
- Conducting frequent sessions among interested parties (stakeholders) to identify improvement opportunities;
- Following up on improvement projects underway;
- Establishing and implementing performance measures and specific internal targets associated with those measures;
- Defining and implementing related operational requirements, practices, and procedures;
- Defining supporting roles and responsibilities to derive clear accountability for conducting assessments and implementing performance improvements;
- Implementing measurement activities such as regular evaluation through operational and procedural audits; and
- Responding to evaluations through the use of an explicit change management process.

Continual improvement management is further supported by gap analysis, establishment of standard operating procedures, internal trend analysis and external benchmarking where appropriate, best practice review and adoption, and other continual improvement tools. It can be used as a framework to help utilities understand improvement opportunities and establish explicit service levels, guide investment and operational decisions, form the basis for ongoing measurement, and provide the ability to communicate clearly with customers and key stakeholders.

IV. Where to Begin: A Self-Assessment Tool

There are many ways to improve utility performance and each utility is unique. Many utilities may choose to start small and make improvements step-by-step, perhaps by working on projects that will yield early successes. Other utilities may choose to take on several improvement efforts simultaneously. Some may prefer to enhance their strengths, while others will prefer to focus on addressing areas for improvement. Each utility should determine for itself the most important issue to address, based on its own strategic objectives, priorities, and the needs of the community it serves.

A thorough assessment of current performance based on the Attributes is a useful first step in identifying options for improvement. It also establishes a quantifiable baseline from which to measure progress. As conditions change, future reassessments will reveal new opportunities and new priorities.

The following Self-Assessment tool can help water and wastewater managers use the EUM Attributes to evaluate their utility's current performance against internal goals or specific needs and determine where to focus improvement efforts. While it can be completed initially by an individual manager, it is more effective when used as a vehicle for conversation and consensus building among the utility's management team and key staff. As appropriate, other stakeholders might be invited to participate in the assessment, including oversight bodies, community and watershed interests, and regulatory authorities.

STEP 1

Candidly Assess Current Conditions

STEP 2

Rank Importance of Each Attribute to Your Entity

STEP 3

Graph Attributes to Determine Importance and Level of Achievement

STEP 4

Choose Attributes

The assessment has four steps: 1) Assess current conditions based on the Attributes; 2) Rank the importance of each Attribute for your utility; 3) Chart the results; and 4) Choose one or more Attributes to focus on. Following completion of the Self-Assessment, a guide for taking action on the results is included in the next section, **Getting to Work: Implementation of Effective Utility Management.**

A blank copy of the Self-Assessment worksheet is available in **Appendix B.**

Step 1: Assess Current Level of Achievement

Using the blank worksheet in **Appendix B**, assess current conditions by rating your utility's systems and approaches and current level of achievement for each Attribute, using a 1 (high achievement) to 5 (low achievement) scale. Consider the degree to which your current management systems effectively support each of the Attributes and their component parts. Consider all components of each Attribute and gauge your rating accordingly. Use these descriptions to guide your rating. You will note that each Attribute has several components represented by the bullet points listed for each.

Your rating can either reflect the lowest level of achievement of all of the bullet points for that Attribute (for example, if you believe that your achievement in one of the bullet points for that Attribute was "5," but another bullet point you rated as "2," your rating for achievement under that Attribute would be "5"), or an average across all of the bullet points for that Attribute. For whatever approach you choose to use when rating, make sure to be consistent in this approach across all Attributes.

Rating	Description
1.	Effective, systematic approach and implementation; consistently achieve goals.
2.	Workable systems in place; mostly achieve goals.
3.	Partial systems in place with moderate achievement, but could improve.
4.	Occasionally address this when specific need arises.
5.	No system for addressing this.

Step 2: Rank Importance of Attributes

Rank the importance of each Attribute to your utility, based on your utility's vision, goals, and specific needs. The ranking should reflect the interests and considerations of all stakeholders (managers, staff, customers, regulators, elected officials, community and watershed interests, and others).

There are Ten Attributes. Considering long-term importance to your utility, rank the most important Attribute 1, the second most important 2, and so on. The least important Attribute would be ranked 10. Your ranking of each Attribute's importance may be influenced by current or expected challenges in that particular area, recent accomplishments in addressing these issues, or other factors. Importance ranking is likely to change over time as internal and external conditions change.

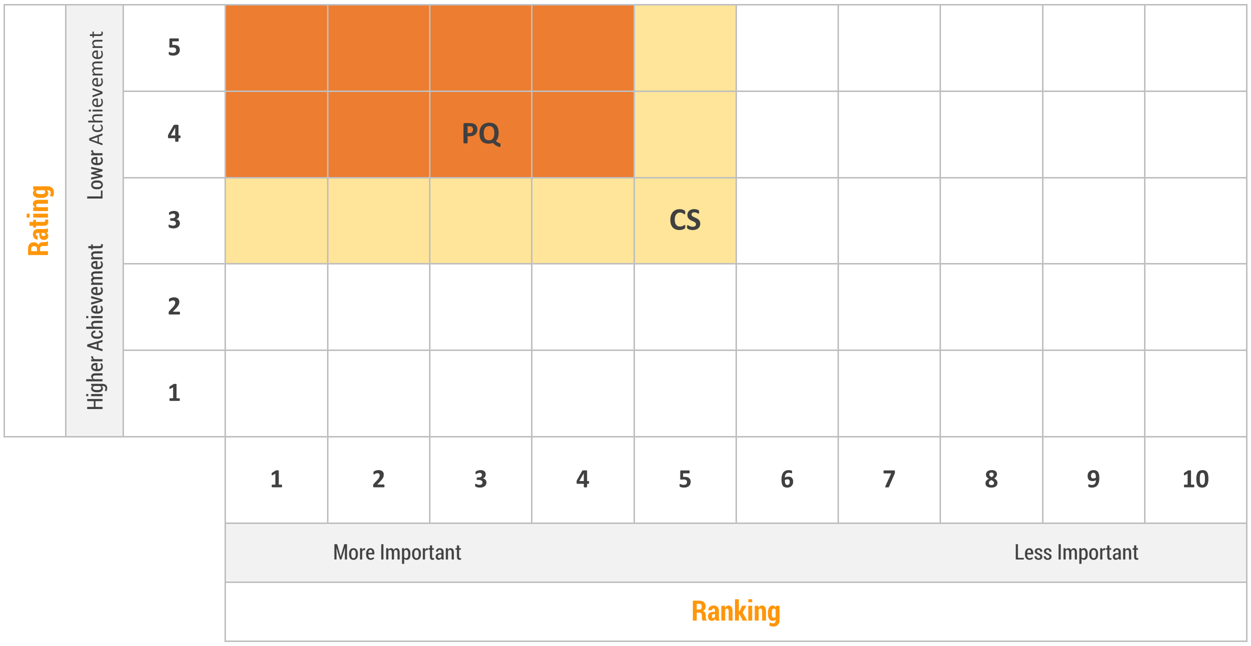
As you fill in numbers on the worksheet in **Appendix B**, please note that your analysis for Step 1 (rating achievement) should be separate and independent from your analysis for Step 2 (ranking importance).

Attribute	Attribute Components
Product Quality (PQ)	• Meets or exceeds regulatory and reliability requirements. • Operates consistent with customer, public health, economic, and ecological needs.
Customer Satisfaction (CS)	• Provides reliable, responsive, and affordable services. • Receives timely customer feedback. • Is responsive to customer needs and emergencies. • Provides tailored customer service and outreach to a range of customer groups (e.g., residential, commercial, industrial, and newly emerging groups such as high-strength waste producers or power companies)
Employee and Leadership Development (ED)	• Recruits, develops, and retains a competent, safety-focused workforce. • Is a collaborative organization dedicated to continual learning, improvement, and adaptation. • Implements procedures for institutional knowledge retention, workplace safety, and continual learning (e.g., standard operating procedures). • Invests in/provides opportunities for professional and leadership development. • Supports an integrated and well-coordinated senior leadership team.
Operational Optimization (OO)	• Conducts ongoing performance improvements informed by performance monitoring. • Minimizes resource use and loss from day-to-day operations. • Is aware of and adopts in a timely manner operational and technology improvements, including operational technology and information technology. • Manages and utilizes data from automated and smart systems.
Financial Viability (FV)	• Understands and plans for full life-cycle cost of utility. • Effectively balances long-term debt, asset values, operations and maintenance expenditures, and operating revenues. • Sets predictable and adequate rates to support utility current needs and plans to invest in future needs, taking into account affordability and the needs of disadvantaged households when setting rates. • Understands opportunities for diversifying revenue and raising capital.
Infrastructure Strategy and Performance (IS)	• Understands the condition of and costs associated with critical infrastructure assets. • Maintains and enhances assets over the long-term at the lowest possible life-cycle cost and acceptable risk. • Coordinates repair efforts within the community to minimize disruptions. • Plans infrastructure investments consistent with community needs, anticipated growth, system reliability goals, and with a robust set of adaptation strategies.
Enterprise Resiliency (ER)	• Works together with staff internally and coordinate with external partners to anticipate and avoid problems. • Proactively establishes tolerance levels and effectively manages risks (including legal, regulatory, financial, environmental, safety, security, cyber, knowledge-loss, talent, and natural disaster-related). • Plans for and actively manages to maintain business continuity.

Attribute	Attribute Components
Community Sustainability (SU)	• Actively leads in promoting and organizing improvements to community and watershed health within utility and with external community partners. • Actively leads in promoting welfare within the community for disadvantaged households. • Uses operations to enhance natural environment. • Efficiently uses water and energy resources, promotes economic vitality, and engenders overall community improvement. • Maintains and enhances ecological and community sustainability including pollution prevention, watershed and source water protection.
Water Resource Sustainability (WS)	• Ensures water availability through long-term resource supply and demand analysis, conservation, fit for purpose water reuse, integrated water resource management, watershed management and protection, and public education initiatives. • Manages operations to provide for long-term aquifer and surface water sustainability and replenishment. • Understands and plans for future water resource variability (e.g., changing weather patterns, including extreme events, such as drought and flooding).
Stakeholder Understanding and Support (SS)	• Engenders understanding and support from oversight bodies, community and watershed interests, and regulatory bodies for service levels, rate structures, operating budgets, capital improvement programs, and risk management decisions. • Actively engages in partnerships and involves stakeholders in the decisions that will affect them. • Actively promotes an appreciation of the true value of water and water services, and water’s role in the social, economic, public and environmental health of the community.

Step 3: Graph Results

Graph each Attribute based on your rating and ranking. For example, if you rated Product Quality (PQ) 4 for achievement and ranked it 3 for importance, you would place it on the graph as illustrated below. Similarly, if you rated Customer Satisfaction (CS) 3 for achievement and ranked it 5 for importance, you would place it on the graph as illustrated below. A blank graph is provided in **Appendix B**.



Step 4: Choose Attributes to Focus On

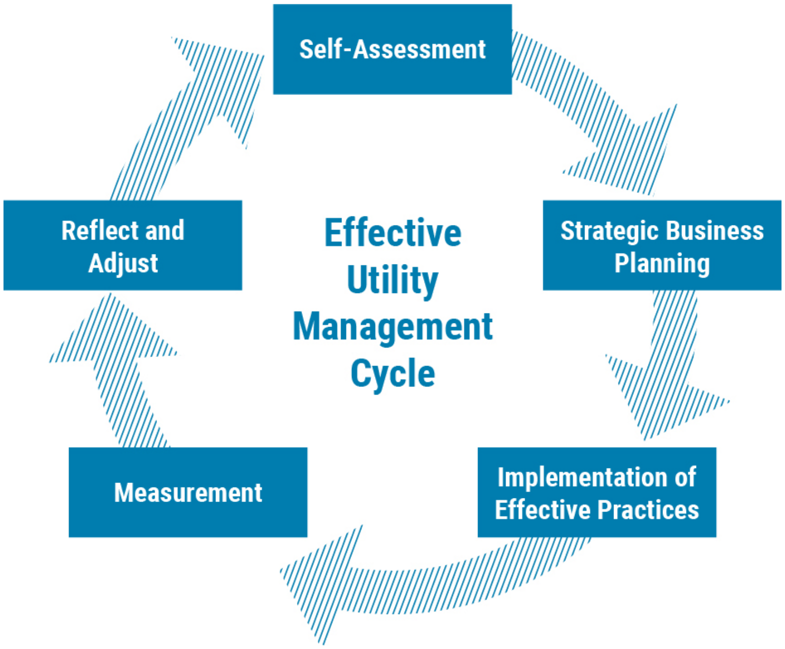
The goal of Effective Utility Management is to establish high-achieving systems and approaches for each Attribute. Ultimately, utilities should strive to improve performance for all Attributes until each can be charted in the lower half of the table (high achieving). Utility managers may wish to focus on one or a few Attributes at a time, aiming to eventually ensure that all Attributes have been addressed and improved upon over time.

Examining the results of the charting exercise in Step 3 can help identify Attributes for focused attention. Attributes that graph into the orange shaded quadrant are both very important (ranked 1-4), and have low achievement (rated 4-5), and would typically be selected as the highest priority Attribute areas for moving forward with improvement actions. Attributes that graph into the yellow shaded area indicate medium importance, and a moderate level of current achievement; these would typically be selected as additional strong candidates for improvement efforts.

Attributes that fall in the lower left-hand quadrant are both important and high-achieving areas for the utility. Some utilities may choose to focus on these areas to continue further improving upon important and high-achieving areas, due to their long-term importance (e.g., water resource adequacy). Specifically examining these areas may also help a utility identify success factors which would be helpful in addressing areas needing improvement. Others may choose to focus on Attributes that would lead to early successes to build confidence in effecting change, Attributes that maximize benefit relative to the utility's key goals, or Attributes that minimize risks (e.g., fines, penalties, lawsuits, poor public perception).

The choice to embark on improvements in one or more areas is up to the judgment of utility managers, and may also involve consideration of resources (staff and financial), leadership support, and other competing activities. Applying strategic business planning, measurement, and other Keys to Management Success is very important for moving each Attribute over time to the "high-achievement" quadrants.

V. Getting to Work: Implementation of Effective Utility Management


Self-Assessment
Strategic Business Planning
Implementation of Effective Practices
Measurement
Reflect and Adjust
Effective Utility Management Cycle

This section focuses on the specific steps that utilities are encouraged to go through to implement Effective Utility Management. The section includes a description of each element of the Effective Utility Management (EUM) cycle, and explains how utilities can take the results of their self-assessment, identify and implement effective practices, measure progress in priority Attribute areas, and do this through an improvement plan.

The EUM self-assessment (see page 11 for more information) serves as a comprehensive starting point for utilities, and the EUM cycle reflects how a utility's self-assessment results can build into a continual improvement management process. **Continual improvement** is one of the five Keys to Management Success for Effective Utility Management, and it operates throughout and supports the entire EUM cycle. The water sector is a rapidly evolving world, and utilities must stay abreast of new technologies, changes in the workforce, transforming customer needs, and much more. To adapt to these shifts, an effective utility must continually assess its performance and priorities, update its strategic plan, and make adjustments where necessary.

Two other Keys are reflected directly in the EUM cycle, **strategic business planning** and **measurement**; these are explained in greater detail later in this section. The two remaining Keys are also important to supporting all aspects of the EUM cycle: **leadership** and **knowledge management**. Leadership can exist at any level of a utility's organizational structure, and can encourage and enable active participation in an Effective Utility Management culture. Knowledge management supports the critical information and operating needs of each step of the cycle of Effective Utility Management. All five of the Keys to Management Success (see page 8 for more information) are integral to Effective Utility Management, and they work in tandem with the Ten Attributes (see page 4 for more information) to support successful utilities.

Beginning with the **self-assessment** exercise in **Section IV**, the EUM cycle is a self-reinforcing progression of assessment, planning, implementation, measurement, and adjusting over time. Each element of the cycle is described below.

Strategic Business Planning

Following completion of the self-assessment, utilities will now have a holistic picture of their current performance and priorities for the future relative to the Ten Attributes. Using these results as a starting point, a utility can begin to move through a strategic business planning process. Strategic business planning provides a framework for decision making and planning for the future. A strategic business plan could include, or be complemented by, an asset management plan and a financial plan for the utility.

Implementation of Effective Practices

After the utility has determined its priority Attribute areas for improvement and established a vision, goals, and objectives for the future through its strategic business plan, it is time to identify and implement effective practices linked to the Attributes in support of these objectives. Effective practices can also be identified in many ways: through learning activities (e.g., conferences, training events, webinars), through interactions and benchmarking activities with other utilities, and through resources created specifically to guide utilities in this area.

Two key resources to help utilities link the Attributes to specific practices are *Moving Toward Sustainability: Sustainable and Effective Practices for Creating Your Water Sector Roadmap,* developed by EPA with extensive input from water sector leaders, and *Performance Benchmarking for Effectively Managed Utilities* (Water Research Foundation), also prepared with extensive utility participation. Both are available at www.WaterEUM.org.

Measurement

To gauge performance and progress on the utility's strategic plan and practice implementation, the next step in the cycle is to establish performance measures relative to key activities. The adage of "you can't improve what you don't measure" applies here. Measurement is a key focus of this *Primer*, with approaches and example measures that utilities can implement addressed in greater depth later in this section and in **Appendix C**.

Reflect and Adjust

At regular intervals, the utility should reflect on its progress toward the goals set forth in its strategic business plan and its improvement plan relative to the Attributes, and determine if adjustments in course are needed, accounting for any changes in the utility's operating context.

Utilities can implement the cycle of Effective Utility Management in a variety of ways. It can be integrated into processes already in place as a part of the utility's operations and management, incorporated into a long-term planning process, or undertaken independently. A short guide for creating an improvement plan based on the self-assessment results follows at the end of this section.

Measuring Performance

Measuring performance is one of the keys to utility management success. This section of the *Primer* provides ideas about how to approach measurement and then offers measures for each Attribute to help utilities understand their current status and measure their progress.

Approaching Measurement

There are two general approaches to performance measurement: internal and external benchmarking. This *Primer* focuses on internal performance measurement. Internal performance measurement focuses on evaluating current internal utility performance status and trends. A robust measurement system will be built around a combination of leading, lagging, and coincidental performance indicators.

- **Leading indicators** provide an indication of the future state of a performance parameter of keen interest to the utility – for example an increase in near misses relative to safety violations can foretell of an increased risk of workplace injuries. Leading indicators provide a utility with the diagnostic ability to proactively manage for its desired performance outcomes. *Leading indicators drive preventative actions.*
- **Lagging indicators** typically reflect a performance parameter of keen interest to a utility (such as compliance rate or water quality conditions) while, at the same time providing performance information that can only be reacted to, making it sometimes challenging to proactively adjust operations before performance moves into an unacceptable range. These indicators, however, are critical to an overall measurement system as they typically focus on key performance outcomes that the utility, by necessity, must document (e.g., compliance with permit limits). *Lagging indicators drive immediate, corrective actions that could have been prevented by using leading and coincidental indicators.*

LEADING, LAGGING, AND COINCIDENTAL INDICATORS

A real-life example of applying indicators when analyzing body mass:

Lagging: At the end of the day, stepping on a scale and recording your weight.

Leading: Tracking the number of calories consumed and the number of calories expended through exercise.

Coincidental: Analyzing the two measurements, calories consumed and calories expended holistically. This will allow you to predict that if calories go up and exercise goes down, you can expect an increase in weight.

- **Coincidental indicators** are a form of leading indicator that draws on the behavior of two or more parameters to signal the future state of a key performance parameter (such as phosphorus discharge concentration). These indicators are important to both proactive management of key performance outcomes, but also to conducting root cause analysis when key performance outcomes vary outside of desirable ranges. *Coincidental indicators drive proactive process control actions.*

Benchmarking is the overt comparison of similar measures or processes across organizations to identify best practices, set improvement targets, and measure progress within or sometimes across sectors. A utility may decide to engage in benchmarking for its own internal purposes or in a coordinated fashion with others.

While performance measures should be tailored to the specific needs of your utility, the following guidelines can help you identify useful measures and apply them effectively.

1. Select measures that support the organization's strategic objectives, mission, and vision, as well as the ten Attributes.
2. Select the right number, level, and type of measures for your organization. Consider how measures can be integrated as a cohesive group (e.g., start with a small set of measures across broad categories and increase number and specificity over time as needed), and consider measures that can be used by different audiences within the organization.
3. Measuring performance will not necessarily require additional staff, but will require resources. Allocate adequate resources to get the effort off to a good start, and fine tune over time to balance the level of measurement effort with the benefit to the organization.
4. Develop clear, consistent definitions for each measure. Identify who is responsible for collecting the data, and how the data will be tracked and reported.
5. Engage the organization at all levels in developing, tracking, and reporting measures, but also assign someone in the organization the role of championing and coordinating the effort.
6. Set targets rationally, based on criteria such as customer expectations, improvement over previous years, industry performance, or other appropriate comparisons. Tie targets to improving performance in the Attributes.
7. Select and use measures in a positive way to improve decision making, clarify expectations, and focus attention, not just to monitor, report, and control.
8. When selecting measures, consider how they relate to one another. Look for cause-and-effect relationships; for example, how improvements in product quality could result in increased customer satisfaction.
9. Develop an effective process to evaluate and respond to results. Identify how, when, and to whom you will communicate results.
10. Incorporate the "Plan-Do-Check-Act" cycle approach into evaluating both the specific measures and the system as a whole. Regularly review the performance measurement system for opportunities to improve.

*... **and remember to celebrate your measured and documented successes!***

Attribute-Related Measures

The list on the following page provides examples of targeted, Attribute-related measures. Taken as a whole, the measures provide a utility with a cohesive, approachable, and generally applicable starting place for gauging progress relative to the Ten Attributes. The list, for brevity, contains measure "headlines" for each

Attribute. Utilities should also reference information in **Appendix C**, which provides further explanation and, where applicable, example calculations.

You can choose and tailor the measures to your own needs and unique, local circumstances. They are intended for your own internal use, even as certain measures (e.g., those noted as Benchmarking Performance Indicators) can support benchmarking purposes. In these cases, the measures have been selected because they are relevant to the Attributes, have been tested and are in use by utilities, are supported by reference information useful for implementation, and generally can act as a good starting point for Attribute-related progress assessment.

The measures presented are both quantitative and qualitative. Most are quantitative, focus on outcomes typically of interest to utility managers (e.g., compliance rate), and include generally applicable example calculations. The qualitative "measures" encourage active assessment of the practices in place to support effective management in each Attribute area. These are mostly "activity measures" and typically have a "yes/no" format. Like the Attributes themselves, certain measures focus on core utility operations. Several measures reflect emerging utility issues, challenges, or opportunities that have received increasing attention from a growing number of utility managers. Other measures may reflect broader interests that are worthy of consideration from a broader community perspective.

List of Attribute-Related Utility Measures

The list below includes a limited number of example measures that can be used to assess performance in each of the Attribute areas. See **Appendix C** for measure descriptions and details.

Product Quality

1. Regulatory compliance
2. Service delivery

Customer Satisfaction

1. Customer complaints
2. Customer service delivery
3. Customer satisfaction

Employee and Leadership Development

1. Employee retention and satisfaction
2. Management of core competencies
3. Workforce development

Operational Optimization

1. Resource optimization
2. Water management efficiency

Financial Viability

1. Budget management effectiveness
2. Financial procedure integrity
3. Bond ratings
4. Rate adequacy

Infrastructure Stability

1. Asset inventory
2. Asset (system) renewal/replacement
3. Water distribution/collection system integrity
4. Infrastructure planning and maintenance

Enterprise Resiliency

1. Recordable incidents of injury or illnesses
2. Insurance claims
3. Risk assessment and response preparedness
4. Ongoing operational resiliency
5. Operational resiliency under emergency conditions

Community Sustainability

1. Watershed-based infrastructure planning
2. Green infrastructure
3. Greenhouse gas emissions
4. Service affordability
5. Community economic development

Water Resource Sustainability

1. Water supply adequacy
2. Supply and demand management
3. Watershed sustainability

Stakeholder Understanding and Support

1. Stakeholder consultation
2. Stakeholder satisfaction
3. Internal benefits from stakeholder input
4. Comparative rate rank
5. Media/press coverage
6. Partnering in your community

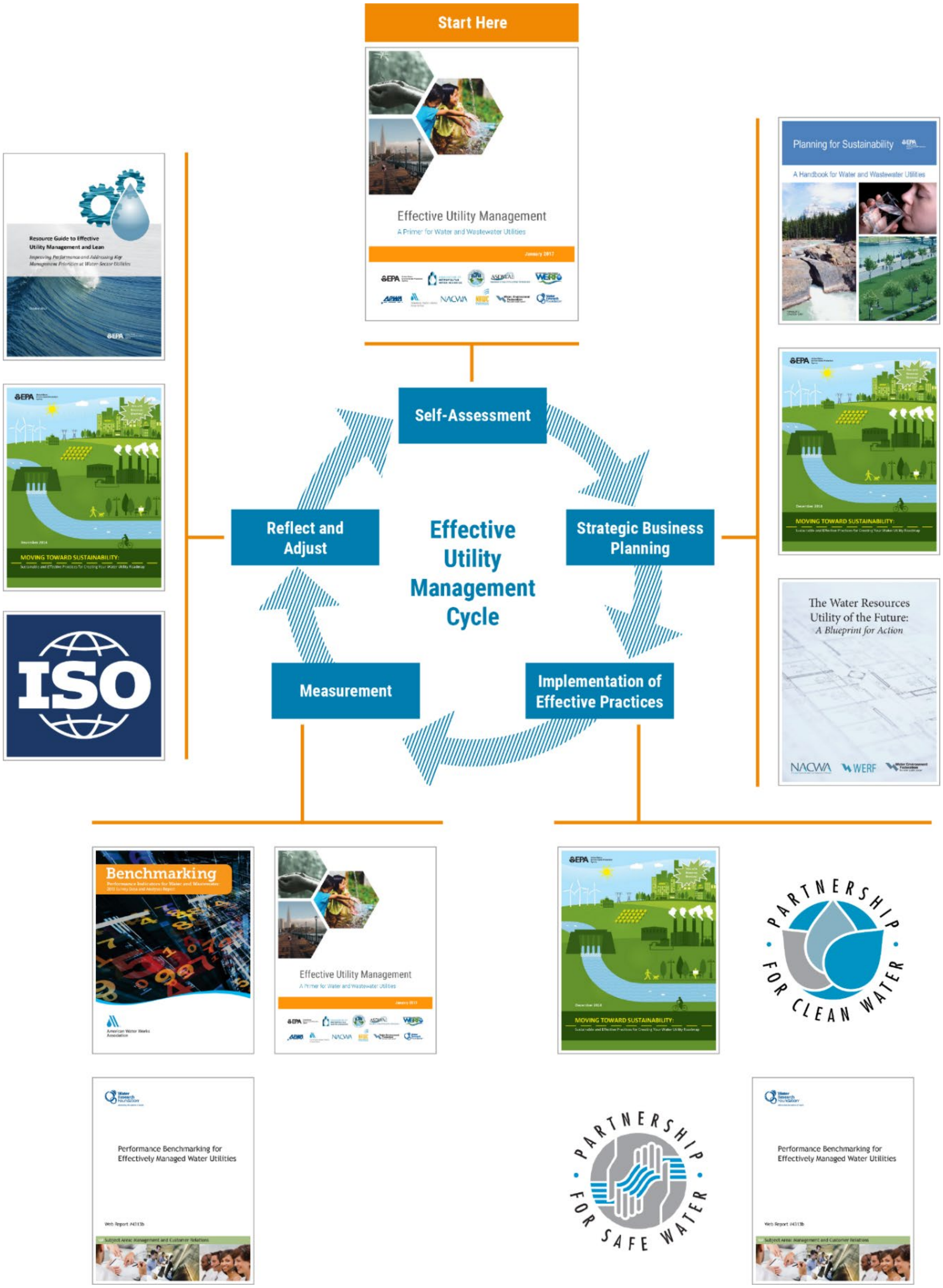
Resources to Support Effective Utility Management Implementation

Effective Utility Management is designed as a broad framework to complement and enhance other prominent utility management initiatives currently in use. In addition to this EUM *Primer*, a wide range of resources exist across the water sector to support each step of the cycle of Effective Utility Management. The resources listed below are examples of materials that can support each step of the EUM cycle.

- **Benchmarking Performance Indicators for Water and Wastewater** (American Water Works Association)
- **Moving Toward Sustainability: Sustainable and Effective Practices for Creating Your Water Utility Roadmap** (U.S. EPA)
- **The Partnership for Clean Water** (American Water Works Association)
- **The Partnership for Safe Water** (American Water Works Association)
- **Performance Benchmarking for Effectively Managed Water Utilities** (Water Research Foundation)
- **Planning for Sustainability: A Handbook for Water and Wastewater Utilities** (U.S. EPA)
- **Resource Guide to Effective Utility Management and Lean: Improving Performance and Addressing Key Management Priorities at Water-Sector Utilities** (U.S. EPA)
- **The Water Resources Utility of the Future: A Blueprint for Action** (National Association of Clean Water Agencies, Water Environment & Reuse Foundation, and Water Environment Federation)

THE DIAGRAM ON THE FOLLOWING PAGE IS A DEPICTION OF HOW EACH RESOURCE FROM THE LIST CAN RELATE TO THE VARIOUS STEPS IN THE CYCLE.

HOW IT FITS TOGETHER



Start Here

Self-Assessment

Strategic Business Planning

Implementation of Effective Practices

Measurement

Reflect and Adjust

Effective Utility Management Cycle

Effective Utility Management
A Primer for Water and Wastewater Utilities
Resource Guide to Effective Utility Management and Lean
Improving Performance and Addressing Key Management Priorities at Water-Sector Utilities
MOVING TOWARD SUSTAINABILITY:
ISO
Planning for Sustainability
A Handbook for Water and Wastewater Utilities
The Water Resources Utility of the Future: A Blueprint for Action
NACWA
WERF
Benchmarking
Performance Indicators for Water and Wastewater
Performance Benchmarking for Effectively Managed Water Utilities
PARTNERSHIP FOR CLEAN WATER
PARTNERSHIP FOR SAFE WATER

Creating an Improvement Plan

Once you have chosen to improve one or more Attributes, the next step is to develop and implement a plan for making the desired improvements. Improvement plans support the implementation of effective practices in your chosen attribute area(s). An effective improvement plan will:

Set Near- and Long-term Goals	Set goals as part of the improvement plan to help define what is being worked toward. Near- and long-term goals for the utility should be linked to the strategic business plan, asset management plan, and financial plan. Goals should also be "SMART." **S – Specific:** *What exactly will be achieved?* **M – Measurable:** *Can you measure whether you are achieving the objective?* **A – Assignable:** *Can you specify who will be responsible for each segment of the objective?* **R – Realistic:** *Do you have the capacity, funding, and other resources available?* **T – Time-Based:** *What is the timeframe for achieving the objective?*
Identify Effective Practices	Each Attribute area for improvement will be supported by effective practices implemented by the utility. A substantial number of water sector resources exist that detail effective utility practices for each of the Attributes.
Identify Resources Available and Resources Needed	For each practice/activity to be implemented as part of the improvement plan, identify resources (financial, informational, staff, or other) that exist on-hand, and those that are needed, to support implementation.
Identify Challenges	For the overall improvement plan and for specific practices/activities to be implemented, identify key challenges that will need to be addressed.
Assign Roles and Responsibilities	For each improvement action, identify roles and responsibilities for bringing the implementation to completion.
Define a Timeline	Establish start date, milestones, and a completion target for each activity/improvement action.
Establish Measures	Establish at least one (or more) measure of performance for items to be implemented under the improvement plan.

VI. Utility Management Resources

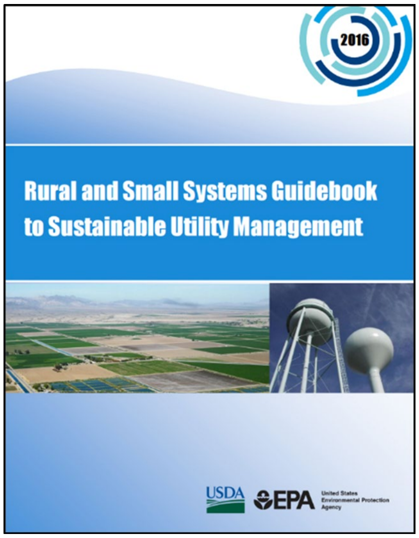
As a companion resource to this Primer, the Collaborating Organizations developed an online Resource Toolbox, which offers additional information and guidance on effective utility management. The Toolbox provides a compilation of resources from the eleven Collaborating Organizations designed to help the water and wastewater utility community further improve the management of its infrastructure.

The Resource Toolbox is organized according to the Ten Attributes of Effectively Managed Water Sector Utilities and five Keys to Management Success, providing a set of resources relevant to each Attribute and Key. The Toolbox also includes information on where to find these resources.

The Resource Toolbox is located at www.WaterEUM.org.

Effective Utility Management for Small and Rural Systems

Small and rural utilities seeking to implement EUM are served by a variety of resources specifically designed for them, including the *Rural and Small Systems Guidebook to Sustainable Utility Management.* The *Guidebook* is a resource jointly developed by EPA and the United States Department of Agriculture (USDA), which adapts the Ten Attributes for use by small and rural systems.



2016

Rural and Small Systems Guidebook to Sustainable Utility Management

USDA EPA United States Environmental Protection Agency

VII. For More Information

This Primer was developed through a collaborative partnership with the following groups. More information about this partnership can be found on their websites or by contacting specific individuals directly.

Association of Clean Water Administrators
Julia Anastasio
Executive Director & General Counsel
1634 I Street NW, Suite 750
Washington DC 20006
janastasio@acwa-us.org
202.756.0600
www.acwa-us.org

American Public Works Association
Anne Jackson
Director of Sustainability
1275 K Street NW, Suite 750
Washington DC 20005
ajackson@apwa.net
202.218.6750
www.apwa.net

Association of State Drinking Water Administrators
Bridget O'Grady
Policy and Legislative Affairs Manager
1401 Wilson Blvd.
Arlington, VA 22209
bogrady@asdwa.org
703.812.9505
www.asdwa.org

American Water Works Association
Cynthia Lane
Director, Engineering and Technical Services
6666 W. Quincy Ave.
Denver, CO 80235
clane@awwa.org
303.347.6176
www.awwa.org

Association of Metropolitan Water Agencies
Carolyn Peterson
Director of Communications and Public Affairs
1620 I Street, NW
Washington DC 20006
peterson@amwa.net
202.331.2820
www.amwa.net

National Association of Clean Water Agencies
Chris Hornback
Chief Technical Officer
1816 Jefferson Place, NW
Washington DC 20036
chornback@nacwa.org
202.833.9106
www.nacwa.org

National Association of Water Companies
Petra Smeltzer
Director of Government Relations
2001 L Street NW, Suite 850,
Washington DC 20036
petra@nawc.com
202.322.8089
www.nawc.org

U.S. Environmental Protection Agency
Jim Horne
Sustainability Program Manager
Office of Wastewater Management
1200 Pennsylvania Avenue, NW
Room 7111 – WJC East
Washington DC 20460
horne.james@epa.gov
202.564.0571
www.epa.gov/sustainable-water-infrastructure

Water Environment Federation
Matt Ries
Chief Technical Officer
601 Wythe Street
Alexandria, VA 22314-1994
mries@wef.org
703.684.2406
www.wef.org

Water Environment & Reuse Foundation
Allison Deines
Director of Special Projects
1199 N Fairfax St, Suite 410
Alexandria, VA 22314-1177
adeines@werf.org
571.384.2116
www.werf.org

Water Research Foundation
Linda Reekie
Research Manager
6666 West Quincy Avenue
Denver, Colorado 80235-3098
lreekie@waterrf.org
303.734.3423
www.waterrf.org

VIII. Appendix A: Key Definitions

Attribute: A basic building block of effective utility management for water sector utilities. Attributes describe characteristics or outcomes of a utility that indicate effective performance.

Benchmarking: The comparison of similar processes or measures across or within organizations and/or sectors to identify best practices, set improvement targets, and measure progress.

Continual Improvement: A systematic approach that supports ongoing efforts to improve products, services, or processes, through incremental steps over time or through "breakthrough" advances all at once.

Effective Utility Management: A comprehensive water sector utility performance assessment and management framework, endorsed by the U.S. Environmental Protection Agency and ten national water sector associations dedicated to improving products and services, increasing community support for water services, and ensuring a strong and viable utility into the future.

Gap analysis: Defining the present state of an enterprise's operations, the desired or "target" state, and the gap between them.

Knowledge Management: The multi-disciplinary process of creating, sharing, using, managing, and preserving the knowledge and information of an organization.

Life-cycle cost: The total of all internal and external costs associated with a product, process, activity, or asset throughout its entire life cycle – from raw materials acquisition to manufacture/construction/installation, operation and maintenance, recycling, and final disposal.

Performance measurement: Evaluation of current status and trends; can also include comparison of outcomes or outputs relative to goals, objectives, baselines, targets, standards, other organizations' performance or processes (typically called benchmarking), etc.

Operations and maintenance expenditure: Expenses used for day-to-day operation and maintenance of a facility.

Operating revenue: Revenue realized from the day-to-day operations of a utility.

Performance measure: A particular value or characteristic designated to measure input, output, outcome, efficiency, or effectiveness.

Source water protection: Efforts to prevent water quality degradation in streams, rivers, lakes, or underground aquifers used as public drinking water supplies.

Standard operating procedure: A prescribed set of actions to be followed routinely; a set of instructions having the force of a directive, covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness.

Strategic plan: An organization's process of defining its goals and strategy for achieving those goals. This often entails identifying an organization's vision, goals, objectives, and targets over a multi-year period of time, as well as setting priorities and making decisions on allocating resources, including capital and people, to pursue the identified strategy.

Stewardship: The careful and responsible management of something entrusted to a designated person or entity's care; the responsibility to utilize its resources properly, including its people, property, and financial and natural assets.

Sustainability: The use of natural, community, and utility resources in a manner that satisfies current needs without compromising future needs or options.

Watershed health: The ability of ecosystems to provide the functions needed by plants, wildlife, and humans, including the quality and quantity of land and aquatic resources.

IX. Appendix B: Self-Assessment

Step 1: Assess Current Conditions

Assess current conditions by rating your utility's systems and approaches and current level of achievement for each Attribute, using a 1 (high achievement) to 5 (low achievement) scale. Consider the degree to which your current management systems effectively support each of the Attributes and their component parts. Consider all components of each Attribute and gauge your rating accordingly. Use these descriptions to guide your rating. You will note that each Attribute has several components represented by the bullet points listed for each.

Your rating can either reflect the lowest level of achievement of all of the bullet points for that Attribute (for example, if you believe that your achievement in one of the bullet points for that Attribute was "5," but another bullet point you rated as "2," your rating for achievement under that Attribute would be "5"), or an average across all of the bullet points for that Attribute. For whatever approach you choose to use when rating, make sure to be consistent in this approach across all Attributes. Mark your answers in the Step 1 column of the table on the next page.

Rating	Description
1.	Effective, systematic approach and implementation; consistently achieve goals.
2.	Workable systems in place; mostly achieve goals.
3.	Partial systems in place with moderate achievement, but could improve.
4.	Occasionally address this when specific need arises.
5.	No system for addressing this.

Step 2: Rank Importance of Attributes

Rank the importance of each Attribute to your utility, based on your utility's vision, goals, and specific needs. The ranking should reflect the interests and considerations of all stakeholders (managers, staff, customers, regulators, elected officials, community and watershed interests, and others).

There are Ten Attributes; considering long-term importance to your utility, rank the most important Attribute 1, the second most important 2, and so on. The least important Attribute would be ranked 10. Your ranking of each Attribute's importance may be influenced by current or expected challenges in that particular area, recent accomplishments in addressing these issues, or other factors. Importance ranking is likely to change over time as internal and external conditions change.

Mark your answers in the Step 2 column of the table on the next page. As you fill in numbers, please note that your analysis for Step 1 (rating achievement) should be separate and independent from your analysis for Step 2 (ranking importance).

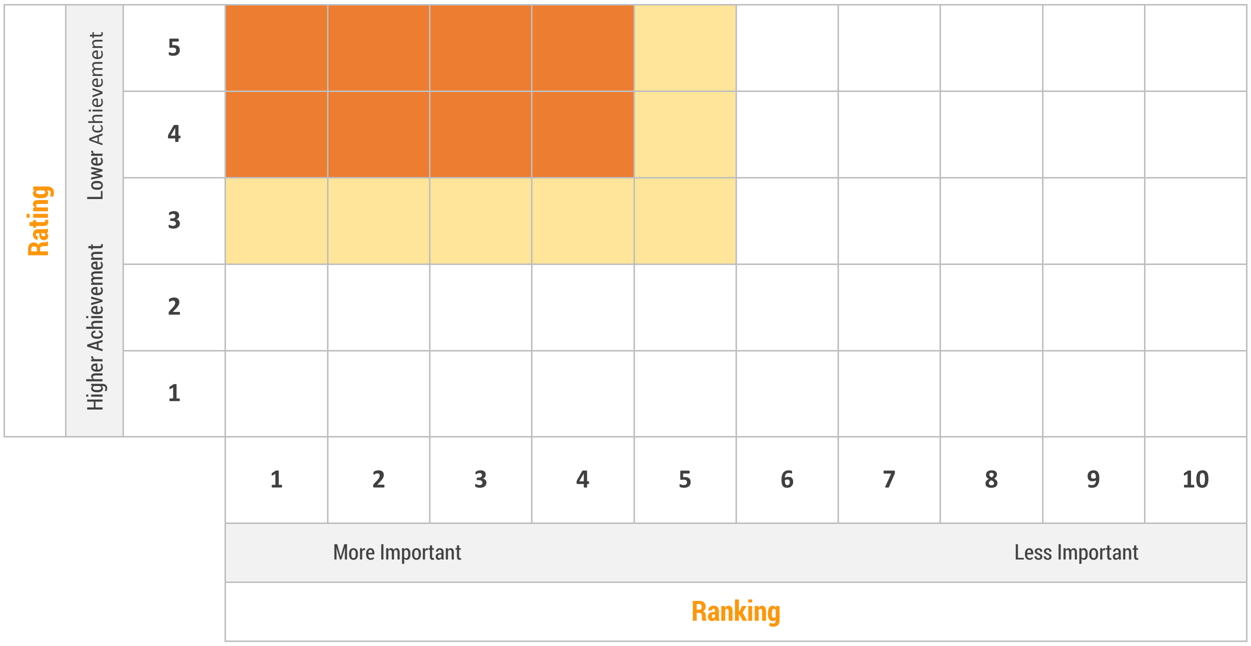
Attribute	Attribute Components	Step 1: Rate Achievement (1-5)	Step 2: Rank Importance (1-10)
Product Quality (PQ)	• Meets or exceeds regulatory and reliability requirements. • Operates consistent with customer, public health, economic, and ecological needs.		
Customer Satisfaction (CS)	• Provides reliable, responsive, and affordable services. • Receives timely customer feedback. • Is responsive to customer needs and emergencies. • Provides tailored customer service and outreach to a range of customer groups (e.g., residential, commercial, industrial, and newly emerging groups such as high-strength waste producers or power companies)		
Employee and Leadership Development (ED)	• Recruits, develops, and retains a competent, safety-focused workforce. • Is a collaborative organization dedicated to continual learning, improvement, and adaptation. • Implements procedures for institutional knowledge retention, workplace safety, and continual learning (e.g., standard operating procedures). • Invests in/provides opportunities for professional and leadership development. • Supports an integrated and well-coordinated senior leadership team.		
Operational Optimization (OO)	• Conducts ongoing performance improvements informed by performance monitoring. • Minimizes resource use and loss from day-to-day operations. • Is aware of and adopts in a timely manner operational and technology improvements, including operational technology and information technology. • Manages and utilizes data from automated and smart systems.		

Attribute	Attribute Components	Step 1: Rate Achievement (1-5)	Step 2: Rank Importance (1-10)
Financial Viability (FV)	• Understands and plans for full life-cycle cost of utility. • Effectively balances long-term debt, asset values, operations and maintenance expenditures, and operating revenues. • Sets predictable and adequate rates to support utility current needs and plans to invest in future needs, taking into account affordability and the needs of disadvantaged households when setting rates. • Understands opportunities for diversifying revenue and raising capital.		
Infrastructure Strategy and Performance (IS)	• Understands the condition of and costs associated with critical infrastructure assets. • Maintains and enhances assets over the long-term at the lowest possible life-cycle cost and acceptable risk. • Coordinates repair efforts within the community to minimize disruptions. • Plans infrastructure investments consistent with community needs, anticipated growth, system reliability goals, and with a robust set of adaptation strategies.		
Enterprise Resiliency (ER)	• Works together with staff internally and coordinate with external partners to anticipate and avoid problems. • Proactively establishes tolerance levels and effectively manages risks (including legal, regulatory, financial, environmental, safety, security, cyber, knowledge-loss, talent, and natural disaster-related). • Plans for and actively manages to maintain business continuity.		

Attribute	Attribute Components	Step 1: Rate Achievement (1-5)	Step 2: Rank Importance (1-10)
Community Sustainability (SU)	• Actively leads in promoting and organizing improvements to community and watershed health within utility and with external community partners. • Actively leads in promoting welfare within the community for disadvantaged households. • Uses operations to enhance natural environment. • Efficiently uses water and energy resources, promotes economic vitality, and engenders overall community improvement. • Maintains and enhances ecological and community sustainability including pollution prevention, watershed and source water protection.		
Water Resource Sustainability (WS)	• Ensures water availability through long-term resource supply and demand analysis, conservation, fit for purpose water reuse, integrated water resource management, watershed management and protection, and public education initiatives. • Manages operations to provide for long-term aquifer and surface water sustainability and replenishment. • Understands and plans for future water resource variability (e.g., changing weather patterns, including extreme events, such as drought and flooding).		
Stakeholder Understanding and Support (SS)	• Engenders understanding and support from oversight bodies, community and watershed interests, and regulatory bodies for service levels, rate structures, operating budgets, capital improvement programs, and risk management decisions. • Actively engages in partnerships and involves stakeholders in the decisions that will affect them. • Actively promotes an appreciation of the true value of water and water services, and water's role in the social, economic, public and environmental health of the community.		

Step 3: Graph Results

Graph each Attribute based on your rating and ranking.

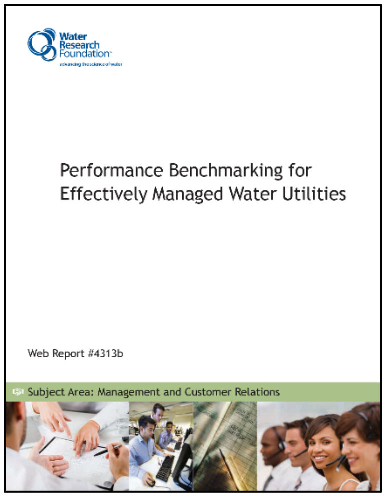


X. Appendix C: Attribute-Related Water Utility Measures

Performance measurement is critical to effectively managing a utility. This section of the *Primer* provides detailed information on a range of measures that utilities can consider, including descriptions and example calculations and questions.

In addition to the example measures described in this section, utilities can reference a variety of resources available to the sector which provide additional specific measures for a variety of practices. Resources available to utilities include:

- **Benchmarking Performance Indicators for Water and Wastewater Utilities** (American Water Works Association)
- **Effective Utility Management Benchmarking Tool** (Water Research Foundation)

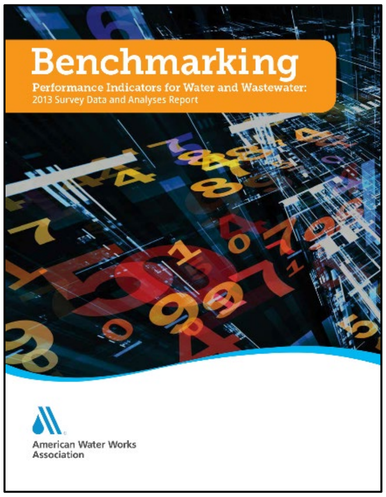


Water Research Foundation

Performance Benchmarking for
Effectively Managed Water Utilities

Web Report #4313b

Subject Area: Management and Customer Relations



Benchmarking

Performance Indicators for Water and Wastewater:
2013 Survey Data and Analyses Report

American Water Works Association

For each of the Attributes, a variety of example calculations and questions are provided in this Appendix for use by water sector utilities. This is not meant to serve as an exhaustive list, but rather a starting point for utilities as they begin to think about how performance can be measured for each Attribute.

Product Quality

1. Regulatory compliance

Description: This measure assesses water product quality compliance, particularly with regard to 40 CFR Part 141 (the National Primary Drinking Water Regulations), the National Pollutant Discharge Elimination System, and any other relevant federal (Clean Water Act, Safe Drinking Water Act, etc.) or state statute/regulations and permit requirements. The scope can include the quality of all related products, including drinking water, fire suppression water, treated effluent, reused water, and biosolids (EPA 503 Regulations), as well as quality related to operating requirements such as pressure and number of sewer overflows.

Example performance measures:

- Drinking water compliance rate (percent): 100 X (number of days in full compliance for the year ÷ 365 days). *This is a Benchmarking Performance Indicator*.

- Wastewater treatment effectiveness rate (percent): 100 X (365 – total number of noncompliance days ÷ 365 days). *This is a Benchmarking Performance Indicator.*
- Number, type, and frequency of "near (compliance) misses": For example, reaching 80-95% of allowable levels of "X" during reporting period, typically per month. Tracking this type of measure could be used to improve performance in these "near miss" areas before violations occur.

2. Service delivery

Description: This measure assesses delivery of quality service based on utility-established objectives and service level targets.

Example performance measures:

- Drinking water flow and pressure (percent): 100 X [number of customers with less than (flow of "X" gallons per minute (gpm) and pressure of "Y" pounds per square inch (psi)—levels set by utility) ÷ total number of customers] (during reporting period, typically per month).
- Fire suppression water flow and pressure (percent): 100 X [hours of time when (flow of "X" gpm and pressure of "Y" psi—levels set by utility) is available for fire suppression at maximum day demand ÷ total number of hours when fire suppression water should be available at maximum day demand] (during reporting period, typically per month).
- Service interruptions (percent): 100 X (number of active account customers experiencing a service interruption of greater than 1 hour ÷ total number of customers during reporting period) (typically per month). Note: the utility may elect to measure planned and unplanned interruptions separately.
- Water quality goals met/not met: Number of days in reporting period (typically one month) where utility-defined beyond-compliance targets are met/not met.
- Sewer backups (amount and percent): Number of customers experiencing backups each year; 100 X (number of customers experiencing backups each year ÷ total number of customers).
- Sewer overflows: Number of sewer overflows per 100 miles of collection system piping, or number of sewer overflows per million gallons treated.
- Water reuse (amount and percent):
  - Amount: Amount of water supplied that is from reused/recycled sources.
  - Percent: 100 X (amount of water supplied that is from reused/recycled water ÷ total amount of water supplied).
  - Then, as desired, these amounts can be broken into recipients/applications (e.g., irrigation, agriculture, industrial processes, etc.).
- Biosolids put to beneficial use (percent): 100 X (amount of biosolids produced that are put to a beneficial use ÷ total amount of biosolids produced) (in wet tons per year).
- Percent of recovered resources that meet customer specifications or regulatory requirements: 100 X (amount of efficiently recovered material ÷ total amount of potentially recovered material).

Customer Satisfaction

1. Customer complaints

Description: This measure assesses the complaint rates experienced by the utility, with individual quantification of customer service and core utility service complaints (note that "service complaints" would not include routine service requests by customers).[1] As a "passive measure," it will not likely be numerically representative (i.e., a statistically valid customer sample group) and is a "starting point" measure for understanding customer service problems.

Example performance measures:

- Number of complaints per 1,000 customers (or other appropriate value based on size of population served) per reporting period, recorded as either customer service or technical quality complaints.
  - Customer service complaint rate: 1,000 X (customer service associated complaints ÷ number of active customer accounts). *This is a Benchmarking Performance Indicator*.
  - Technical quality complaint rate: 1,000 X (technical quality associated complaints ÷ number of active customer accounts). *This is a Benchmarking Performance Indicator*.

For both calculations, utilities may wish to subcategorize complaints by type and aspect (e.g., customer service into billing, problem responsiveness, interruptions, etc., and technical quality into service deficiencies such as taste, odor, appearance, flow/pressure, etc.) and by type of customer (e.g., residential, industrial, commercial, etc.)

2. Customer service delivery

Description: This measure requires the utility, based on internal objectives and customer input, to set desirable customer service levels, then determine an appropriate (target) percentage of time to meet the performance levels. Once established, the utility can track how often it meets the service levels, helping the utility to determine how well customer needs are being satisfied (e.g., have 95 percent of service calls received a response within 60 minutes). A utility can average across individual measures to determine the overall percentage of service level commitments met.

Example performance measures:

- Call responsiveness (percent): 100 X (number of calls responded to within "X" minutes ÷ total number of calls during reporting period) (typically per month).
- Error-driven billing adjustment rate (percent): 100 X (number of error-driven billing adjustments during reporting period ÷ number of bills generated during reporting period). *This is a Benchmarking Performance Indicator*.
- Service start/stop responsiveness (percent): 100 X (number of stop/start service orders processed within "X" days ÷ total number of stop/start service orders during reporting period).

[1] From AWWA and AwwaRF, *Selection and Definition of Performance Indicators for Water and Wastewater Utilities*, p. 41. 2004. Note: This material is copyrighted and any reprinting must be by permission of the American Water Works Association.

- First call resolution (percent): 100 X (number of calls for which problem was resolved/fixed/scheduled to be fixed at the time of the first call ÷ total number of calls during reporting period).

3. Customer satisfaction

Description: This is an overarching customer satisfaction measure based on requested customer feedback (surveys), not calls received or internal customer satisfaction service level commitments. A utility can measure customer satisfaction immediately after service provision or use a periodically performed, more comprehensive customer satisfaction survey. After-service surveys are simpler and easier for the utility to develop and implement without professional advice, but they tend to over represent the most satisfied (e.g., those who just received service) and the most dissatisfied (e.g., those who just called with complaints) customers. Comprehensive surveys can provide statistical validity enabling extrapolation to the population served. A utility can verify survey information through customer conversations, either as follow up to a survey, during public meetings or focus groups, or by some other method (e.g., individual telephone calls).

Example performance measures:

- Overall customer satisfaction: Percent of positive or negative customer satisfaction survey responses based on a statistically valid survey or on an immediately after-service survey. Satisfaction responses can be divided into categories such as: highly satisfied/satisfied/moderately satisfied/unsatisfactory; exceeding expectations/meeting expectations/not meeting expectations; numerical scales (e.g., 1-5); or other divisions. Customer satisfaction information is often also gathered and assessed by topic areas such as product quality, service reliability, billing accuracy, customer service, costs/rates/value, crew courtesy, notification around street construction/service interruptions, etc.

Employee and Leadership Development

1. Employee retention and satisfaction

Description: This measure gauges a utility's progress toward developing and maintaining a competent and stable workforce, including utility leadership.

Example performance measures:

- Employee turnover rate (percent): 100 X (number of employee departures ÷ total number of authorized positions per year). Can be divided into categories such as:
  - Voluntary turnover (percent): 100 X (number of voluntary departures ÷ total number of authorized positions per year). (Perhaps the best indicator of retention problems.)
  - Retirement turnover (percent): 100 X (number of retirement departures ÷ authorized positions per year). (Measures vulnerability to loss/retention of institutional knowledge.)
  - Experience turnover (percent): 100 X (number of years of experience represented by all departures ÷ total years of experience with the organization) (at the beginning of the year). (These are harder data to collect but provide a good assessment of institutional knowledge loss potential and therefore the need to retain/capture institutional knowledge.)

- Employee job satisfaction (percent): 100 X (number of employees with “X” job satisfaction level ÷ total number of employees) (based on implementation and monitoring over time of a comprehensive employee survey). Can be divided into work type or job classification categories, etc., and cover overall satisfaction and topics deemed relevant to longer-term employee satisfaction and retention, such as:
    - Compensation and benefits
    - Management
    - Professional development and long-term advancement opportunities
    - Work and teamwork
    - Procedures
    - Fairness and respect
    - Communication
    - Positive work environment
    - Recognition for achievements
- Employee salary competitiveness relative to market rate: Average percentile rank of employee salaries compared to salaries in surrounding service areas, as determined by a market rate comparison.

2. Management of core competencies

Description: This measure assesses the utility’s investment in and progress toward strengthening and maintaining employee core competencies.

Example performance measures:

- Presence of job descriptions and performance expectations: Percentage of classifications with current job descriptions and related performance expectations.
- Training hours per employee: Total of qualified formal training hours for all employees ÷ total FTEs (FTE = 2,080 hours per year of employee time equivalent) worked by employees during the reporting period. *This is a Benchmarking Performance Indicator*.
- Certification coverage (percent): 100 X (number of certifications achieved or maintained ÷ number of needed certifications per year) (across the utility).
- Employee evaluation results (assumes utility evaluates employee performance in a routine way and documents results): Results of employee evaluations (e.g., employee growth not clearly demonstrated, employee growth only demonstrated in certain areas or for certain labor categories, etc.).
- Presence of employee-focused objectives and targets: Percentage of employees with written employee-focused organizational objectives and targets.(Targets could be, for instance, related to quantity, quality, timeliness, or cost. A timeliness target could, for example, relate to the number of hours it takes on average to complete a routine task.)

3. Workforce development

Description: This measure assesses utility long-term workforce succession planning efforts to ensure critical skills and knowledge are retained and enhanced over time, particularly in light of anticipated retirement volume in coming years. Focus is on preparing entire groups or cohorts for needed workforce succession, including continued training and leadership development.

Example performance measures:

- Key position vacancies: Average time that critical-skill positions are vacant due to staff departures per vacancy per year.
- Key position internal/external recruitment (percent): 100 X (number of critical-skill positions that are filled internally (through promotion, transfer, etc. rather than outside recruitment) versus filled through outside recruitment ÷ total number of positions filled per year). (This will help the utility to understand if internal workforce development is covering long-term succession needs.)
- Long-term succession plan coverage (percent): 100 X (number of employees (or cohorts, work units, etc.) covered by a long-term workforce succession plan that accounts for projected retirements and other vacancies in each skill and management area ÷ total number of employees) (or cohorts, work units, etc.).
- Internal leadership development:
    - Percentage of staff and leadership positions with defined competencies.
    - Are internal or external leadership development/training/skills development opportunities provided to employees (yes/no)?

Operational Optimization

1. Resource optimization

Description: This measure examines resource use efficiency, including labor and material per unit of output or mile of collection/distribution system.

Example performance measures:

- Customer accounts per employee: Number of accounts ÷ number of FTEs. (FTE = 2,080 hours per year of employee time equivalent.) *This is a Benchmarking Performance Indicator*.
- MGD water delivered/processed per employee: Average MGD delivered/processed ÷ FTEs per year. *This is a Benchmarking Performance Indicator*.
- Chemical use per volume delivered/processed: Amount of chemicals used ÷ MG delivered/processed during reporting period. (Alternatively can use dollar amount spent on chemicals ÷ MG delivered/processed; in this case a rolling average for amount spent would account for periodic bulk purchases.)
- Energy use per volume delivered/processed: KWH ÷ MG delivered/processed during reporting period. (Alternatively can use dollar amount spent on energy ÷ MG delivered/processed.)
- O&M cost per volume delivered/processed: Total O&M cost ÷ MG delivered/processed during reporting period.

A utility can also apply the above resource use per volume delivered/processed calculations to resource use per mile (or 100 miles) of collection/distribution system, (i.e., chemical use per mile, energy use per mile, or O&M cost per mile).

2. Water management efficiency

Description: This measure assesses drinking water production and delivery efficiency by considering resources as they enter and exit the utility system.

Example performance measures:

- Production efficiency: Ratio of raw water volume taken into the treatment system to treated water produced.
- Meter function (percent): 100 X (total number of active billable meters minus stopped or malfunctioning meters ÷ total number of active billable meters).

Financial Viability

1. Budget management effectiveness

Description: This measure has short-term and long-term aspects. The short-term calculations are commonly used financial performance indicators, and the long-term calculation is a more comprehensive analytical approach to assessing budget health over the course of several decades.

Example performance measures:

Short-term (typically per year):

- Revenue to expenditure ratio: Total revenue ÷ total expenditures.
- O&M expenditures (percent): 100 X (O&M expenditures ÷ total operating budget).
- Capital expenditures (percent): 100 X (capital expenditures ÷ total capital budget).
- Debt ratio: Total liabilities ÷ total assets. Total liabilities are the entire obligations of the utility under law or equity. Total assets are the entire resources of the utility, both tangible and intangible. Utilities often have different debt-risk acceptability levels, thus the ratio itself should be considered within each utility's unique circumstances. *This is a Benchmarking Performance Indicator*.
- Current level of operating reserves as a percentage of goal.

Long-term:

- Life-cycle cost accounting: Has the utility conducted a life-cycle cost accounting analysis[2] that explicitly incorporates accepted service level risks, asset condition, budget needs based on the values (net present values) of utility current and future assets, etc., and made financial and budget management decisions accordingly (yes/no)?

[2] Section 707 of Executive Order 13123 defines life-cycle costs as, "…the sum of present values of investment costs, capital costs, installation costs, energy costs, operating costs, maintenance costs, and disposal costs over the life-time of the project, product, or measure." Life-cycle cost analysis (LCCA) is an economic method of project evaluation in which all costs arising from owning, operating, maintaining, and disposing of a [facility/asset] are considered important to the decision. LCCA is particularly suited to the evaluation of design alternatives that satisfy a required performance level, but that may have differing investment, operating, maintenance, or repair costs; and possibly different life spans. LCCA can be applied to any capital investment decision, and is particularly relevant when high initial costs are traded for reduced future cost obligations. See also: https://energy.gov/nepa/downloads/eo-13148-greening-government-through-leadership-environmental-management-2000, http://www.wbdg.org/resources/lcca.php.

2. Financial procedure integrity

Description: This measure gauges the presence of internal utility processes to ensure a high level of financial management integrity.

Example performance measures:

- Number of control deficiencies and material weaknesses reported on annual audits.
- Does the utility have financial accounting policies and procedures (yes/no)?
- Are financial results and internal controls audited annually (yes/no)?
- Have the number of control deficiencies and material weaknesses been reduced from previous audits (yes/no)?
- Does the utility have a formal policy for the bill collection process (yes/no)?

3. Bond ratings

Description: This measure uses bond ratings as a general indicator of financial viability; however, they are not always within a utility's control and are less important if a utility is not participating in capital markets. Smaller utilities often struggle to obtain high ratings. Even though a higher bond rating is desirable and this provides a general indicator of financial health, the bond rating should not be considered alone. It should be considered in light of other factors such as the other measures suggested for this Attribute.

Example performance measure:

- Bond ratings.
- Change in bond ratings: Does the change reflect the utility's financial management in a way that can and should be acknowledged and, if need be, addressed?

4. Rate adequacy

Description: This measure helps the utility to consider its rates relative to factors such as external economic trends, short-term financial management, and long-term financial health. It recognizes that a "one size fits all" calculation would not be realistic due to each utility's unique situation and the number of variables that could reasonably be considered. The following three questions prompt assessment of key components of rate adequacy.

Example performance measures:

- How do your rate changes compare currently and over time with the inflation rate and the Consumer Price Index (CPI) or Consumer Price Index for All Urban Consumers (CPI-U)? (Rate increases below CPI for very long may suggest rates are not keeping up with utility costs.) (Using a rolling rate average over time will adjust for short-term rate hikes due to capital or O&M spending needs.)
- Have you established rates that fully consider the full life-cycle cost of service and capital funding options? (See the life-cycle cost accounting discussion, above.)
- Does your utility maintain a rate stabilization reserve to sustain operations during cycles of revenue fluctuation, in addition to 60- (or 90-) day operating reserves?

Infrastructure Strategy and Performance

1. Asset inventory

Description: This measure gauges a utility's efforts to assess assets and asset conditions, as the first steps towards building a comprehensive asset management program.

Example performance measures:

- Inventory coverage (percent): 100 X (total number of critical assets inventoried within a reasonable period of time (e.g., 5-10 years) ÷ total number of critical assets). A utility will need to first define what it considers to be a critical asset. Typically, critical assets are those that you decide would have major consequences if they were to fail (major expense, system failure, safety concerns, etc.). A complete inventory will involve understanding the following for each asset:
  - Age and location;
  - Asset size and/or capacity;
  - Valuation data (e.g., original and replacement cost);
  - Installation date and expected service life;
  - Maintenance and performance history; and
  - Construction materials and recommended maintenance practices.[3]
- Condition assessment coverage (percent): 100 X (total number of critical assets with condition assessed and categorized into condition categories within a reasonable period of time (e.g., 5-10 years) ÷ total number of critical assets). Condition categories could include: unacceptable, improvement needed, adequate, good, and excellent to reflect expected service levels and acceptable risks.

2. Asset (system) renewal/replacement

Description: This measure assesses asset renewal/replacement rates over time. The measure should reflect utility targets, which will vary depending on each utility's determinations of acceptable risks for different asset classes. An asset class may consist of a cohort of pipe based on age/material, or a particular component of plants or lift stations. Generally, an asset class would have an expected service life, and this should be factored into calculations for an appropriate asset renewal/replacement rate. Decisions on asset replacement typically factor in internally agreed-upon risks and objectives, which may differ by asset class and other considerations. For instance, a utility may decide to run certain assets to failure based on benefit-cost analysis.

Example performance measures:

- Asset renewal/replacement rate (percent): 100 X (total number of assets replaced per year for each asset class ÷ total number of assets in each asset class). For example, a two percent per year replacement target (50-year renewal) for a particular asset class could be identified as the basis for performance monitoring.

  — or —

[3] From the U.S. General Accounting Office, *Water Infrastructure: Comprehensive Asset Management Has Potential to Help Utilities Better Identify Needs and Plan Future Investments*. GAO-04-461. March 2004. Available: http://www.gao.gov/new.items/d04461.pdf.

- Asset (system) renewal/replacement rate: 100 X (total actual expenditures or total amount of funds reserved for renewal and replacement for each asset group ÷ total present worth for renewal and replacement needs for each asset group). *This is a Benchmarking Performance Indicator*.

3. Water distribution/collection system integrity

Description: For drinking water utilities, this measure quantifies the number of pipeline leaks and breaks. Distribution system integrity has importance for health, customer service, operational, and asset management reasons. For wastewater utilities, this measure examines the frequency of collection system failures. When tracked over time, a utility can evaluate whether its failure rate is decreasing, stable, or increasing. When data are maintained to characterize failures by pipe type and age, type of failure, and cost of repairs, decisions regarding routine maintenance and replacement/renewals can be better made.

Example performance measure (drinking water utilities):[4]

- Non-revenue water (NRW): Water supplied to the network that does not return revenue to the utility, including unbilled authorized consumption, apparent losses (theft, customer metering inaccuracies, systematic data handling errors), and real losses (leakage from the pipe network and distribution storage) as defined in the AWWA M36 Manual. May be expressed as volume or value:
  - Volume:
    - Total volume for audit year; and/or
    - Volume per connection per year; and/or
    - Volume per connection per day.
  - Value:
    - Total cost of NRW by total cost of water system operations; and/or
    - Cost of NRW per connection per year.
- Infrastructure leakage index (ILI): Current Annual Real Loss ÷ Unavoidable Annual Real Loss (at current average system operating pressure. Measure would be expressed as a unitless ratio. *Automatic derivation of this measure provided in the AWWA Free Water Audit Software from annual water audit inputs.*
- Audit Validation Level: Level of validation (self-reported, 1, 2 or 3) conducted on the most recent water audit, as defined by Water Research Foundation Project 4639A.[5]

Example performance measure (wastewater utilities):

- Collection system failure rate (percent): 100 X (total number of collection system failures ÷ total miles of collection system piping per year). *This is a Benchmarking Performance Indicator*.

4. Infrastructure planning and maintenance

Description: This measure addresses planning for future infrastructure needs and ongoing maintenance for existing infrastructure, which is critical to overall infrastructure strategy and performance. Planned maintenance includes both preventive and predictive maintenance. Preventive maintenance is performed

[4] For more information, visit: http://www.awwa.org/store/productdetail.aspx?productid=51439782 and http://www.awwa.org/resources-tools/water-knowledge/water-loss-control.aspx.

[5] For more information, visit: *http://www.waterrf.org/Pages/Projects.aspx?PID=4639*

according to a predetermined schedule rather than in response to failure. Predictive maintenance is initiated when signals indicate that maintenance is due. All other maintenance is categorized as corrective or reactive.

Example performance measures:

This measure can be approached in different ways. Calculating costs may be preferable to encourage business decisions based on total cost; however, the reliability of costs is uncertain. Hours are likely to be less variable than costs, but not all utilities track hours. Thus, cost and hours ratios are desirable, where possible.

- Planned maintenance ratio by hours (percent): 100 X (hours of planned maintenance ÷ (hours of planned + corrective maintenance)). *This is a Benchmarking Performance Indicator*.
- Planned maintenance ratio by cost (percent): 100 X (cost of planned maintenance ÷ (cost of planned + corrective maintenance)). *This is a Benchmarking Performance Indicator*.
- Is there a formal process to prioritize infrastructure needs/future investments and allocate the necessary funding (yes/no)?
- Is there a formal process for identifying areas of uncertainty and building in needed flexibility during the infrastructure planning phase (yes/no)?

Enterprise Resiliency

1. Recordable incidents of injury or illnesses

Description: This measure addresses incidence rates, which can be used to show the relative level of injuries and illnesses and help determine problem areas and progress in preventing work-related injuries and illnesses.

Example performance measure:

The U.S. Bureau of Labor Statistics has developed instructions for employers to evaluate their firm's injury and illness record. The calculation below is based on these instructions, which can be accessed at: http://www.bls.gov/iif/osheval.htm. The 200,000 hours used in the formulas below represent the equivalent of 100 employees working 40 hours per week, 50 weeks per year, and provides the Bureau of Labor Statistics' standard base for the incidence rates.

- Total recordable incident rate: (Number of work-related injuries and illnesses X 200,000) ÷ employee hours worked.
- Number of near misses: A "near miss" is an unsafe situation or condition where no personal injury was sustained and no property was damaged, but where, given a slight shift in time or position, injury and/or damage could have occurred.

2. Insurance claims

Description: This measure examines the number, type, and severity of insurance claims to understand insurance coverage strength/vulnerability.

Example performance measures:

- Number of insurance claims: Number of general liability and auto insurance claims per 200,000 employee hours worked.

- Severity of insurance claims: Total dollar amount of general liability and auto insurance claims per 200,000 employee hours worked.

3. Risk assessment and response preparedness

Description: This measure asks whether utilities have assessed their all-hazards (natural and human-caused) vulnerabilities and risks and made corresponding plans for critical needs. Risk assessment in this context includes a vulnerability assessment regarding, for example, power outages, lack of access to chemicals, cybersecurity, extreme weather events, curtailed staff availability, etc.

Example performance measures:

- Emergency Response Plan (ERP) coverage and preparedness:
    - Does the utility have an ERP in place (yes/no)?
    - Number and frequency of ERP exercises per year: 100 X (number of critical employees who participate in ERP exercises ÷ total number of critical employees).
    - Frequency with which the ERP is reviewed and updated.
    - Does the utility discuss/coordinate ERP with other agencies/departments (e.g., city, state, police, fire, public health) (yes/no)?
- Vulnerability management: Is there a process in place for identifying and addressing system deficiencies (e.g., deficiency reporting with an immediate remedy process, established intervals between comprehensive vulnerability assessments) (yes/no)?

4. Ongoing operational resiliency

Description: This measure assesses a utility's operational reliability during ongoing/routine operations.

Example performance measure:

- Uptime for critical utility components on an ongoing basis (percent): 100 X (hours of critical component uptime ÷ hours that critical components have the physical potential to be operational). Note: a utility can apply this measure on an individual component basis or summed across all identified critical components. Also, a utility can make this measure more precise by adjusting for planned maintenance periods.
- Cybersecurity:
    - Does the utility document and periodically review network architecture (including defining network boundaries and network asset inventory)? (yes/no) *This is a Benchmarking Performance Indicator.*
    - Does the utility implement formal, written cybersecurity policies that include specific operational aspects associated with service delivery and assurance (not enterprise)? (yes/no) *This is a Benchmarking Performance Indicator.*

5. Operational resiliency under emergency conditions

Description: This measure assesses the operational preparedness and expected responsiveness in critical areas under emergency conditions.

Example performance measures (all apply to emergency conditions and, where relevant, factor in anticipated downtimes relative to required/high demand times):

- Power resiliency: Period of time (e.g., hours or days) for which backup power is available for critical operations (i.e., those required to meet 100 percent of minimum daily demand). (Note: “minimum daily demand” is the average daily demand for the lowest production month of the year.)
- Treatment chemical resiliency: Period of time (e.g., hours or days) minimum daily demand can be met with water treated to meet SDWA standards for acute contaminants (i.e., E.coli, fecal coliform, nitrate, nitrite, total nitrate and nitrite, chlorine dioxide, turbidity as referenced in the list of situations requiring a Tier 1 Public Notification under 40 CFR 141.202), without additional treatment chemical deliveries. (Note: “minimum daily demand” is the average daily demand for the lowest production month of the year.)
- Critical parts and equipment resiliency: Current longest lead time (e.g., hours or days) for repair or replacement of operationally critical parts or equipment (calculated by examining repair and replacement lead times for all identified critical parts and equipment and taking the longest single identified time).
- Critical staff resiliency: Average number of response-capable backup staff for critical operation and maintenance positions (calculated as the sum of all response-capable backup staff ÷ total number of critical operation and maintenance positions).
- Treatment operations resiliency (percent): Percent of minimum daily demand met with the primary production or treatment plant offline for 24, 48, and 72 hours. (Note: “minimum daily demand” is the average daily demand for the lowest production month of the year.)
- Sourcewater resiliency: Period of time (e.g., hours or days) minimum daily demand can be met with the primary raw water source unavailable. (Note: “minimum daily demand” is the average daily demand for the lowest production month of the year.)

Community Sustainability

1. Watershed-based infrastructure planning

Description: This measure addresses utility efforts to consider watershed-based approaches when making management decisions affecting infrastructure planning and investment options. Watershed protection strategies can sometimes, for example, protect source water quality limiting the need for additional or enhanced water treatment capacity.

Example performance measure:

- Does the utility employ alternative, watershed-based approaches to align infrastructure decisions with overall watershed goals and potentially reduce future infrastructure costs (yes/no)? Watershed-based approaches include, for example: centralized management of decentralized systems; stormwater management; source water protection programs; and conjunctive use of groundwater, source water, and recycled water to optimize resource use at a basin scale. (See also “green infrastructure” below.)

2. Green infrastructure

Description: This measure addresses green infrastructure, which includes both the built and natural/unbuilt environment. Utilities may promote source water protection and conservation green infrastructure approaches in support of water conservation (e.g., per capita demand reduction) and water quality protection objectives. Green infrastructure approaches can include: low-impact development techniques (e.g., minimization of impervious surfaces, green roofs); protection of green spaces and wildlife habitat; incentives for water-efficient domestic appliance use and landscaping; green building standards such as those promoted through the Leadership in Energy and Environmental Design (LEED) program; management of energy, chemical, and material use; etc.[6] Utilities often coordinate these efforts with community planning offices.

Example performance measures:

- Has the utility explored green infrastructure approaches and opportunities that are aligned with the utility's mandate, goals, and objectives and community interests (yes/no)?
- Does the utility have procedures that incorporate green infrastructure approaches and performance into new infrastructure investments (yes/no)?

3. Greenhouse gas emissions

Description: This measure will help drinking and wastewater utilities to understand and reduce their individual contributions to area greenhouse gas emissions. Trends indicate that water utility emissions of these gases will likely be of interest to stakeholders. Monitoring of these emissions is becoming more common among water sector utilities, and some utilities are beginning voluntary efforts to reduce their emissions (e.g., through production of reusable methane energy by wastewater utilities).

Example performance measures:

- Net (gross minus offsets) greenhouse gas emissions in tons of carbon dioxide (CO2), nitrous oxide (N2O), methane (CH4), and, as applicable, hydrofluorocarbons (HFCs) and perfluorocarbons (PFCs). Start by establishing an emissions baseline and then track emission trends in conjunction with minimizing/reducing emissions over time, where possible.[7] Emissions inventories often incorporate indirect emissions such as those generated during the production and transport of materials and chemicals.
- Percent of utility energy demand met by renewable energy resources.

4. Service affordability

Description: This measure addresses drinking water and wastewater service affordability, which centers on community members' ability to pay for water services. The true cost of water/wastewater services may be higher than some low-income households can afford, particularly when rates reflect the full life-cycle cost of water services. To the extent possible within its operating and regulatory contexts, the utility will want to

[6] For more information about green infrastructure, visit https://www.epa.gov/npdes/green-infrastructure.

[7] EPA's industry-government "Climate Leaders" partnership involves completing a corporate-wide inventory of their greenhouse gas emissions. Information and related guidance is available at http://www.epa.gov/stateply/index.html.

consider and balance keeping water services affordable while ensuring the rates needed for long-term infrastructure and financial integrity.

Example performance measures:

- Bill affordability (households for which rates may represent an unaffordable level) (percent): 100 X (number of households served for which average water bill is > "X" percent (often 2-2.5%) of median household income[8] ÷ total number of households served).

Coupled with:

- Low-income billing assistance program coverage (percent): 100 X (number of customers enrolled in low-income billing assistance program ÷ number of customers who are eligible for enrollment in low-income billing assistance program). (The utility can try to increase participation in the program for eligible households that are not participating).

5. Community economic development

Description: This measure assesses the extent to which utility operations play a role in local economic development (e.g., by attracting new employers to the area, enabling residential or commercial growth, or through job creation).

Example performance measures:

- Change in tax base (dollars or percent change) related to new water infrastructure.
- Number of jobs created by utility infrastructure investments. Jobs may be:
  - Internal to the utility;
  - Contracted by the utility; or
  - Through a new employer brought to the community as a result of utility infrastructure.
- Green infrastructure economic benefits:
  - Crime reduction (percent change); and
  - Increase in local property values (percent change).

Water Resource Sustainability

1. Water supply adequacy

Description: This measure assesses short-term and long-term water supply adequacy and explores related long-term supply considerations.

Example performance measures:

- Short-term water supply adequacy: Period of time for which existing supply sources are adequate. This can be measured as a ratio of projected short-term (e.g., 12-month rolling average) monthly

[8] This calculation focuses on identifying low-income households based median household incomes (MHI); however, MHI is not strongly correlated with the incidence of poverty or other measures of economic need. Further, populations served by small utilities in rural settings tend to have lower MHI and higher poverty rates, but fewer options for diversifying water/wastewater service rates based on need compared to larger municipal systems.

supply to projected short-term monthly demand. Often an index or scale is used, for example, short-term supply relative to severe drought (assigned a "1") to abundant supply conditions (assigned a "5").

- Long-term water supply adequacy: Projected future annual supply relative to projected future annual demand for at least the next 50 years (some utilities project out as far as 70-80 years). Statistical forecasting and simulation modeling and forecasting techniques are typically used for such long-term projections. Analysis variables in addition to historical record (e.g., historical and year-to-date reservoir elevation data), forecasted precipitation, and flows (including surface and groundwater, as applicable) can include:
  - Future normal, wet, dry, and very dry scenarios;
  - Anticipated population changes;
  - Future service areas;
  - Availability of new water supplies including both traditional, and alternative supplies, such as recycled water, groundwater banking, desalinization, or groundwater highest and best use; and
  - Levels of uncertainty around the above.
- Water Reuse (water beneficially reused):
  - Amount (percentage or gallons) of reclaimed water used in place of fresh water or drinking water for non-potable uses.
  - Amount (percentage or gallons) of reclaimed water used for potable purposes.
  - Amount (gallons or acre feet) of reclaimed water added to drinking water reservoir(s).
  - Area (acres) of land irrigated using only recycled water.

2. Supply and demand management

Description: This measure explores whether the utility has a strategy for proactive supply and demand management in the short and long terms. Strategy needs will depend on community circumstances and priorities, anticipated population growth, future water supply in relation to anticipated demand, demand management and other conservation options, and other local considerations.

Example performance measures:

- Does the utility have a demand management/demand reduction plan (yes/no)? Does this plan track per capita water consumption and, where analytical tools are available to do so, accurately attribute per capita consumption reductions to demand reduction strategies (such as public education and rebates for water-efficient appliances) (yes/no)?
- Do demand scenarios account for changes in rates (which can change for many reasons) and conservation-oriented, demand management pricing structures (yes/no)?
- Does the utility have policies in place that address, prior to committing to new service areas, the availability of adequate dry year supply (yes/no)? Alternatively, does the utility have a commitment to denying service commitments unless a reliable drought-year supply, with reasonable drought use restrictions, is available to meet the commitment (yes/no)?

3. Watershed sustainability

Description: This measure explores whether the utility has a strategy for proactive watershed management and/or partnerships to ensure an effective integration of utility and watershed investments and practices, to achieve overall optimized performance for the community and the utility.

Example performance measures:

- Amount of pollutants/contaminants managed through source control practices (avoiding the need for treatment plant upgrades, etc.).
- Has the utility developed a source water protection plan (yes/no)?
- Does the utility partner with regional stakeholders to protect and enhance its watershed (yes/no)?
- Percent of wet weather impacts (e.g., flooding, CSOs, SSOs, gallons of infiltrated water not reaching collection systems) managed through watershed (natural treatment) processes: 100 X (Number of wet weather impacts managed through watershed processes ÷ total number of wet weather impacts).
- Area (in acres) of enhancements to wetland areas for treatment/storage of wet weather flows.
- Amount of nutrient removal via watershed approaches:
  - Cost savings derived from nutrient control through watershed processes as an alternative to treatment plant nutrient removal; and
  - Percent of nutrient removal requirements met through watershed processes rather than treatment at the plant.
- Environmental benefits:
  - Amount of movement or reduction of saltwater front (in feet).
  - Amount of avoided freshwater diversion from sensitive ecosystems.

Stakeholder Understanding and Support

1. Stakeholder consultation

Description: This measure addresses utility actions to reach out to and consult with stakeholders about utility matters, including utility goals, objectives, and management decisions.

Example performance measures:

- Does the utility identify stakeholders, conduct outreach, and actively consult with stakeholders about utility matters (yes/no)? Elements of this plan can include:
  - Number of active contacts with stakeholders in key areas (e.g., from local government, business, education, non-governmental groups)?
  - Does the utility actively seek input from stakeholders (yes/no)?
  - Frequency with which the utility actively consults with stakeholders. This measure should go beyond counting the number of calls or times information is sent out or posted on websites to items such as number of stakeholder outreach and education activities, number of opportunities for stakeholders to provide input, participation of stakeholders on utility committees, etc.
- Does the utility actively consider and act upon stakeholder input (yes/no)?

2. Stakeholder satisfaction

Description: This measure addresses stakeholder perceptions of the utility. Stakeholder satisfaction can be measured through surveys sent to stakeholders, formal feedback surveys distributed to stakeholders at events, etc.

Example performance measures:

- Overall satisfaction (percent): 100 X (number of stakeholders who annually rate the overall job of the utility as positive ÷ total number of stakeholders surveyed).
- Responsiveness (percent): 100 X (number of stakeholders who annually rate utility responsiveness to stakeholder needs as positive ÷ total number of stakeholders surveyed).
- Message recollection for outreach programs targeted to specific stakeholder groups (percent): (a) 100 X (number of stakeholders who recall key messages ÷ total number of stakeholders surveyed); and (b) 100 X (number of stakeholders who recall the message source (TV, utility mailers, newsletters, etc.) ÷ total number of stakeholders surveyed).

3. Internal benefits from stakeholder input

Description: This measure addresses the value utility employees believe stakeholder engagement has provided to utility projects and activities. Measurement by the utility can focus on surveying utility employees running projects that have stakeholder involvement.

Example performance measures:

- 100 X (number of utility projects or activities where stakeholders participated and/or provided input for which utility employees believe there was value added as a result of stakeholder participation and input ÷ total number of projects where stakeholders participated and/or provided input).
- Overall value added (percent): 100 X (number of utility employees who rated their overall sense of value added from stakeholder participation and input as (high value added, some value added, little value added, no value added) ÷ total number of utility employees surveyed).

4. Comparative rate rank

Description: This measure depicts how utility rates compare to similar utilities (e.g., utilities of the same type (drinking water, wastewater) that are similar in terms of geographic region, size of population served, etc.). A utility can use the measure internally or to educate stakeholders. It should be noted that the lowest rate is not necessarily best (see Financial Viability). When comparing rates with other utilities, it is important to make sure to account for other variables that can affect rates to ensure that you are comparing “apples to apples.” For example, when comparing a wastewater collection and treatment utility's rates to a utility providing treatment only, include the average rate of the separate wastewater collection utility in a combined rate.

Example performance measure:

- Typical monthly bill for the average household as a percentage of typical monthly bills for similar utilities.

5. Media/press coverage

Description: This measure captures media portrayal of the utility (newspaper, TV, radio, etc.) in terms of awareness, accuracy, and tone.

Example performance measures:

- Amount of coverage: Total number of media stories (social media, newspaper, TV, radio, etc.) concerning the utility per year.
- Media coverage tone (percent): 100 X (number of media stories concerning the utility that portray the utility in a positive way ÷ total number of media stories concerning the utility) per year.
- Media coverage accuracy (percent): 100 X (number of media stories that accurately describe the utility ÷ total number of media stories concerning the utility) per year.
- Number of outreach events conducted to build support for utility, value of water, and value of water services.

6. Partnering in your community

Description: This measure assesses how the utility actively engages with community organizations to advance important initiatives, engage partners in decision making, and to position the utility as an anchor institution in the community. Partnering in this manner can result in many different types of benefits for the utility and the community, including the increased understanding and support for utility needs and the value of water and water services to the community.

Example performance measures:

- Performance improvements resulting from a partnership (e.g., reduced volume of flooding or greenhouse gas emissions).
- Number and type of specific projects completed associated with partnerships (e.g., rain gardens installed, innovative technologies implemented, innovative practices adopted).
- Level of partner/community support for utility and the value of water (e.g., number of community members/partners participating in utility events or providing positive feedback for utility services).

ADDITIONAL ATTRIBUTE-SPECIFIC MEASUREMENT RESOURCES

The following resources provide additional measures that are specific to various Attributes. The list is not meant to be exhaustive, but rather, serves as a starting place for utilities seeking additional resources for measures.

- **The Energy Roadmap** (Water Environment Federation)
- **National Biosolids Partnership** (Water Environment Federation)
- **The Nutrient Roadmap** (Water Environment Federation)
- **On-Demand WasteWater Library (OWWL)** (Water Environment Federation)
- **The Value of Water** (http://thevalueofwater.org/)
- **Work for Water** (American Water Works Association and Water Environmental Federation)
- **Water Advocates** (Water Environment Federation)
- **AWWA Water and Wastewater Rate Survey** (American Water Works Association) *subscriber only*
- **AWWA Compensation Survey** (American Water Works Association) *subscriber only*
- **NACWA Financial Survey** (National Association of Clean Water Agencies)

Effective Utility Management: A Primer for Water and Wastewater Utilities

January 2017

Appendix J

AWWA CYBERSECURITY RESULTS MANATEE

Category	Control	Priority	Referenced Standards	Level Of Implementation	Project	Notes
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.	Priority 1 Controls	DHS CAT: 2.7.7 Investigation and Analysis	Not Implemented		
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Priority 1 Controls	AWWA G430-14: 4.6 Access Control and Intrusion Detection NIST 800-82r2: 6.2.1 Access Control	Not Implemented		
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Priority 1 Controls	DHS CAT: 2.15.11 Permitted Actions without ID or Authentication	Not Implemented		
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	Priority 1 Controls	ISA 62443-3-3: 9.3 Network Segmentation NIST 800-53: Appendix F-SC: SC-7 Boundary Protection NIST 800-82r2: 5.6 Recommended Defense-in-Depth Architecture	Not Implemented		
IA-3	Role based access control system established including policies and procedures.	Priority 1 Controls	DHS CAT: 2.15 Access Control NIST 800-53: Appendix F-AC: AC-3 Access Enforcement	Not Implemented		
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).	Priority 1 Controls	DHS CAT: 2.5.5 Control System Documentation NIST 800-53: Appendix F-AC: AC-3 Access Enforcement	Not Implemented		
IA-5	Access control for diagnostic tools and resources and configuration ports.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.13.1.1 Network Controls NIST 800-53: Appendix F-AC: AC-3 Access Enforcement	Not Implemented		
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Priority 1 Controls	NIST 800-53: Appendix F-AC: AC-17 Remote Access NIST 800-82r2: 5.15 Authentication and Authorization	Not Implemented		
PE-1	Security perimeters, card controlled gates, manned booths, and procedures for entry control.	Priority 1 Controls	DHS CAT: 2.4.3 Physical Access Control, NIST 800-53: Appendix F-PE: PE-3 Physical Access Control, ISO/IEC 27001: Annex A: A.11.1.1 Physical security perimeter	Partially Implemented		
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1 Secure areas, NIST 800-53: Appendix F-PE: PE-5 Access Control for Output Devices	Partially Implemented		
PE-3	Physical security and procedures for offices, rooms, and facilities.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1.3 Securing offices and facilities, NIST 800-53: Appendix F-PE: PE-4 Access Control for Transmission Medium	Partially Implemented		
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Priority 1 Controls	DHS CAT: 2.4 Physical and Environmental Security, ISO/IEC 27001: Annex A: A.11.1.4 Protecting against external and environmental threats, NIST 800-53: Appendix F-CP: CP-2 Contingency Plan	Partially Implemented		
PE-5	Physical security and procedures for working in secure areas.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1.5 Working in secure areas, NIST 800-53: Appendix F-PE: PE-1 Physical and Environmental Policy and Procedures	Partially Implemented		
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from IT/PCS areas	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1.6 Delivery and Loading areas, NIST 800-53: Appendix F-PE: PE16 Delivery and Removal	Not Implemented		
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	Priority 1 Controls	DHS CAT: 2.4 Physical and Environmental Security,ISO/IEC 27001: Annex A: A.11.1.4 Protecting against external and environmental, NIST 800-53: Appendix F-CP: CP-7 Alternate Processing Site	Partially Implemented		
PE-8	Physical/logical protection against power failure of equipment (UPS).	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.2.2 Supporting utilities, NIST 800-53: Appendix F-CP: CP-8 Telecommunications Services	Fully Implemented and Maintained		
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.2.3 Cabling security, NIST 800-53: Appendix F-PE: PE-9 Power Equipment and Cabling	Partially Implemented		
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	Priority 1 Controls	DHS CAT: 2.8.11 Cryptographic Key Establishment and Management, ISA 62443-3-3: 9 Restricted Data Flow, NIST 800-82r2: 6.2.16.1 Encryption	Not Implemented		
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.	Priority 1 Controls	NIST 800-53: Appendix F-AC: AC-17 Remote Access	Not Implemented		
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	Priority 1 Controls	NIST 800-82r2: 5.1 Network Segmentation and Segregation	Partially Implemented		
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.	Priority 1 Controls	NIST 800-82r2: 5.4 Logically Separated Control Network	Not Implemented		
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	Priority 1 Controls	NIST 800-82r2: 5.5 Network Segregation	Not Implemented		
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Priority 1 Controls	NIST 800-82r2: 6.2.1.3 Virtual Local Area Network (VLAN)	Not Implemented		
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Priority 1 Controls	DHS CAT: 2.15.16 Passwords	Not Implemented		
SC-23	Wireless communications links encrypted.	Priority 1 Controls	NIST 800-82r2: 6.2.1.5 Wireless	Not Implemented		
SC-24	Communications links encrypted.	Priority 1 Controls	NIST 800-82r2: 6.2.1.5 Wireless	Not Implemented		
SC-25	Virtual Private Network (VPN) using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	Priority 1 Controls	NIST 800-82r2: 5.10.2 Remote Support Access, NIST 800-82r2: 5.4 Logically Separated Control Network	Not Implemented		
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.	Priority 1 Controls	ISA 62443-3-3: 9.2 Restricted Data Flow Rationale, NIST 800-82r2: 5.5.4 Firewall with DMZ between Corporate Network and Control Network	Not Implemented		
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.	Priority 1 Controls	NIST 800-53: Appendix F-AU: AU-10 Non-Repudiation	Not Applicable		
SI-3	Interactive system for managing password implemented to ensure password strength.	Priority 1 Controls	NIST 800-53: Appendix F-IA: IA-5 Authenticator Management	Not Implemented		
AT-1	A security awareness and response program established to ensure staff is aware of security policies and incident response/notification procedures.	Priority 2 Controls	DHS CAT: 2.11 Security Awareness and Training ISA 62443-2-1: A.3.2.4 Staff Training and Security Awareness	Not Implemented		

AT-2	Security training including Incident response training for employees, contractors and third party users based on job roles.	Priority 2 Controls	AWWA G430-14: 4.3 Defined Security Roles and Employee Expectations DHS CAT: 2.11.3 Security Training	Not Implemented		
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	Priority 2 Controls	ISA 62443-3-3: 6 Use Control NIST 800-82r2: 6.2.3 Audit and Accountability	Not Implemented		
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.	Priority 2 Controls	DHS CAT: 2.1 Security Policy, ISO/IEC 27001: Annex A: A.5 Information security policy	Not Implemented		
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.	Priority 2 Controls	ISA 62443-2-1: A.3.2.3 Organizing for security, ISO/IEC 27005: 27005 Whole Document, NIST 800-53: Appendix J: AR-1 Governance and Privacy Program	Not Implemented		
AU-4	Information security responsibilities defined and assigned.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.6.1.1 Information systems roles and responsibilities NIST 800-53: Appendix F-AU: AU-1 Audit and Accountability Policies and Procedures	Not Implemented		
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.	Priority 2 Controls	DHS CAT: 2.12.2 Continuity of Operations Plan ISA 62443-2-1: A.3.2.5 Business continuity plan ISO/IEC 27003: 27003 8.2 Conduct risk assessment	Not Implemented		
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	Priority 2 Controls	NIST 800-124: 2.2.1-5 Lack of Physical Security Controls	Not Implemented		
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.14.2.9 System acceptance testing	Not Implemented		
CM-3	Separation of duties implemented for user processes including risk of abuse.	Priority 2 Controls	ISA 62443-2-1: A.3.3.5.3 Separation of duties ISO/IEC 27001: Annex A: A.6.1.2 Segregation of duties NIST 800-53: Appendix F-AC: AC-5 Separation of Duties	Not Implemented		
CM-5	SLAs for all third parties established, including levels of service and change controls.	Priority 2 Controls	DHS CAT: 2.5.9 Outsourced Control System Services NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Not Implemented		
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.	Priority 2 Controls	DHS DID: 3.4 Intrusion Detection Systems NIST 800-53: Appendix F-CM: CM-11 User-Installed Software	Not Implemented		
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high risk locations.	Priority 2 Controls	DHS CAT: 2.15.5 Authenticator Management	Not Implemented		
IA-9	Multifactor authentication system established for critical areas.	Priority 2 Controls	ISA 62443-1-1: 5.3 Defense in Depth ISA 62443-3-3: 5.3 Human User ID and Authentication NIST 800-34: 3.2 Conduct the Business Impact Analysis NIST 800-82r2: 6.2.7 Identification and Authentication	Not Implemented		
IR-1	Incident response program established to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events.	Priority 2 Controls	AWWA G430-14: 4.11 Emergency Response and Recovery Plans and Business Continuity Plans DHS CAT: 2.12.16 Control System Backup NIST 800-61R2: Whole Document	Not Implemented		
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.11.2.6 Security of equipment and assets off-premises NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Partially Implemented		
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.	Priority 2 Controls	ISO/IEC 27002: 27002 15.3 Information Systems Audit Considerations NIST 800-53: Appendix F-AU: AU-6 Audit Review, Analysis, and Reporting	Not Implemented		
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.6.2.3 Addressing security in third party agreements NIST 800-124: 4.1 Security for the Enterprise Mobile Device Solution Life Cycle - Initiation NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Not Implemented		
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	Priority 2 Controls	NIST 800-53: Appendix F-SI: SI-5 Security Alerts, Advisories, and Directives	Partially Implemented		
RA-2	Third party agreement process to ensure that external vendors and contractors utilize appropriate security measures for access, processing, communicating, or managing the organization's information or facilities.	Priority 2 Controls	NIST 800-53: 2.5 External Service Providers NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Not Implemented		
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).	Priority 2 Controls	NIST 800-34: 3.2 Conduct the Business Impact Analysis NIST 800-53: Appendix F-CM: CM-6 Configuration Settings	Not Implemented		
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Priority 2 Controls	NIST 800-53: Appendix F-SA: SA-11 Developer Security Testing and Evaluation	Not Implemented		

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.	Priority 2 Controls	NIST 800-53: Appendix F-SI: SI-4 Information System Monitoring	Not Implemented		
SC-5	Anomaly based IDS/IPS established including policies and procedures.	Priority 2 Controls	NIST 800-53: Appendix F-SI: SI-4 Information System Monitoring	Not Implemented		
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	Priority 2 Controls	NIST 800-82r2: 5.6 Recommended Defense-in-Depth Architecture	Not Implemented		
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.	Priority 2 Controls	DHS CAT: 2.9.5 Information Exchange NIST 800-53: Appendix F-AC: AC-21 Information Sharing	Not Implemented		
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.	Priority 2 Controls	DHS DID: 3.1.1 Architectural Zones ISA 62443-1-1: 5.8 Security Zones ISA 62443-3-3: 9.3 Network Segmentation NIST 800-82r2: 5.4 Logically Separated Control Network	Not Implemented		
SC-9	Process isolation established to provide a manual override "air gap" between highly sensitive systems and regular environments.	Priority 2 Controls	ISA 62443-3-3: 9.3.3 Physical Network Segmentation	Partially Implemented		
SI-5	Privileged program controls established to restrict usage of utility programs that could reset passwords or override controls as well as IT audit tools that can modify or delete audit data.	Priority 2 Controls	DHS DID: 3.5.1 Log and Event Management NIST 800-53: Appendix F-IA: IA-2 Identification and Authentication	Not Implemented		
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.13.2.4 Confidentiality or non-disclosure agreements	Not Implemented		
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.	Priority 3 Controls	DHS CAT: 2.15.28 External Access Protections ISA 62443-1-1: 5.5 Threat-Risk Assessment	Not Implemented		
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.5.1.2 Review of the policies for information security NIST 800-53: Appendix G: PM-1 Information Security Program Plan	Not Implemented		
CM-4	Separation of duties implemented for development, production, and testing work.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.6.1.2 Segregation of duties NIST 800-53: Appendix F-AC: AC-5 Separation of Duties	Not Implemented		
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.	Priority 3 Controls	DHS CAT: 2.15.26 Wireless Access Restrictions DHS DID: 3 Isolating and Protecting Assets: Defense-in-Depth Strategies ISA 62443-3-3: 5.8 Wireless access management	Partially Implemented		
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.11.2.1 Equipment siting and protection NIST 800-53: Appendix F-PE: PE-15 Water Damage Protection	Partially Implemented		
IR-3	A legal/contractual/regulatory framework established 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.	Priority 3 Controls	DHS CAT: 2.9.7 Information and Document Retrieval	Not Applicable		
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.8.3.1 Management of removable media NIST 800-53: Appendix F-MP: MP-1 Media Protection Policy and Procedures	Not Implemented		
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.	Priority 3 Controls	ISA 62443-3-3: 11.1 Control system component inventory ISO/IEC 27001: Annex A: A.8 Asset Management NIST 800-53: Appendix F-CM: CM-8 Information System Component Inventory NIST 800-53: Appendix F-CM: CM-9 Configuration Management Plan	Partially Implemented		
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.8.1.1 Inventory of Assets NIST 800-53: Appendix G: PM-5 Information System Inventory	Partially Implemented		
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.	Priority 3 Controls	DHS CAT: 2.3.1 Personnel Security Policy and Procedures	Partially Implemented		
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third party users.	Priority 3 Controls	DHS CAT: 2.3.9 Personnel Roles	Partially Implemented		
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.	Priority 3 Controls	DHS CAT: 2.3.8 Personnel Accountability ISO/IEC 27001: Annex A: A.11.2.9 Clear desk and clear screen policy ISO/IEC 27002: 27002 11.2.9 Clear desk and clear screen policy	Not Implemented		

PS-4	Disciplinary process for security violations established.	Priority 3 Controls	DHS CAT: 2.3.8 Personnel Accountability ISA 62443-2-1: A.3.3.2 Personnel security ISO/IEC 27001: Annex A: A.7.2.3 Disciplinary process	Not Implemented		
SA-1	Authorization process established for new systems or changes to existing information processing systems.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.14.2 Security in development and support processes NIST 800-53: Appendix G: PM-10 Security Authorization Process	Not Implemented		
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.	Priority 3 Controls	DHS CAT: 2.6.3 Configuration Change Control ISO/IEC 27001: Annex A: A.14.2.2 System change control procedures NIST 800-53: Appendix F-SA: SA-10 Developer Configuration Management	Not Implemented		
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.	Priority 3 Controls	NIST 800-82r2: 6.2.5 Configuration Management	Not Implemented		
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.	Priority 3 Controls	DHS CAT: 2.15.25 Access Control for Mobile Devices NIST 800-34: Executive Summary	Not Implemented		
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.14.2.3 Technical review of applications after operating platform changes NIST 800-53: Appendix F-CM: CM-3 Configuration Change Control	Not Implemented		
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.	Priority 3 Controls	DHS CAT: 2.5 System and Services Acquisition ISO/IEC 27001: Annex A: A.14.2.9 System acceptance testing	Not Implemented		
SI-4	Organization-wide clock synchronization system in place.	Priority 3 Controls	NIST 800-53: Appendix F-AU: AU-8 Time Stamps	Not Implemented		
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.14.2.2 System change control procedures NIST 800-53: Appendix F-CM: CM-1 Configuration Management Policy and Procedures	Not Implemented		
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.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.9.2.1 User registration and de-registration NIST 800-53: Appendix F-IA: IA-4 Identifier Management	Not Implemented		
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.	Priority 4 Controls	AWWA G430-14: 4.4 Up-to-Date Assessment of Risk DHS CAT: 2.12 Incident Response NIST 800-61R2: Whole Document	Not Implemented		
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.11.2.4 Equipment maintenance NIST 800-53: Appendix F-MA: MA-2 Controlled Maintenance	Partially Implemented		
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.13.2.4 Confidentiality or non-disclosure agreements NIST 800-53: Appendix F-AC: AC-19 Access Control for Mobile Devices	Partially Implemented		
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).	Priority 4 Controls	DHS CAT: 2.13 Media protection NIST 800-53: Appendix F-MP: MP-6 Media Sanitization	Not Implemented		
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Priority 4 Controls	ISA 62443-2-1: A.3.2.6 Security Policies and Procedures NIST 800-53: Appendix G: PM-1 Information Security Program Plan	Partially Implemented		
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.8.2.1 Classification of Information NIST 800-53: Appendix F-RA: RA-2 Security Categorization	Not Implemented		

Appendix K

AWWA CYBERSECURITY TOOL OUTPUT

American Water Works Association

Dedicated to the World's Most Important Resource®

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

Tool and Guidance Revision History		
Version	Date	Description
1.0	4/4/2014	Initial Release
2.0	2/22/2017	Revised to match updated Cybersecurity Guidance tool. The Use Case descriptions were revised for clarity. Use cases were added to address wireless communications. An additional 12 cyber controls were added.
3.0	9/4/2019	Revised to improve user interface. Explicitly supports AWIA 2018 §2013 compliance. Updates to the use cases and controls, and alignment with NIST Cybersecurity Framework v1.1. Provide Microsoft Excel-based output to allow for self-assessment of controls and development of an improvement plan.

Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

CONTENTS

ACKNOWLEDGEMENTS

This project was funded by the American Water Works Association (AWWA), utilizing Water Industry Technical Action Fund (WITAF), WITAF Project #039, and managed by Kevin M. Morley.

Project Advisory Committee

- Norm Anderson, Carollo Engineers
- John Brosnan, Santa Clara Valley Water District
- Don Dickinson, Phoenix Contact
- Patrick Norton, Tampa Bay Water
- Robert Raffaele, American Water

Project Contractors

- Andrew Ohrt, West Yost Associates
- Dan Groves, West Yost Associates
- Jeff Pelz, West Yost Associates
- Joel Cox, West Yost Associates
- Murphy Altunel, West Yost Associates
- Bailey Bartolucci, West Yost Associates
- Judith H. Germano, GermanoLaw LLC
- Gwen M. Schoenfeld, GermanoLaw LLC
- Gemma Kite, Horsley Witten Group, Inc.
- Tom Noble, Horsley Witten Group, Inc.
- Will Keefer, Horsley Witten Group, Inc.

Subject Matter Expert Panel

- Danielle Anderson, City of Minneapolis Water Treatment and Distribution Services Division
- Will Bianchini, Onondaga County Water Authority
- Andy Bochman, Idaho National Laboratory
- Jacques Brados, Black and Veatch
- Geoffrey Brown, Alameda County Water District
- Bernie Bullert, SL-Serco
- Travis Cochrane, City of Corpus Christi
- Jeff Cooley, City of Vacaville Public Utilities
- Steve Crumley, City of Minneapolis Water Treatment and Distribution Services Division
- Charley Cunningham, City of Sacramento Department of Utilities
- Bob Daly, EMA Inc.
- Jon Eaton, City of Eagan Public Utilities
- Bill Fisher, National Institute of Standards and Technology
- Jamie Foreman, City of Carmel Public Works
- Glen Goins, The Automation Group
- Andrew Hildick-Smith, Massachusetts Water Resource Authority
- Daniel Honore, Village of Pleasant Prairie Utility Department
- Dr. Connie Justice, Indiana University Purdue University Indianapolis
- Marlene Ladendorff, Schneider Electric
- Michael Lewis, City of Albany Public Works
- Jim Livermore, CDM Smith
- Mike Malone, Eastern Municipal Water District
- Blas Moreno, Prince William County Service Authority
- Ariz Naqvi, Alameda County Water District
- Debbie Newberry, United States Environmental Protection Agency
- Janine Nielsen, Rockwell Automation, Inc.
- Kevin Owens, Control Cyber Inc.
- Cayce Parrish, United States Environmental Protection Agency
- David Paul, AquaEngineers
- Chuck Redding, City of Sacramento Department of Utilities
- Nelson Sims, DC Water and Sewer Authority
- Chris Walcutt, Black and Veatch
- Jennifer Lyn Walker, WaterISAC
- Linda Warren, Launch! Consulting

Acronym and Abbreviation Table	
Acronym /Abbreviation	Description
ANSI	American National Standards Institute
AWIA 2018	America's Water Infrastructure Act of 2018
AWWA	American Water Works Association
CCE	Consequence-Centered Engineering
CFR	Code of Federal Regulations
CIA	Confidentiality Integrity and Availability
CIA	Confidentiality, Integrity, and Availability
CIE	Cyber-Informed Engineering
CIR	Committed Information Rate
CISSP	Certified Information Systems Security Professional
ERP	Emergency Response Planning
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
INL	Idaho National Laboratory
ISA	International Society of Automation
IT	Information Technology
LAN	Local Area Network
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OPSEC	Operations Security
PCI	Payment Card Industry
PCS	Process Control Systems
PII	Personally identifiable information
PLC	Programmable Logic Controller
QoS	Quality of Service
RRA	Risk and Resilience Assessment
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SME	Subject Matter Experts
SSN	Single Sign On
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WITAF	Water Industry Technical Action Fund

EXECUTIVE SUMMARY

Within the last several decades, cybersecurity threats, including such things as cyber-terrorism and ransomware attacks, have grown from the esoteric practice of a few specialists to a problem of general concern. Critical infrastructure systems serving the people of the United States have been found to be particularly vulnerable to such attacks. As noted in the Cybersecurity Risk and Responsibility in the Water Sector[1]:

"Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data."

In response to the general threat to critical infrastructure, a wide array of standards and guidelines are available to assist organizations with implementing security controls to mitigate the risk from cyber-attacks. The scope of these documents is large, and the security controls in the standards often require significant planning and years of implementation.

In February 2013, the American Water Works Association (AWWA) Water Utility Council initiated a project (WITAF #503) to address the absence of practical, step-by-step guidance for protecting water sector process control systems (PCS)[2] from cyber-attacks. This action was timely as it corresponded with the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as called for in Executive Order 13636 - Improving Critical Infrastructure Cybersecurity.[3] The NIST Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

This AWWA Water Sector Cybersecurity Risk Management Guidance (AWWA Guidance) and associated AWWA Cybersecurity Assessment Tool (AWWA Assessment Tool), collectively referred to as AWWA Guidance and Assessment Tool, is a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council. The original goal of this AWWA guidance was to provide water sector utility owners/operators with a consistent and repeatable assessment tool and recommended course of action to reduce vulnerabilities to cyber-attacks as recommended in ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636. The guidance is also expected to communicate a "call to action" for utility executives acknowledging the significance of securing PCS and enterprise systems (e.g. information technology) given their role in supporting water utility operations.

This AWWA Guidance and Assessment Tool update was developed to assist community water systems (i.e. utility) in complying with section 2013 of America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270).[4] AWIA requires all community water systems serving populations of 3,300 or more to conduct and certify completion of an assessment of the risks to, and resilience of their systems, including an emergency response plan. The new requirement places emphasis on assessing and mitigating cybersecurity risks that could impact the following:

- Electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;

[1] American Water Works Association, *Cybersecurity Risk and Responsibility in the Water Sector*, 2018.

[2] The term process control system (PCS) is preferred over industrial control system (ICS) to avoid confusion with incident command system (ICS) common in national emergency response planning.

[3] Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[4] The text of AWIA §2013 is included in Appendix A.

- The monitoring practices of the system (including network monitoring); and
- The financial infrastructure of the system (accounting and financial business systems operated by a utility, such as customer billing and payment systems).

Utilities may have PCS and enterprise systems that are physically or logically connected. In addition, many business applications that utilities rely on to support critical day-to-day operations reside within enterprise systems. To account for this, enterprise systems are explicitly included in the AWIA requirements for the risk and resilience assessment (RRA) and emergency response plan (ERP).

A panel of subject matter experts was consulted to identify the most pressing cybersecurity issues facing water utilities today. In response to these issues, a recommended grouping of cybersecurity practices was developed. This grouping identifies cybersecurity practice areas considered to be the most critical for managing cyber risk in the water sector. This guidance provides a discussion of the recommended practice areas and why they are important to supporting a robust cybersecurity risk management strategy.

These recommended practices are defined by a set of 99 cybersecurity controls that are organized in a manner to facilitate implementation based on actionable tasks. The outputs of the AWWA Assessment Tool are designed to present these controls to users in a concise, straightforward manner, facilitate documentation and support future compliance actions and improvement.

The AWWA Assessment Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user provides information about the manner in which their PCS and enterprise systems are used. Based on these practices, use cases are selected to recommend controls. For each recommended control, specific references to existing cybersecurity standards are also provided.

The AWWA Assessment Tool emphasizes actionable recommendations with the highest priority assigned to those that are expected to provide the greatest impact in the short term. It should be noted, however, that the tool does not assess the extent to which a utility has implemented any of the recommended controls. This is the responsibility of the utility. To facilitate this, additional tool outputs were added and are discussed in the following sections.

This resource is a living document, and further revisions and enhancements will be made based on the quickly evolving cyber-threat landscape and user feedback.

Use of this Guidance to Support AWIA §2013 Compliance

As noted above, one objective of the AWWA Cybersecurity Guidance and Assessment Tool is to support utilities with AWIA §2013 compliance actions. Additional guidance is provided in subsequent sections of this document.

Utility staff responsible for AWIA §2013 compliance may not be cybersecurity technologists or responsible for the secure and reliable operation of the PCS and/or enterprise systems. Therefore, it is recommended that a utility convene internal and external support staff, including, but not limited to:

- Utility compliance staff responsible for AWIA §2013 compliance.

- Utility staff responsible for and knowledgeable of the design, operation, and maintenance of the utility’s PCS and enterprise systems (information technology).
- Utility leadership responsible for overall operation of the utility (utility staff with the authority to accept risks should be present).
- External support staff including cybersecurity vendors, engineering firms, etc., if needed.

This approach will improve the quality and timeliness of data collection. In addition, it is expected to reduce the overall time required to complete compliance actions while also improving the cybersecurity posture[5] of the organization.

Cybersecurity Guidance and Tool Output Information Security

The output of the Assessment Tool should be classified as critical infrastructure security information. In many states, this means that it is protected from public informaton requests. To maintain a high level of information security after the output is generated, AWWA strongly recommends the following:

- If your utility has a data classification system in place, treat the output and associated information as the most protected type of information. It is recommended that this be done with consideration to the FOIA/sunshine laws in your jurisdiction.
- If your utility does not have a data classification system in place:
  - Store this data in a secure location.
  - Restrict access to this information as much as possible. For example: do not email this document.

RECOMMENDED CYBERSECURITY PRACTICES

Overview

These practices are comprised of recommendations to improve the cybersecurity posture of water and wastewater utilities. They are actionable recommendations designed to produce maximum improvement in the short term and provide a foundation for longer term implementation of a comprehensive cybersecurity risk management strategy.

The terminology used within this section and other standards is fundamentally technical. AWWA strived to make the guidance and user experience as “plain English” as possible. However, some additional insight into the networking and network component terminology may be helpful to the reader. It is recommended that the reader refer to Appendix B: Network Architecture Reference Diagram and Definitions.

Practice Categories

The practice categories were chosen by Subject Matter Experts (SME) teams during a Definition Workshop. Each team identified important areas of cybersecurity to be addressed and policies, activities, and systems that should be implemented. The recommendations from the SMEs were collected, integrated (to avoid duplication), and loosely organized into the ten domains of the Certified Information Systems Security Professional (CISSP) Common Book of Knowledge. Several reviews and additions followed until there was consensus that the practives categories and recommendations were comprehensive. The categories (like their NIST framework counterparts) are not mutually exclusive and contain significant overlap. In addition, the AWWA Assessment Tool output categorizes the

[5] The cumulative strength of a utility’s cybersecurity policies, controls, and how effectively they mitigate risk.

recommended controls into these practice areas. The following is a description of each practice category.

Governance and Risk Management

This category is concerned with the management and executive control of the security systems of the organization; it is associated with defining organizational boundaries and establishing a framework of security policies, procedures, and systems to manage the confidentiality, integrity, and availability (CIA) of the organization. One of the key components of system governance is developing and maintaining an accurate, up-to-date inventory of PCS and enterprise system components.

Cyber supply chain risk management is an important component in the design, operation, and maintenance of PCS and enterprise systems. This includes such things as establishing cybersecurity requirements for suppliers, communication of these requirements, and verifying the requirements are met.

From the perspective of long-term security, this is the most important category because it creates a managed process for increasing security. It also engages the executive team by including security risks as an important part of enterprise risk management.

Although this category of recommendations represents an essential part of an organization's security posture, the related cybersecurity controls have been assigned a slightly lower priority in order to emphasize actionable recommendations that can have significant short-term effects.

Business Continuity and Disaster Recovery

This category is concerned with ensuring that the control system continues running even when faults occur and with rapid recovery after a service disruption.

Business Continuity Planning is a structured method for an organization to prepare for and reduce the probability and impact of systems and operational failure. A key component of Business Continuity Planning is the Disaster Recovery Plan, which deals with longer disruptions from more impactful events.

Both plans require a managed process that identifies potentially disruptive events, estimates their impact, and then develops and monitors mitigation strategies.

Server and Workstation Hardening

This category is concerned with securing servers and workstations against cyber-attacks; it identifies best practices to minimize the probability of unauthorized access to servers, and to maintain the CIA properties of the servers and the systems within them. For example, this category includes whitelisting, which restricts the applications that are permitted to run on servers and workstations throughout the enterprise.

Access Control

This category is concerned with ensuring that only authorized personnel are permitted to access computing resources within the organization; it pertains to best practices for restricting access to computing resources and information to authorized users. For example, Single Sign On (SSN) is an access control mechanism that requires users to sign on only once; the SSN system can then use those credentials to control access to a variety of applications. However, care should be taken to ensure that different passwords are used to access PCS and enterprise systems.

Application Security

This category is concerned with ensuring that computer programs do only what they are supposed to do; for example, suppose that a module of a Supervisory Control And Data Acquisition (SCADA) system is supposed to receive data from a Programmable Logic Controller (PLC) and save it. Application security contains best practices to ensure that the module is not susceptible to buffer-overflow attacks and that the data it receives does not get corrupted as it is handled by the module.

Application Security is a complex and extensive area involving the design, implementation, and testing of program modules as well as the testing and monitoring of integrated systems after implementation. Utilities should develop standard design and implementation requirements that define the testing required by software vendors and system integrators, as well as doing their own testing of the integrity of results.

Encryption

This category is concerned with ensuring that only appropriate encryption schemes are used within an organization's security systems and that the cryptography is used wherever it is needed. For example, there is general confusion of what is an appropriate encryption scheme: sometimes packing or compression algorithms are called encryption. Also, cryptographic systems must be used wherever they are needed, for example, if the data will be traveling on a public channel or via a wireless circuit, or if there is a need to provide non-repudiation of a message or a document (by using a cryptographic signature).

Weak encryption schemes are particularly dangerous because they provide little protection and create a false sense of security and complacency. Proprietary encryption schemes should be avoided since they typically have not gone through comprehensive testing and often contain flaws. Also, only encryption schemes that are referenced by appropriate standards and use keys of proper length should be considered secure.

Data Security

This category is concerned with various types of protected data that a utility may collect, transfer and store. This includes payment information like credit and debit cards, personally identifiable information (PII), and health information protected according to Health Insurance Portability and Accountability (HIPAA) requirements. These requirements are included in this category.

Telecommunications, Network Security, and Architecture

This category is concerned with the security of the network infrastructure from the data connector on the wall to the enterprise switches, routers, and firewalls. This includes the physical security of the cables, the telecom closets, and the computer rooms, and the protection of the data as it travels on public channels and wireless circuits. Spam filtering and website blocking are also included in this category.

The focus of this category is establishing a "defense-in-depth" network architecture with the network at its core. It also addresses adherence to new standards for PCS network security, particularly network topology requirements within the vicinity of PCS systems and PLC controls. Another area addressed in this category is network management, including port level security.

Physical Security of PCS Equipment

Physical security is a basic requirement for all PCS and enterprise systems. Once physical access to a network device or server is achieved, compromising equipment or systems is usually a trivial matter. The recommended practices in this category focus on preventing and restricting physical access to only authorized personnel with a need to perform some action on the hardware. The recommendations in this group are also related to monitoring, detecting, and responding to unauthorized physical access.

Service Level Agreements (SLA)

This category is concerned with the definition and management of contracts that specify services requirements to the organization. The contract manager under the direction of the executive team is responsible for defining, negotiating, executing, and monitoring these contracts to ensure appropriate service delivery to the organization.

An SLA is a contract which requires minimum levels of performance for services provided. For example, the Committed Information Rate (CIR) is part of a typical Wide-Area Network (WAN) SLA and specifies the minimum bandwidth that a data circuit may have.

SLAs for PCS network systems typically focus on quality of service (QoS) rather than bandwidth. PCS systems do not require high bandwidth but cannot operate properly if the bandwidth falls below certain known thresholds. Conversely, SLAs for enterprise systems will focus on confidentiality and integrity of information stored or in transit on the network.

Operations Security (OPSEC)

OPSEC is concerned with refining operational procedures and workflows to increase the security properties (CIA) of an organization. For example, a utility may want to restrict what employees post on their social media pages about the organization's security procedures. OPSEC also includes access granting policies and procedures, security guard rotation schedules, backup recovery procedures, etc.

Education

This category is concerned with bringing security awareness to the employees, clients, and service providers of the organization.

Education involves identifying best practices and providing formal training on the security policies and procedures of the enterprise as well as security awareness and incident response. It involves test practice of the key security processes and actions to ensure quick and accurate response to security incidents within the enterprise.

Personnel Security

This category is concerned with the personal safety of employees, clients, contractors, and the general public. Personnel security starts as part of the hiring process and ends after the employee leaves the organization. It handles periodic reaccreditation of employees and updates of the policies and procedures that govern staff. The purpose of personnel security is to ensure the safety and integrity of staff within the organization. Personnel security also applies to external contractors and service personnel, with the objective to ensure appropriate, lower privileged access to facilities.

Cyber-Informed Engineering

Cyber-Informed Engineering (CIE)[6, 7] and the associated Consequence-Centered, Cyber-Informed Engineering (CCE)[8] are methodologies recently developed and promulgated by Idaho National Laboratory (INL). The methodologies emphasize the integration of cyber risk considerations into the full engineering life-cycle to reduce risk. These approaches recognize that, while extremely important, a cyber-hygiene centered approach cannot address the rapidly evolving cyber threats that all critical infrastructure owners and operators face. Therefore, utilities need to take additional measures to ensure that their systems are cyber-resilient.

[6] Anderson, Robert S., Benjamin, Jacob, Wright, Virginia L., Quinones, Luis, and Paz, Jonathan. Cyber-Informed Engineering. United States: N. p., 2017. Web. https://doi.org/10.2172/1369373

[7] Wright, Virginia. Cyber-Informed Engineering. Fermilab Colloquium. September 21, 2016. https://vms.fnal.gov/asset/detail?recid=1944478&recid=1944478

[8] Bochman, Andy. The End of Cybersecurity. Harvard Business Review. May 2018.

CYBERSECURITY TOOL USER GUIDANCE

Overview

The Assessment Tool uses several steps to collect user input on the utility's current cybersecurity posture and provides recommended controls to facilitate AWIA §2013 compliance and cybersecurity improvements. PLEASE NOTE: AWWA DOES NOT COLLECT ANY DATA ENTERED INTO THE TOOL OR ABOUT USERS OF THE TOOL. Rather, this guidance and the Assessment Tool provide the user with recommended controls based on how the utility describes the application of certain technologies and practices in their day-to-day operations. No security sensitive information is required or shared by the user. The process flow of the tool is segmented to address the two primary phases of AWIA §2013, 1) Risk and Resilience Assessment (RRA; dark blue box) and 2) Emergency Response Planning (ERP; green box), is illustrated in Figure 1.

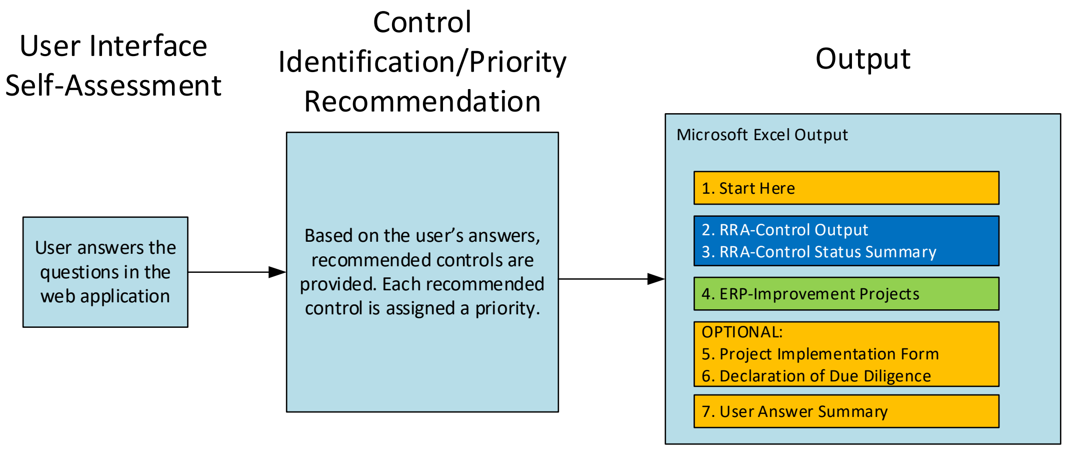

User Interface Self-Assessment
Control Identification/Priority Recommendation
Output
User answers the questions in the web application
Based on the user's answers, recommended controls are provided. Each recommended control is assigned a priority.
Microsoft Excel Output
1. Start Here
2. RRA-Control Output
3. RRA-Control Status Summary
4. ERP-Improvement Projects
OPTIONAL:
5. Project Implementation Form
6. Declaration of Due Diligence
7. User Answer Summary

Figure 1. AWWA Cybersecurity Tool Process

The following sections provide additional detail on the individual inputs, processing steps, and outputs of the AWWA Assessment Tool.

User Interface

First, the user answers questions on the policies, procedures and use of their PCS and enterprise systems in the web application. The AWWA Assessment Tool automatically maps the utility's PCS and enterprise system configuration and practices to the recommended control. The questions designed to capture the utility's PCS and enterprise system configuration and practices are included in a worksheet format in Appendix C of this guidance.

Use-Cases

A use-case is an elemental pattern of behavior as described by the user of a system; the use-cases in this document are basic descriptions of important processes from the user's perspective. Based on the use-cases selected, the tool provides recommended cybersecurity controls. Appendix D includes a table summarizing the use-cases included in the tool. These are no longer visible to the user, but were retained to maintain consistent mapping of controls.

Cybersecurity Controls

A security control is a measure to support effective cyber defense. Most of the controls in this document are measures designed to reduce risk; they were developed from many industry standards which were correlated, integrated, and enhanced. For example, multiple similar controls were merged into a single, more comprehensive control. Some controls are complex and might resemble an administrative program, a computer system, or an engineering design methodology. Many cybersecurity service vendors provide computer systems to implement controls of greater complexity (e.g., network monitoring tools). Appendix E provides a list of the cybersecurity controls developed for this document and a table mapping the controls presented in Appendix E to the controls presented in the NIST Cybersecurity Framework v1.1 is included as Appendix F.

Each control was assigned a priority level based on its criticality and potential impact to the security of the utility. The recommended controls are categorized into priorities 1, 2, 3, and 4, with priority 1 being the highest. For each recommended control, a reference is provided to a set of existing cybersecurity standards. Priority levels are adapted from SANS[9] and are defined as follows:

- **Priority 1 Controls** – These controls represent the minimum level of acceptable security for PCS and enterprise systems. If not already in place, these controls should be implemented immediately. In some cases, they could be considered q*uick wins* that provide solid risk reduction without major procedural, architectural, or technical changes to an environment. Alternatively, a control may provide substantial and immediate risk reduction against common attacks. Generally, these will be cyber-hygiene measures. Utilities with many Priority 1 controls to implement will likely be reactive to any cyber-attack.

- **Priority 2 Controls** – These controls build on those in the Priority 1 category. Despite being Priority 2, these controls have the potential to provide a significant and immediate increase in the security of the organization. Generally, these will be more sophisticated cyber-hygiene measures to improve the process, architecture, and technical capabilities of the utility. These improvements include capabilities such as monitoring of networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

- **Priority 3 Controls** – These controls improve information security configuration and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage. These controls lay the foundation for sustained implementation of a managed security system. These controls include

[9] SANS. CIS Critical Security Controls: Guidelines. https://www.sans.org/critical-security-controls/guidelines. Last accessed May 1, 2019.

more sophisticated longer-term approaches to managing cyber-risk including CIE and cyber supply chain risk management.

- **Priority 4 Controls** – These controls are more complex and provide proactive protection against more sophisticated attacks. These include new technologies, policies, and methods that provide maximum security but are more complex and potentially more expensive than commoditized security solutions.

Maturity is a concept that is widely used in other sectors. Generally, the maturity of an organization's cybersecurity posture is the extent to which a utility has implemented the recommended controls. It is also reflective of a utility moving from a *reactive* to a *proactive* cybersecurity posture. Adapted from SANS,[10] Figure 2 illustrates notional levels of maturity.

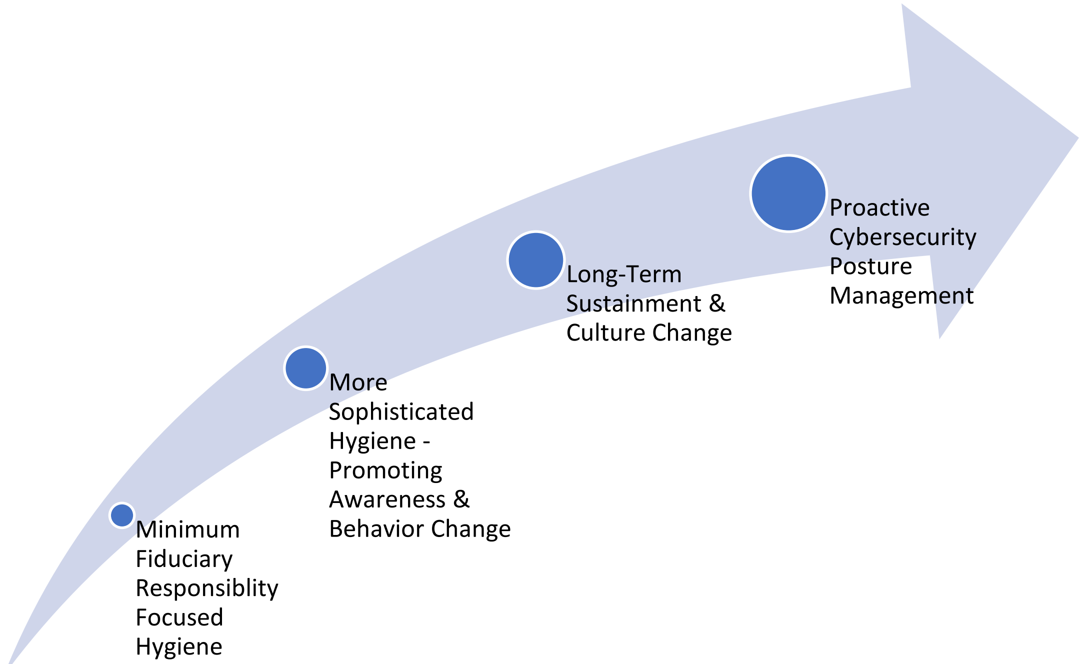

Minimum Fiduciary Responsiblity Focused Hygiene
More Sophisticated Hygiene - Promoting Awareness & Behavior Change
Long-Term Sustainment & Culture Change
Proactive Cybersecurity Posture Management

Figure 2. Conceptual Cybersecurity Maturity Levels of an Organization

The maturity levels in Figure 2 are comparable to Tiers 1 through 4 in the NIST Cybersecurity Framework. The Tiers range from Tier 1 – Partial to Tier 4 - Adaptive. The Tiers describe the degree to which a utility's cybersecurity risk management practices exhibit the characteristics defined in the NIST Cybersecurity Framework.[11]

Using this guidance and the Assessment Tool, utilities should assess the controls in place and their associated implementation status (i.e. maturity) on a recurring basis relative to the current and anticipated needs of the organization, the current cybersecurity posture of the organization, and the

[10] SANS.org. https://www.sans.org/sites/default/files/10_24%20Blog%203%20Commandments.png. Last accessed May 1, 2019.

[11] NIST Cybersecurity Framework. An Introduction to the Components of the Framework. https://www.nist.gov/cyberframework/online-learning/components-framework. Last accessed May 28, 2019.

threat landscape. Broadly, the objective should be to continuously move from the minimum controls in place for fiduciary responsibility and a reactive posture to a proactive posture.

Recommended Cybersecurity Practices and Improvement Projects

Each Practice Category identified in has numerous associated recommended controls and potential improvement projects. Some additional details on potential improvement projects are provided below:

1. **Governance and Risk Management**
   a. Develop a formal, written Cybersecurity Policy that addresses the specific operational needs of PCS and enterprise systems.
   b. Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans.
   c. Perform a vulnerability assessment (e.g. CSET or physical assessment) on a regular basis.
   d. To aid in developing contingency plans, maintain current network asset inventory, baseline, "gold disk," including:
      i. Applications
      ii. Data
      iii. Servers
      iv. Workstations/HMI
      v. Field devices (e.g. PLCs)
      vi. Communications and network equipment
   e. Develop and enforce hardware and software standards in order to limit number of system components
   f. Develop standard specifications language that defines cybersecurity standards for inclusion in all procurement packages for PCS and enterprise systems

2. **Business Continuity and Disaster Recovery**
   a. Develop resilience plans including: Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan. These plans should include:
      i. Crisis Management Team (including at least one representative from executive management) – with authority to declare an alert or a disaster and who monitors and coordinates the necessary recovery activities.
      ii. Manual overrides to allow temporary manual operations of key processes during an outage or a cyber-attack.
      iii. Strategies for system redundancy (or offline standby) to ensure key system components can be restored within acceptable timeframes.
   b. Ensure that corporate Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan includes procedures and contact list for PCS and enterprise systems.
   c. Conduct exercises to test and revise plans and build organizational response capabilities.

d. Implement change management program for PLC software; maintain fully commented backups for all PLC programs and test restore process on a periodic basis.
e. Implement change management program for enterprise systems with routine backups and restoration exercises.
f. Test backup and recovery plans regularly.

3. Server and Workstation Hardening

a. Implement whitelisting (allows only specified applications to execute on each specific computer).
b. Maintain support contracts with HMI software vendor and implement antivirus, anti-malware, and operating system patches in accordance with vendor's direction.
c. Implement security patch management program with periodic vulnerability scanning.
d. Implement change management program for applications and infrastructure (routers, etc.)
e. Harden critical servers and workstations.
f. Remove local administrator rights, delete/disable default accounts (OS and application).
g. Rename Administrator account.
h. Disable USB, DVD, and other external media ports.
i. Disable auto-scan of removable media.

4. Access Control

a. Secure PCS and enterprise system access.
    - i. Physical access to facilities and equipment.
    - ii. Application access to key software functions.
    - iii. External access should be controlled. Address requirements for:
        1. File exchange into or out of a network. Include system and software updates.
        2. Data exchange between PCS and enterprise systems such as email (alarms), historical databases, CMMS, LIMS, etc.
        3. Establish off-line or isolated system for testing and patch management, including applications and device programs.
        4. Identify what is required for remote access. Restrict remote access to lowest level of privilege required.
    - iv. Vendor, contractor system access on plant (incl. package systems). Vendor or contractor access to system should be manually initiated.
    - v. Equipment (e.g. network equipment, field devices) access

b. Secure remote access
    - i. Use VPN technologies to protect information in transit.
    - ii. Require multifactor authentication (e.g. tokens) for remote access to sensitive functions.
    - iii. Limit access to only the minimal level required (e.g. view-only web page).

c. Implement multi-factor authentication for all workstations.

d. Laptops that are used to control PCS or program field devices should be "dedicated for PCS use only" and ports to Internet disabled. All non-essential software should be removed.

5. Application Security

a. Require each PCS or enterprise system user to utilize unique credentials (usernames and passwords) which provide only the required level of access needed to perform their job. Establish policy for strength of password and periodic renewal. Implement automatic lock out after adjustable number of failed log-in attempts.

b. Provide separate accounts for administrator and user functions. Do not allow users to operate with administrator rights unless they are actually administering the system.

c. Provide separate credentials for PCS access compared to enterprise system access. Require different passwords between systems.

d. Implement audit controls such as logging and monitoring of system access and modification.

e. Aggregate system logs and conduct frequent review of network, application and systems events.

6. Encryption

a. Implement device and/or storage encryption where theft or loss of a device is a possibility:

   i. Smartphones, tablets containing sensitive system information.

   ii. Laptops containing programs or other sensitive information.

   iii. Equipment (e.g. administrator passwords).

   iv. Removable media (e.g. tape, disk, USB removable storage).

b. Implement communications encryption:

   i. Wireless communications should be encrypted where possible, regardless of type or range.

   ii. Wired communications over shared infrastructure (e.g. leased, shared) should be encrypted using VPN technologies to protect sensitive information in transit.

c. Implement "best available" encryption.

   i. Use strongest available encryption on existing equipment.

   ii. Identify encryption requirements in specifications for new equipment.

d. Implement encryption of confidential data in on-line repositories.

7. Data Security

a. Implement appropriate measures to accept, process, store, and/or transmit customer billing information. The Payment Card Industry (PCI) priorities include:

   i. Remove sensitive authentication data and limit data retention.

   ii. Protect systems and networks, and be prepared to respond to a system breach.

   iii. Secure payment card applications.

   iv. Monitor and control access to your systems.

        v. Protect stored cardholder data.
        vi. Finalize remaining compliance efforts, and ensure all controls are in place.

b. Implement controls to protect Personally Identifiable Information (PII)
    i. Understand how PII is defined based on local, state, and federal statutes
    ii. Develop a privacy policy.
    iii. Develop a data breach response policy.

c. Implement controls to achieve and maintain HIPAA compliance
    i. Establish a program to maintain minimal compliance with HIPAA requirements.
    ii. Develop a privacy policy.
    iii. Develop a data breach response policy.

8. Telecommunications, Network Security, and Architecture

a. Implement Layered Network Security with multiple levels of protection
    i. Utilize stateful or application layer firewalls, filtering routers, packet filtering or similar devices between networks.
    ii. Implement Intrusion Detection/Prevention Systems to identify and alarm on or block unauthorized access.
    iii. Implement security information and event management (SIEM)/anomaly detection to provide real-time monitoring of all PCS equipment and enterprise systems.

b. Implement network separation
    i. Implement physical (e.g. dedicated hardware) and/or logical separation (IP subnets, VLANs) to protect sensitive functions:
        1. Between PCS, enterprise systems, and other networks.
        2. Within PCS and enterprise systems:
            a. Servers
            b. HMI
            c. Field equipment
            d. Network management
            e. Third party controlled equipment
        3. Over shared communications equipment or links

c. Implement port-level security on all network devices.

d. Evaluate the risks and benefits of “pulling the plug” between PCS and the outside world.

e. Develop an architecture that will allow critical operations to continue if isolated.

f. Implement network management system to monitor system performance and identify potential bottlenecks.

g. Document and periodically review PCS network architecture and enterprise system network architecture (including definition of network boundaries).

9. **Physical Security of PCS Equipment**

    a. Control access to:

        i. Unused network ports
        ii. Removable media
        iii. Equipment cabinets and closets
        iv. Control room
        v. Facilities
        vi. Communications pathways

10. **Service Level Agreements**

    a. Identify all external dependencies and establish written Service Level Agreements and support contracts with internal and external support organizations to clearly identify expectations for response time and restoration of shared or leased network infrastructure and services, including equipment or services provided by:

        i. Equipment or service managed by IT departments
        ii. PCS vendors
        iii. Telecommunications and Internet providers
        iv. Power sources/power supply (within facilities)
        v. System vendors
        vi. System integrators

    b. Leverage procurement policies to limit number of external support organizations.

    c. Establish SLA's with staff and contracted employees for responsiveness and agreement to respond in emergency conditions.

11. **Operations Security (OPSEC)**

    a. Provide clear demarcation between business and PCS functions. Isolate all non-PCS functions and block access from PCS equipment to:

        i. Internet browsing
        ii. Email
        iii. Any other non-PCS access to remote systems or services

    b. Implement mobile device and portable media controls.

12. **Cyber Informed Engineering**

    a. Conduct a consequence / impact analysis to prioritize scenarios.
    b. Design and implement a system architecture to limit the potential impacts of an attack.
    c. Include engineered controls in addition to traditional IT controls.
    d. Simplify system design to the extent practical.
    e. Conduct resilience planning to improve response and recovery actions.
    f. Control information on the engineering of the system to prevent unwanted distribution.
    g. Control procurement processes.

h. Control system interdependencies.
i. Establish and maintain a cyber-aware culture of employees, contractors, and visitors.
j. Complete a digital asset inventory to document hardware, software, and firmware currently in use.

13. Education

a. Implement a cybersecurity awareness program that includes social engineering.
b. Provide on-going cross training for enterprise system and PCS staff that identifies current best practices and standards for PCS cybersecurity.
c. Provide basic network and radio communications training for PCS technicians.
d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.
e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.
f. Provide periodic security awareness training to all employees that identifies risky behaviors and threats.
g. Promote information sharing within your organization.

14. Personnel Security

a. Implement a personnel security program for internal and contracted personnel that includes:
    i. Training
    ii. Periodic background checks
b. Require annual and new employee signoff on cybersecurity policy(ies), which includes agreeing to a confidentiality statement

AWWA Assessment Tool Output

The AWWA Assessment Tool currently produces an automatically generated output file to help utilities achieve both compliance and improve their cybersecurity posture. This file is designed to facilitate a cycle of improvement through an easily repeatable and documentable process. These outputs are detailed in the following sections.

This output is automatically generated as a Microsoft Excel spreadsheet workbook. This file is designed to support utilities with compliance requirements of AWIA §2013. In addition, the output file is formatted in a manner to support building an improvement plan. Use of this output file involves the following steps:

- Step 1. Select the implementation status of each recommended control from a drop-down list on the RRA-Control tab.
- Step 2. Review the results on the RRA-Control Status Summary tab.
- Step 3. On the ERP-Improvement Projects tab, select the table column headers, navigate to the Data tab at the top of the spreadsheet, and select the Filter tool in your Excel ribbon. On the Improvement Project column, click the filter icon in the cell and select "Partially Implemented" and "Planned and Not Implemented." On the Priority column select "Sort Smallest to Largest." Sorting by Control Status and Priority allows the user to identify the highest priority

recommended controls for implementation. Additional grouping of the recommended controls may be done by sorting of the "Improvement Projects" column.

- Step 4. Use the project implementation plan to design cybersecurity improvement projects.
- Step 5. Complete the Declaration of Due Diligence for communication with utility leadership and for documenting compliance.
- Step 6. Print the results for inclusion with compliance documentation, communication with stakeholders, and improvement project/risk and resilience management strategy development.

There are seven tabs in the file, including:

Tab 1. **Start Here** – This tab provides context and high-level instructions for the use of the output file.

Tab 2. **RRA-Control Output** – This summarizes the recommended cybersecurity controls, provides users the functionality to document the recommenced cybersecurity control status, and identifies improvement projects. This tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013. This is the only tab that requires user input.

Tab 3. **RRA – Control Status Summary** – This tab provides two tables. The first summarizes the recommended controls' status by priority. This is shown in a "heat map" format to visually indicate the number of controls of various priority and their associated status. The second table identifies the number of controls associated with each improvement project categories as identified in the guidance document. These projects account for recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented" on the RRA-Control Output tab.

Tab 4. **ERP-Improvement Projects** – This tab provides two tables. The first is the same as the second table on tab 3. The second table is a sorted version of the controls summarized on tab 2. The intent of this second table is to allow the user to aggregate controls into projects. This table provides Priority 1 controls across each practice area. This tab is designed to facilitate compliance with the ERP requirements included in AWIA §2013. Mitigation strategies and resources may include equipment, policies and people. Once controls are aggregated into projects on this sheet, these may be grouped together using the Project Implementation Form included as tab 5.

Tab 5. **Project Implementation Form** – This is an optional sample project planning form. Full completion of the information in this form will facilitate successful project delivery.

Tab 6. **Declaration of Due Diligence** – The optional draft form is provided for use with the AWWA Assessment Tool output. The draft text is intended to facilitate communication with utility decision makers and support long-term cybersecurity risk management.

Tab 7. **User Answer Summary** – This tab provides a summary of AWWA Assessment Tool questions and associated user answers. Also included on this tab is a control status summary table. This table is presented in a "heat map" format to visually indicate the importance of controls by priority and status.

Additional details for the RRA-Control Output (Tab 3) and ERP-Improvement projects tabs (Tab 4) are provided in the following sections.

RRA-Control Output Tab

The RRA-Control Output tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013 by supporting "…assessment of the risks to, and resilience of, its system." This tab lists each of the controls recommended by the tool based on the user inputs. The recommended controls are categorized into Priorities 1, 2, 3, and 4, with Priority 1 being the highest. For each control, there are multiple columns that are available to the user to provide documentation of the level of implementation of each control at their organization.

Within this tab, the Control Status column is the only column that requires additional user input. The cells requiring input are colored blue for identification purposes. The user must select the implementation status of the recommended control within the utility/system/facility under evaluation.

The options for implementation levels include:

1. **Not Planned and/or Not Implemented** – Risk Accepted – The control is not currently implemented or planned for implementation. The organization accepts risks associated with the control not being implemented.
2. **Planned and Not Implemented** – The control has not been implemented. However, implementation of the control is planned.
3. **Partially Implemented** – The control is partially implemented by internal or external resources.
4. **Fully Implemented and Maintained** – The control is fully implemented and actively maintained by internal or external resources.

Utility staff should use the output to document controls already in place and those that are most important to implement. This will likely require working with additional stakeholders to document the state of implementation of the various recommended controls. Improvement project categories are provided for each recommended control.

ERP-Improvement Projects Tab (Tab 4)

This tab is designed to facilitate compliance with the ERP requirements included in AWIA §2013 (b) "Emergency Response Plan", including:

- "(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;"
- "(2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;"
- "(3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and"
- "(4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system."

There are two tables within this output tab. The first is the Cyber Resilience Improvement Projects table. This table identifies improvement projects and the associated number of controls. Additional rows are available for user-identified projects. These projects address all recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented."

The second table is the Control Summary. This table provides a summary of controls and levels of implementation from user input on the RRA-Control Output tab. This is provided in a heat map format to allow a utility to easily see a high-level control summary organized by control status and priority.

Utility staff should use this output to create an implementation strategy for the most important controls identified by the RRA Support Output. It is important to note that this will likely require working with additional stakeholders to document a strategy for implementation of additional controls.

REFERENCE STANDARDS

To provide the user with more detailed information on the steps necessary to implement the recommended cybersecurity controls, specific references to existing AWWA, NIST, and International Society of Automation (ISA) standards are provided. The references provide the specific paragraph or section number in the referenced standard in which the applicable information can be found. Table 3 provides a list of the referenced standards. Each standard listed is publicly available; however, access to several of the standards listed below require payment.

List of Standards & Guidance

	Name	Version/Revision Date
ANSI/AWWA G430-14	Security Practices for Operation and Management	November 2014
ANSI/AWWA G440-17	Emergency Preparedness Practices	August 2017
AWWA J100-10 (R13)	Risk and Resilience Management of Water and Wastewater Systems	2013
AWWA Manual M19	Emergency Planning for Water and Wastewater Utilities, Fifth Edition	2018
DHS-CAT	U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers	April 2011
DHS ICS-CERT	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies	September 2016
HIPAA	45 Code of Federal Regulations (CFR) Part 160 and Part 164	August 2002
INL CIE	Cyber-Informed Engineering	March 2017
ISA 62443-1-1	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models	October 2007
ISA 62443-2-1	Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program	January 2009
ISA TR62443-2-3-2015	Security for industrial automation and control systems Part 2-3: Patch management in the IACS environment	2015
ISA 62443-3-3	Security for industrial automation and control systems	August 2013

	Name	Version/Revision Date
	Part 3-3: System security requirements and security levels	
ISA-62443-4-1-2018	ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements	2018
ISA-62443-4-2-2018	Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components	2018
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	October 2013
ISO/IEC 27003	Information technology — Security techniques — Information security management system implementation guidance	February 2010
ISO/IEC 27005	Information technology — Security techniques — Information security risk management	June 2011
PCI-DSS v3.2.1	Payment Card Industry – Data Security Standard	May 2018
NIST Cybersecurity Framework	Cybersecurity Framework v1.1	April 2018
NIST 800-34r1	Contingency Planning Guide for Federal Information Systems	May 2010
NIST 800-53r4	Security and Privacy Controls for Federal Information Systems and Organizations	April 2013
NIST 800-61r2	Computer Security Incident Handling Guide	August 2012
NIST 800-82r2	Guide to Industrial Control Systems (ICS) Security	May 2015
NIST 800-124r1	Guidelines for Managing the Security of Mobile Devices in the Enterprise	June 2013
NIST 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	April 2015
Various	State specific data breach laws	Various

Appendix A: America's Water Infrastructure Act (AWIA) of 2018 §2013

SEC. 2013. COMMUNITY WATER SYSTEM RISK AND RESILIENCE.

(a) Risk and Resilience Assessments.-

(1) In general.-- Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system. Such an assessment—

(A) shall include an assessment of—

(i) the risk to the system from malevolent acts and natural hazards;

(ii) the resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;

(iii) the monitoring practices of the system;

(iv) the financial infrastructure of the system;

(v) the use, storage, or handling of various chemicals by the system; and

(vi) the operation and maintenance of the system; and

(B) may include an evaluation of capital and operational needs for risk and resilience management or the system.

(2) Baseline information.--The Administrator, not later than August 1, 2019, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information on malevolent acts of relevance to community water systems, which shall include consideration of acts that may--

(A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or

(B) otherwise present significant public health or economic concerns to the community served by the system.

(3) Certification.—

(A) Certification.--Each community water system described in paragraph (1) shall submit to the Administrator a certification that the system has conducted an assessment complying with paragraph (1). Such certification shall be made prior to—

(i) March 31, 2020, in the case of systems serving a population of 100,000 or more;

(ii) December 31, 2020, in the case of systems serving a population of 50,000 or more but less than 100,000; and

(iii) June 30, 2021, in the case of systems serving a population greater than 3,300 but less than 50,000.

(B) Review and revision.--Each community water system described in paragraph (1) shall review the assessment of such system conducted under such paragraph at least once every 5 years after the applicable deadline for submission of its certification under subparagraph (A) to determine whether such assessment should be revised. Upon completion of such a review, the community water system shall submit to the Administrator a certification that the system has reviewed its assessment and, if applicable, revised such assessment.

(4) Contents of certifications.--A certification required under paragraph (3) shall contain only--

(A) information that identifies the community water system submitting the certification;

(B) the date of the certification; and

(C) a statement that the community water system has conducted, reviewed, or revised the assessment, as applicable.

(5) Provision to other entities.--No community water system shall be required under State or local law to provide an assessment described in this section (or revision thereof) to any State, regional, or local governmental entity solely by reason of the requirement set forth in paragraph (3) that the system submit a certification to the Administrator.

(b) Emergency Response Plan.--Each community water system serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates findings of the assessment conducted under subsection (a) for such system (and any revisions thereto). Each community water system shall certify to the Administrator, as soon as reasonably possible after the date of enactment of America's Water Infrastructure Act of 2018, but not later than 6 months after completion of the assessment under subsection (a), that the system has completed such plan. The emergency response plan shall include—

(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;

(2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;

(3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and

(4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

Appendix B: Network Architecture Reference Diagram and Definitions

PCS and enterprise system architecture provides an extensive list of new terminology for users of this guidance document and AWWA Assessment Tool to learn and understand. The Industrial Control System – Computer Emergency Response Team (ICS-CERT) has provided an exceptional resource for PCS owners and operators to refer to. The secure architecture design in Figure 3[12] "is the result of an evolutionary process of technology advancement and increasing cyber vulnerability presented in the Recommended Practice document, *Control Systems Defense in Depth Strategies*."[13] While this is specifically directed at PCS owners and operators, much of the terminology is compatible with enterprise systems.

[12] ICS-CERT. *Secure Architecture Design*. https://ics-cert.us-cert.gov/Secure-Architecture-Design#nogo. Last accessed May 1, 2019

[13] DHS. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf. Last accessed May 1, 2019. September 2016.

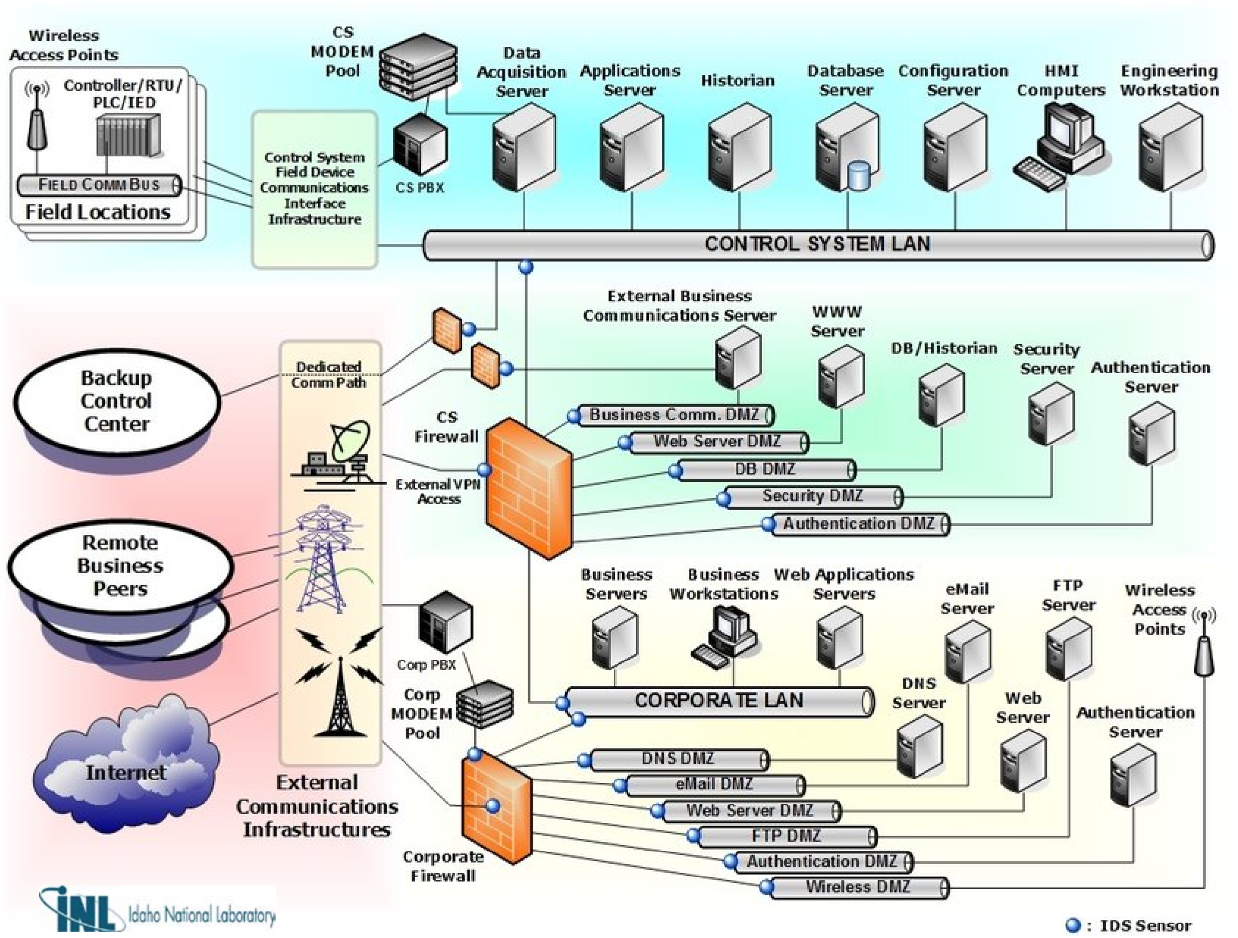


Figure 3. Secure Architecture Design

Appendix C: User Interface Questions

#	Question	Additional Details	Yes /No
1	Are any data transferred to or from your PCS network, by any electronic means?	Examples of electronic data transfer include both automatic (e.g. automated export of data from the PCS environment) and manual (e.g. transfer of data to/from the PCS environment via thumb drive). Examples of data that may be transferred include: • Water quality data collected by the PCS and transferred for regulatory reporting • Asset performance data for asset management • Operating system / software patches and updates	
2	Do users manually transfer any electronic data to or from your PCS environment?	Users include anyone internal or external with access to PCS. This may include operators, technicians, and third-party consultants. Users are able to initiate transfer of data to and from the PCS. Examples of manual data transfer include: • USB • Portable media device • Temporary network connections (an ad hoc network connection for transferring data from one computer to another) • Shared drives • Cloud file share (e.g. DropBox)	
3	Are any electronic data transferred to or from your PCS environment using an automated process, without user interaction?	Examples of automated transfer of data include: • Automated software or firmware updates • Licensing • Operating System updates • Antivirus signatures • Database transfer • Network monitoring by devices external to the PCS	

#	Question	Additional Details	Yes /No
4	Are any users allowed to access your PCS environment remotely?	Users include any personnel with internal or external access to the PCS environment. These may include operators, technicians, and third-party consultants. Devices can be any network enabled device either corporate supplied or personal. Examples of remote access include: • Operations staff access the PCS environment from mobile device. This includes web view and read only. • Users have access to remote physical site using any non-PCS environment.	
5	Is remote access to your PCS network allowed via mobile devices?	Devices can be any network enabled device either corporate supplied or personal. This includes web view and read only. Examples of mobile devices include: • Laptops • Tablets • Cellphones • Smart Phones	
6	Is remote access to your PCS allowed at physically secured fixed location(s)?	Examples of remote access from physically secured fixed location include: • Control center managing remote sites • Control center remotely managing a treatment center • Office desktop computer • Computer at secured office used for managing remote booster station	
7	Do you use resources outside your organization to support and/or maintain your PCS environment?	Examples of resources outside of the organization supporting and/or maintaining your PCS environment include: • Subsystems owned and operated by 3rd party • Systems Integrators • Equipment Manufacturers • Consultants • Vendors	

#	Question	Additional Details	Yes /No
8	Do resources (e.g. service providers) outside your organization provide PCS support via remote access?	Examples of resources outside your organization providing support by remote access includes: - "Black box" solution vendor - "Black box" refers to piece of equipment on a network with contents and/or function that are unknown to the user/owner/operator. - Vendor panel solution - Vendor panel refers to a control panel provided by a vendor to monitor or operate a treatment or distribution process. For example: a vendor provided ultrafiltration unit would have an accompanying control panel to control the ultrafiltration process. - Network administration, from external sources.	
9	Do internal staff provide support for your PCS via remote access?	Remote access is from outside (for example, from home) of the controlled or control room environments. Devices can be any smart phone, tablet, laptop either corporate supplied or personal. Examples of internal staff providing support by remote access include: - Remote operation and monitoring - Remote troubleshooting	
10	Are all changes or updates made to your PCS environment first tested in a development, testbed, non-production, and/or training environment prior to being deployed and implemented in the field/production environment?	- These changes/updates include any programming of logic controllers, human machine interfaces, instrumentation, or any devices involved with the PCS. - System changes or updates do not negatively impact PCS operation. - PCS changes are tested in a non-production environment before they are made in the field/production environment. - Testing is performed to ensure the proper operation and interaction with other system components before deployment. - Changes or updates may be made by either internal or external resources.	
11	Does your PCS include 3rd party network communication services?	Examples of 3rd party network communications services include: - Cellular (3G, 4G, 5G) - Dedicated leased line (copper, fiber) - Communication over internet - City/county communication network not dedicated to PCS	

#	Question	Additional Details	Yes /No
12	Does your PCS network use licensed or unlicensed wireless radios between facilities?	Unlicensed wireless spectrum frequencies – Unlicensed wireless devices operate in one of the frequency bands set aside by the Federal communications Commission (FCC) for industrial, scientific or medical (ISM) applications. Frequencies within the unlicensed wireless spectrum are free to use. Licensed wireless spectrum frequencies – Frequencies or frequency bands designated by the Federal Communications Commission (FCC) as reserved for organizations with licenses. Examples of licensed or unlicensed wireless spectrum services include: • Radio - 450MHz • Radio - 900MHz • WiFi - 2.4GHz • WiFi - 5GHz • WiFi - 6GHz • Microwave	
13	Does your PCS share a LAN or WAN with non-PCS equipment?	Examples of non-PCS equipment include: • Security cameras • Access control equipment • Enterprise network services at a facility with a shared communication path • Voice over Internet Protocol (VOIP) • Fire Alarms • Vault or Panel Intrusion Alarms	
14	Do you use Wi-Fi within the PCS environment to transfer data in support of operations or monitoring?	• Does your PCS communication network have wireless access points? • Wi-Fi is defined in IEEE 802.11	
15	Do you use virtualization technology for your PCS?	Virtualization Technology – Technology capable of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. Examples of virtualization technology include: • VMware • Oracle VM • HyperV	

#	Question	Additional Details	Yes /No
16	Is the virtualization technology dedicated to PCS only?	Virtualization Technology – Technology capable of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. • A separate physical host(s) is used for PCS virtual machines. • All non-PCS virtual machines reside on non-PCS physical host(s).	
17	Does your organization accept, process, store or transmit credit card or debit card information, or accept payment with pre-paid cards branded with American Express, Discover, JCB, MasterCard or Visa International logos?	This information may be collected and stored for service payment purposes. Using a third-party company for processing PCI may cut down on risk exposure but does not exclude a company from PCI DSS compliance. Customer billing information including: • Credit/debit card numbers • Credit/debit card numbers with name, expiration date or service code • Sensitive authentication data (including magnetic stripe, PINs, CVV, etc.) NOTE: Includes organizations that have outsourced payment services.	
18	Does your organization own, license, acquire or maintain any personally identifiable information (PII)?	PII is any information that may be used to identify an individual. This includes customers, employees, and contractors. Examples of PII include: • Customer billing information and addresses • Employee personal information, including SSN, birthdate, etc. Each state has its own data breach notification law(s) regarding PII. Depending on the state statute, a non-exhaustive list of possible examples may include (alone or in conjunction with other information) tax identification numbers, social security numbers, government issued identification numbers, account numbers, health information, email addresses in conjunction with a password, unique biometric information, etc.	

#	Question	Additional Details	Yes /No
19	Is your organization an employer that creates or receives health information that is HIPAA protected?	HIPAA defines protected health information (written, electronic, or oral) as information, including demographic data, that identifies an individual (or there is a reasonable basis to believe it can identify an individual) and that relates to: • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual. Examples of HIPAA protected information include: • Employee medical records • Employee vaccine records • Health and safety records may include HIPAA protected records • Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).	
20	Is your organization responsible for the engineering design and implementation of critical infrastructure?	The water/wastewater sector is defined as critical infrastructure by the federal government (42 U.S.C. 5195(e)). Examples of holding responsibility for engineering services include: • Utility has an internal engineering department • Utility hires engineering consultants • You are part of a stakeholder organization that has internal resources or hires external resources to design and implement critical infrastructure	
21	Does your organization have a supply chain risk management program?	Do you currently require your supplier to provide any chain-of-custody documents? An example of supply chain risk management program includes ordering and confirming treatment chemicals are NSF certified.	

#	Question	Additional Details	Yes /No
22	Does your organization have a supply chain risk management program that specifically addresses cybersecurity?	Does the supply chain risk management program specify how delivery for procured products – hardware, software, and/or data will be validated and monitored to ensure their integrity? Examples of specifically addressing cybersecurity in supply chain risk management include: • Documenting information protection practices of supplier • Integrity management program for components provided by sub-suppliers • Supplier contracts include appropriate language to meet objectives of the organization's cybersecurity program	

Appendix D: Cybersecurity Use-Cases

Category/ Code	Use Case	Description
Architecture		
AR1	Dedicated Process Control Network	All network and communications infrastructure is dedicated exclusively to SCADA with no equipment or communications paths shared with non-SCADA networks.
AR2	Shared WAN	Network wide-area communications infrastructure is shared with some non-SCADA networks.
AR3	Shared LAN	Network local-area communications (within control system) is shared with non-SCADA networks.
AR4	Unlicensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using unlicensed (ISM 900 MHz, 2.4 or 5 GHz) spectrum.
AR5	Licensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using licensed spectrum.
AR6	Communications via Internet	Network wide-area communications fully or partially comprised of links over Internet services using public address space.
AR7	Communications via 3rd party carrier	Network wide-area communications fully or partially comprised of links over 3rd party carrier services (e.g. cellular, Metro-E/Ethernet/LAN).
AR8	Dedicated process control server virtualization	Virtualized server infrastructure dedicated to SCADA/Process Control with no equipment shared with non-SCADA/Process Control systems.
AR9	Shared server virtualization	Virtualized server infrastructure shared between SCADA/Process Control and non-SCADA/Process Control systems.
AR10	802.11 Wireless used in Control System	802.11 unlicensed wireless technologies used within control system.
AR11	Connection to non-SCADA Network	Connection to non-SCADA network through direct connection or firewall/DMZ.
Network Management & System Support		
NM1	Local network management and system support by SCADA/Process Control personnel in physical proximity of equipment	Access to configure network infrastructure located in immediate vicinity of user (serial or network) by SCADA/Process Control personnel.
NM2	Plant network management and	Access to configure network equipment located on same facility from centralized location by SCADA/Process Control personnel.

Category/ Code	Use Case	Description
	system support by SCADA/Process Control personnel	
NM3	Remote network management and system support by SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by SCADA/Process Control personnel.
NM4	Local network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in immediate vicinity of user (serial or network) by non-SCADA/Process Control personnel.
NM5	Plant network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in another physical facility by non-SCADA/Process Control personnel.
NM6	Remote network management and system support by non-SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by non-SCADA/Process Control personnel.
Program Access		
PA1	Outbound messaging	Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.
PA2	Outbound file transfer	Interactive sending of files from system to other locations by user.
PA3	Inbound file transfer	Interactive receiving of files from other locations to system by user.
PA4	Software updates	Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.
PA5	Data exchange	Automated, non-interactive exchange of data (e.g. database-to-database exchange, ntp or other external data) with systems located externally. (Implies full-time connection.)
PA6	Network management communications	Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)

Category/ Code	Use Case	Description
PLC Programming and Maintenance		
PLC1	Local PLC programming and maintenance	Access to PLC programming and maintenance is local to device (serial or network).
PLC2	Plant PLC programming and maintenance	Access to PLC programming and maintenance from a centralized on-site location.
PLC3	Remote PLC programming and maintenance	Access to PLC programming and maintenance from an off-site location.
PLC4	Third party SCADA/Process Control presence	SCADA/PCS equipment (e.g. PLC, RTU) owned and operated by third party (e.g. business partner) located on SCADA/Process Control network with external access by third party.
PLC5	Third party SCADA/Process Control package systems	SCADA/PCS sub-systems owned and operated by third parties located within plant facility with direct network connection to SCADA/Process Control system (package system) with on-site access by third party.
User Access		
UA1	Control room system access with control	Access to system with full read-write capability from on-plant, physically-secure "control room" location.
UA2	Plant system access with control from fixed locations	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).
UA3	Remote system access with control from fixed locations	Access to system with full read-write and/or read-only/view-only capability from location outside "control room" environment and located outside the physical perimeter of the facility workstations or HMI.
UA4	Remote system access with web view from fixed locations	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated computer.
UA5	Plant system access with control from mobile device	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor) on mobile device.
UA6	Remote system access with control from mobile device	Access to system with full read-write capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.
UA7	Remote system access with	Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.

Category/ Code	Use Case	Description
	view-only from mobile device	
UA8	Remote system access with web view from mobile device	Access to web displays of system data with read-only/view capability from location outside “control room” environment and located outside the physical perimeter of the facility via web browser on non-dedicated mobile device.
UA9	Training environment	System training conducted on production SCADA/Process Control system by third parties.
UA10	Development environment by SCADA/Process Control staff	System development conducted on production SCADA/Process Control network by SCADA/Process Control personnel.
UA11	Development environment by external staff or third parties	System development conducted on production SCADA/Process Control network by non-SCADA/Process Control personnel.
Data Security		
DS1	Accept, store or process credit card information	Organization accepts, processes, stores, or transmits credit or debit card information or certain pre-paid payment cards.
DS2	Storage of PII	Organization owns, licenses, acquires or maintains PII.
DS3	Storage or maintenance of protected health information that is HIPAA protected.	Organization creates or receives protected health information.
Cyber Informed Engineering		
CIE1	Engineering design and implementation of critical infrastructure.	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threat during the design and implementation phase.
Supply Chain		
SU1	Supply chain risk management program	Organization has a supply chain risk management program.
SU2	Supply chain risk management program cybersecurity.	Organization’s supply chain risk management process addresses cybersecurity.

Appendix E: Cybersecurity Controls

AT: Awareness and Training		***Cybersecurity Practice Areas/Recommended Projects***	***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.	Education	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.	Education; Cyber-Informed Engineering	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.
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.	Governance and Risk Management	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: Audit and Accountability		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	Application Security; Governance and Risk Management	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-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.	Governance and Risk Management	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.	Governance and Risk Management	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.	Governance and Risk Management	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.	Business Continuity and Disaster Recovery	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-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	Governance and Risk Management; Business Continuity and Disaster Recovery	The business continuity plan is revised annually. Revisions are informed by planned exercises, actual events, or documented changes.
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	Business Continuity and Disaster Recovery	The PCS has a testing/development environment to allow changes to be implemented without immediate effects to the production environment.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Governance and Risk Management	Reviews of the organization’s confidentiality/non-disclosure agreements are periodically scheduled by a responsible party.
CM: Configuration Management		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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.	Governance and Risk Management	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.	Governance and Risk Management	The Emergency Response Plan is stored in a central repository and clearly displays the version and date of when it was implemented.
CM-3	Separation of duties implemented for user processes including risk of abuse.	Application Security; Governance and Risk Management	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.	Application Security; Personnel Security; Governance and Risk Management	A SCADA technician must have a second technician review changes made to production equipment before they are implemented.
CM-5	SLAs for all third parties established, including levels of service and change controls.	SLA	A security policy that outlines which access permissions are distributed to third party employees.
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Governance and Risk Management	Inviting all affected parties to discussions to prevent the development of vulnerabilities in the facility.
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.	Telecommunications, Network Security, and Architecture; SLA	IT monitors SCADA computers for processor usage that could indicate cryptojacking activity.

A: Identification and Authentication & Access Control		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Access Control; Application Security; Governance and Risk Management	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.	Access Control; Application Security; Governance and Risk Management	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.	Access Control; Application Security; Governance and Risk Management	SCADA software implements unique usernames and passwords with different levels of control based on roles.
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).	Access Control; Application Security; Governance and Risk Management	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-5	Access control for diagnostic tools and resources and configuration ports.	Access Control	PLC programming software is only available at select workstations and only accessible to SCADA technicians.
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Access Control; Service Level Agreements; Governance and Risk Management	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.	Access Control; Governance and Risk Management	To use the plant guest network, users are required to accept a user agreement.
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	Governance and Risk Management	An operator misplaces a managed phone. Based on the missing equipment policy, they contact IT to report the device lost.
IA-9	Multifactor authentication system established for critical areas.	Access Control	Remote access to the SCADA system requires two factor-authentication.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Governance and Risk Management	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.	Access Control	The controls to critical equipment are only available at a local secured terminal.
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	Access Control	An operator attempts to connect to a known hacking website. The connection is blocked. The operator and IT are notified of the attempt.

IR: Incident Response, Contingency Planning, & Planning		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
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.	Governance and Risk Management; Data Security	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.	Governance and Risk Management; Data Security	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.	Governance and Risk Management; Data Security	The Emergency Response Plan is reviewed and updated once a year by responsible staff.

MA: Maintenance		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Service Level Agreement Governance and Risk Management; Cyber-Informed Engineering	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-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.	Governance and Risk Management	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.
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	Governance and Risk Management	The condition of offsite equipment and risk factors acting on the equipment are periodically reviewed and assessed via an independent party.

MP: Media Protection		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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).	Governance and Risk Management	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.
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	Governance and Risk Management	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.	Governance and Risk Management	Company policies and procedures are available in a central, secure, shared location.

PE: Physical and Environmental Protection		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
PE-1	Security perimeters, card-controlled gates, manned booths, and procedures for entry control.	Access Control; Physical Security	Personnel are required to present a badge to access the PCS.
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Access Control; Physical Security	Access to the server room is restricted to authorized staff only.
PE-3	Physical security and procedures for offices, rooms, and facilities.	Access Control; Governance and Risk Management; Physical Security	Staff lock doors that allow access to PCS assets. Security guards inspect doors to make sure they are locked properly.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Access Control; Physical Security	Fire suppression unit installed around critical equipment.
PE-5	Physical security and procedures for working in secure areas.	Access Control; Physical Security	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.	Access Control; Physical Security	Server room and PLC cabinets are isolated from areas that delivery personnel and customers may visit.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	Physical Security	The utility monitors facilities using security cameras.
PE-8	Physical/logical protection against power failure of equipment UPS.	Physical Security; Service Level Agreements	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.	Physical Security	A utility has a standby power source with separated power cabling for critical sites.

PM: Program Management & Security Assessment and Authorization		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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.	Governance and Risk Management; Cyber-Informed Engineering	A database is used to keep track of building conditions in the facility.
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	Governance and Risk Management;	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.	Telecommunications, Network Security, and Architecture; Governance and Risk Management;	A utility has a network intrusion detection system (NIDS) to monitor network traffic.
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	SLAs; Governance and Risk Management	Third parties must review and sign an information exchange policy before connecting to the system.
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	Governance and Risk Management	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.

PS: Personnel Security		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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.	Governance and Risk Management; Personnel Security	A background check on employees is required before they may be given access to the PCS system.
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third-party users.	Governance and Risk Management; Personnel Security	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.	Governance and Risk Management; Personnel Security	Confidential documents are stored in locked file cabinets when not in use, as required by policy.
PS-4	Disciplinary process for security violations established.	Governance and Risk Management; Personnel Security	An operator who props open doors to critical areas could face disciplinary action as outlined in the utility's policies and procedures.

RA: Risk Assessment		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	Governance and Risk Management	A third-party system integrator would need to contact IT before connecting to the system's network.
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.	Governance and Risk Management; SLAs	System integrators can only access the facility's equipment remotely from a Virtual Private Network (VPN) connection.
SA: System and Services Acquisition		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
SA-1	Authorization process established for new systems or changes to existing information processing systems.	Governance and Risk Management	A change management/review process is used to evaluate suggested changes to facility.
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.	Governance and Risk Management; SLAs	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.	Governance and Risk Management; Server and Workstation Hardening	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.	Operations Security; Governance and Risk Management	Remote access is restricted to only the most necessary applications and only allowed through secure measures.
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	Governance and Risk Management	System backups are tested on a regular basis by completing a system restoration to the test environment.
SI: System and Information Integrity		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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.	Governance and Risk 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.	Governance and Risk Management	Acquired assets are inspected, assessed, and documented before implementation with existing systems.

SI-3	Interactive system for managing password implemented to ensure password strength.	Access Control; Application Security	When configuring a new user's password, it must meet minimum character length requirements.
SI-4	Organization-wide clock synchronization system in place.	Telecommunications, Network Security, and Architecture	All managed network devices synchronize their clocks to a known good source.
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.	Application Security; Telecommunications, Network Security, and Architecture	Utility has implemented tiered access so non-administrator users are unable to make changes to system security settings.
DS: Data Security		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
DS-1	A program established to ensure compliance with the minimum PCI requirements for your associated level.	Governance and Risk Management; Data Security	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.	Business Continuity and Disaster Recovery; Governance and Risk Management; Data Security	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.	Business Continuity and Disaster Recovery; Governance and Risk Management; Data Security	Current practices are reviewed by legal counsel for legal compliance with HIPAA.
CIE: Cyber-Informed Engineering		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
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.	Cyber-Informed Engineering	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.
SU: Supply Chain		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
SU-1	A supply chain risk management program.	Governance and Risk Management	Chain of custody documentation is required for all chemicals used in treatment.
SU-2	A supply chain risk management program that includes cybersecurity.	Governance and Risk Management	Preferred vendors for computer hardware, software and peripherals are identified and selected based on evaluation of their supply chain among other criteria.

SC: System and Communications Protection		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	Governance and Risk Management	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communication.
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Access Control; Application Security	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.	Governance and Risk Management	All external communication with the PCS is implemented via DMZ.
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.	Governance and Risk Management; Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are placed on a separate subnet.
SC-5	Anomaly based IDS/IPS established including policies and procedures.	Telecommunications, Network Security, and Architecture	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.
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	Governance and Risk Management; Telecommunications, Network Security, and Architecture	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
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.	Governance and Risk Management; Telecommunications, Network Security, and Architecture	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.	Operations Security; Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are placed on a separate subnet rather than being on a single "flat" network.
SC-9	Process isolation established to provide a manual override “air gap” between highly sensitive systems and regular environments.	Operations Security; Telecommunications, Network Security, and Architecture	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-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).	Server and Workstation Hardening; Governance and Risk Management	Ports are disabled for all network devices when not in use.
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).	Server and Workstation Hardening; Governance and Risk Management	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.	Access Control; Governance and Risk Management	Remote access to the SCADA system requires two factor-authentication.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Governance and Risk Management	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.	Operations Security; Telecommunications, Network Security, and Architecture	"Whitelisting" of network components is done to manage data transfer between and within network segments.
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.	Operations Security; Telecommunications, Network Security, and Architecture	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.	Operations Security; Telecommunications, Network Security, and Architecture	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-17	Virtual Local Area Network (VLAN) for logical network segregation.	Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are on a separate subnet.
SC-18	Minimize wireless network coverage.	Telecommunications, Network Security, and Architecture	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-19	802.1X user authentication on wireless networks.	Telecommunications, Network Security, and Architecture	No "open" WiFi connections are allowed.
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.	Telecommunications, Network Security, and Architecture	WiFi equipment in the plant does not connect directly to SCADA network.
SC-21	Unique wireless network identifier SSID for control network.	Telecommunications, Network Security, and Architecture	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).	Telecommunications, Network Security, and Architecture	A wireless LAN specific domain controller is in place.
SC-23	Wireless communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture	All data transferred via the wireless network is encrypted using current wireless communication best practices.
SC-24	Communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture	All data transferred via the wired network is encrypted using current wireless communication best practices.
SC-25	VPN using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	Encryption; Telecommunications, Network Security, and Architecture	An operator who can access the system remotely must do so through a secured VPN client configuration.

Appendix F: Cross Reference to NIST 1.1 Cybersecurity Framework

The following table provides a cross-reference between the Cybersecurity Controls incorporated into the AWWA Cybersecurity Guidance Tool and the Framework Core (Appendix A) included in the Cybersecurity Framework issued by NIST on April 16, 2018.

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY	Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried	PM-2
		ID.AM-2	Software platforms and applications within the organization are inventoried	PM-2
		ID.AM-3	Organizational communication and data flows are mapped	PM-2
		ID.AM-4	External information systems are catalogued	MA-3
		ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	PM-5
		ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	PE-4, PS-2
	Business Environment	ID.BE-1	The organization's role in the supply chain is identified and communicated	RA-2, PS-2, CM-5
		ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	MA-2
		ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	IR-2
		ID.BE-4	Dependencies and critical functions for delivery of critical services are established	IR-2
		ID.BE-5	Resilience requirements to support delivery of critical services are established	IR-3
	Governance	ID.GV-1	Organizational information security policy is established	IR-2, AU-2
		ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PS-2, AU-4, AU-6
		ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	IR-3
		ID.GV-4	Governance and risk management processes address cybersecurity risks	AU-3, AU-5, CM-6
	Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented	AU-5, RA-1, IR-2
		ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	AU-5, PM-3, IR-2

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY – cont'd		ID.RA-3	Threats, both internal and external, are identified and documented	AU-5, RA-1, IR-2
		ID.RA-4	Potential business impacts and likelihoods are identified	AU-5, RA-1, IR-2
		ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	AU-5
		ID.RA-6	Risk responses are identified and prioritized	IR-1
	Risk Management Strategy	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	IR-2
		ID.RM-2	Organizational risk tolerance is determined and clearly expressed	SA-4
		ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	SC-4
	Supply Chain Risk Management	ID.SC-1:	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SU1
		ID.SC-2:	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	SU2
		ID.SC-3:	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	SU2
		ID.SC-4:	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	SU1
PROTECT	Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users	IA-1, RA-1, SC-19
		PR.AC-2	Physical access to assets is managed and protected	PE-1, PE-2, PE-3
		PR.AC-3	Remote access is managed	IA-7, SC-12, SC-18, SC-21, RA-2
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	IA-3, SC-22
		PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	SC-8, SC-9, SC-14, SC-15, SC-16, SC-17, SC-20, SC-25

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*	Awareness & Training	PR.AT-1	All users are informed and trained	AT-1, AT-2
		PR.AT-2	Privileged users understand roles & responsibilities	AT-1, AT-2
		PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	AT-2
		PR.AT-4	Senior executives understand roles & responsibilities	AT-1
		PR.AT-5	Physical and information security personnel understand roles & responsibilities	PS-4, AT-1
	Data Security	PR.DS-1	Data-at-rest is protected	PM-5, MP-2
		PR.DS-2	Data-in-transit is protected	PM-4, SC-14, SC-23, SC-24
		PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	PM-1
		PR.DS-4	Adequate capacity to ensure availability is maintained	MA-1, CM-7
		PR.DS-5	Protections against data leaks are implemented	IA-4
		PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	IR-3
		PR.DS-7	The development and testing environment(s) are separate from the production environment	CM-4
	Information Protection Processes and Procedures (IP)	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained	SA-3
		PR.IP-2	A System Development Life Cycle to manage systems is implemented	CM-1, CM-6
		PR.IP-3	Configuration change control processes are in place	SA-3
		PR.IP-4	Backups of information are conducted, maintained, and tested periodically	SA-5
		PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	PE-4
		PR.IP-6	Data is destroyed according to policy	MP-1
		PR.IP-7	Protection processes are continuously improved	AU-6
		PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	AU-7
		PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	ANSI/AWWA J100/G440/M19
		PR.IP-10	Response and recovery plans are tested	PS-4

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – ***cont.***		PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	AT-2
		PR.IP-12	A vulnerability management plan is developed and implemented	AU-5
	Maintenance	PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-1
		PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-1
	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PM-3
		PR.PT-2	Removable media is protected and its use restricted according to policy	MP-1
		PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality (whitelisting)	SC-10, SC-19
		PR.PT-4	Communications and control networks are protected	IA-7
DETECT	Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	Not addressed
		DE.AE-2	Detected events are analyzed to understand attack targets and methods	SC-5
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	Not addressed
		DE.AE-4	Impact of events is determined	PM-3
		DE.AE-5	Incident alert thresholds are established	CM-7
	Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events	CM-7
		DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	PE-1, CM-7
		DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	CM-7, SA-5
		DE.CM-4	Malicious code is detected	SC-5
		DE.CM-5	Unauthorized mobile code is detected	SA-4
		DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	IA-2
		DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	PS-1
		DE.CM-8	Vulnerability scans are performed	IR-2
	Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability and adequate awareness of anomalous events	PS-2
		DE.DP-2	Detection activities comply with all applicable requirements	IR-3

Function	Category	Sub-Category	Description	AWWA Guidance Control
DETECT – ***cont.***		DE.DP-3	Detection processes are tested	ANSI/AWWA G430, G440
		DE.DP-4	Event detection information is communicated to appropriate parties	IA-2
		DE.DP-5	Detection processes are continuously improved	SC-4
RESPOND	Response Planning	RS.PL-1	Response plan is executed during or after an event	AT-1
	Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed	ANSI/AWWA G430, G440
		RS.CO-2	Events are reported consistent with established criteria	G430
		RS.CO-3	Information is shared consistent with response plans	SC-6
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans	ANSI/AWWA G430, G440
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	MA-2
	Analysis	RS.AN-1	Notifications from detection systems are investigated	SC-5
		RS.AN-2	The impact of the incident is understood	ANSI/AWWA J100
		RS.AN-3	Forensics are performed	AT-3
		RS.AN-4	Incidents are categorized consistent with response plans	AT-3
	Mitigation	RS.MI-1	Incidents are contained	IR-1
		RS.MI-2	Incidents are mitigated	IR-1
		RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	IR-2
	Improvements	RS.IM-1	Response plans incorporate lessons learned	ANSI/AWWA G430, G440
		RS.IM-2	Response strategies are updated	ANSI/AWWA G430, G440
RECOVER	Recovery Planning	RC.RP-1	Recovery plan is executed during or after an event restoration of systems or assets affected by cybersecurity events	AU-7
	Improvements	RC.IM-1	Recovery plans incorporate lessons learned	ANSI/AWWA G430, G440
		RC.IM-2	Recovery strategies are updated	ANSI/AWWA G430, G440
	Communications	RC.CO-1	Public relations are managed	ANSI/AWWA G430, G440
		RC.CO-2	Reputation after an event is repaired	ANSI/AWWA G430, G440
		RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	ANSI/AWWA G430, G440

NOTES

NOTES

About AWWA

AWWA is an international, nonprofit, scientific and educational society dedicated to providing total water solutions assuring the effective management of water. Founding 1881, the Association is the largest organization of water supply professionals in the world. Our membership includes nearly 4,200 utilities that supply roughly 80 percent of the nation’s drinking water and treat almost half of the nation’s wastewater. Our over 50,000 total memberships represent the full spectrum of the water community: public water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource. AWWA unites the diverse water community to advance public health, safety, the economy, and the environment.

Appendix L
CATALOG OF RECOMMENDATIONS

Catalog of Control Systems Security: Recommendations for Standards Developers

April 2011

Homeland Security

Control Systems Security Program

National Cyber Security Division

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, or any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

ACKNOWLEDGMENT

This document was developed by the U.S. Department of Homeland Security to help facilitate the development of control systems cybersecurity industry standards. The original author team consisted of representatives from the Department of Homeland Security Control Systems Security Program (CSSP), National Institute of Standards and Technology (NIST), Argonne National Laboratory (ANL), Idaho National Laboratory (INL), Oak Ridge National Laboratory (ORNL), Pacific Northwest National Laboratory (PNNL), and Sandia National Laboratories (SNL).

For additional information or comments, please send inquires to the Control Systems Security Program at cssp@hq.dhs.gov with the word “Catalog” in the subject line.

EXECUTIVE SUMMARY

This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommendations in this catalog are grouped into 19 families, or categories, that have similar emphasis. The recommendations within each family are displayed with a summary statement of the recommendation, supplemental guidance or clarification, and a requirement enhancements statement providing augmentation for the recommendation under special situations.

This catalog is not limited for use by a specific industry sector. All sectors can use it to develop a framework needed to produce a sound cybersecurity program. The number of new and updated published Cyber Security Standards and guidelines has increased significantly this past year. An attempt has been made to reference and include the best practices introduced by these new and updated documents to interested users for consideration as input into individual industrial cybersecurity plans under development and review. This catalog should be viewed as a collection of guidelines and recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cybersecurity standards for control systems. The recommendations in this catalog are intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cybersecurity standards specific to their individual security needs. These recommendations are subservient to existing legal rules and regulations pertaining to specific industry sectors, and the user is urged to consult and follow those applicable regulations.

CONTENTS

TABLES

ACRONYMS

AC	access control
AGA	American Gas Association
AT	awareness and training
AU	audit and accountability
CA	security assessment and authorization
CAG	consensus audit guidelines
CC	critical control
CD	compact disc
CIKR	critical infrastructures and key resources
CIP	critical infrastructure protection
CM	Configuration Management
CP	Contingency Planning
DHS	Department of Homeland Security
DNS	Domain Name System
DOE	Department of Energy
DVD	digital video disc
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IA	identification and authenticity
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	IP Security
IPS	intrusion prevention system
IR	incident response
ISA	International Society of Automation
ISO	International Organization for Standardization

IT	information technology
Key	cryptographic key
MA	System Development and Maintenance
MP	media protection
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OSI	Open System Interconnection
PDF	portable document file
PE	physical and environmental protection
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	planning
PM	program management
PS	personnel security
RA	risk assessment
RFID	radio frequency identification
RG	regulatory guide
SA	system and services acquisition
SC	System and communications protection
SCADA	Supervisory Control and Data Acquisition
SD	secure digital memory card
SI	system and information integrity
SP	Special Publication
TCB	Trusted Computing Base
UHF	ultra high frequency
USB	universal serial bus
US-CERT	United States Computer Emergency Readiness Team
VHF	very high frequency
VoIP	Voice-Over Internet Protocol
VPN	Virtual Private Network

Catalog of Control Systems Security: Recommendations for Standards Developers

1. INTRODUCTION

Protecting critical infrastructures and key resources (CIKR) is essential to the security, public health and safety, economic vitality, and way of life for our nation's citizens. Fundamental to the protection of CIKR is ensuring the security of the systems that control these infrastructures. Developing and applying robust security standards enables control systems to be secure.

Development of security standards specific to CIKR control systems is maturing. However, many standards lack the detailed guidance needed to ensure adequate protection from the emerging threats of cyber attacks on control systems. This catalog of recommended security controls is specifically designed to provide various industry sectors the framework needed to develop sound security standards, guidelines, and best practices. These recommendations are not intended to replace the need for applying sound engineering judgment, best practices, and risk assessments. Decisions regarding when, where, and how these standards should be used are best determined by the specific industry sectors. This document provides those decision-makers with a common catalog (framework) from which to select security controls for control systems.

The term "control systems," as used throughout this document, includes supervisory control and data acquisition systems, process control systems, distributed control systems, and other control systems specific to any of the critical infrastructure industry sectors. Although differences in these systems exist, their similarities enable a common framework for discussing and defining security controls. Currently, control system security standards and guidelines are being created by a variety of Standards Development Organizations to meet the needs of different industry sectors and regulatory environments. However, the standards produced for a specific sector may not always be consistent, compatible, or comparable with similar standards developed in another sector. These developing standards often have differing priorities, emphases, and levels of detail concerning specific security controls based on specific industrial acceptable risks and regulations.

This document attempts to encompass these differences and provide a way to clarify security programs for similar control systems. Use of this document is not limited to a specific industry sector. This catalog should be viewed as a collection of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cybersecurity standards for control systems. While many of the documents referenced in the preparation of this catalog are still in draft or do not apply directly to control systems, they still supply information useful for the security of control systems.

Throughout the development of this document, the following aspects of control systems were considered:

- **Proprietary Control System Technology**—A large percentage of deployed control system hardware and software is proprietary. However, some vendors are moving toward marketing products that use nonproprietary, commercial off-the-shelf technologies, as these newer systems provide more functions, with better efficiency, costs (acquisition, operation, and maintenance), and effectiveness. Control system networks also may use proprietary or industry-specific protocols. The proprietary nature of installed control systems currently requires professionals with system-specific knowledge to operate them, but that is slowly changing as older systems get replaced and upgraded.

- **Control System Equipment Life Cycle**—The life cycle for control system hardware is from 5 to 15 years (or more) as compared to the 2 to 3-year (or shorter) life cycle for information technology (IT) business systems. Building security into control system equipment is a recent development.

Typically, legacy control systems do not contain the standard security functionality included in many IT systems such as cryptography or auditing.

- **Real Time Operation**—The systems that control CIKR are designed and constructed to be in operation continuously. Any interruption in service may have catastrophic results to human life and property. This is a key difference between control systems and IT business systems. Real time operation presents a unique challenge for securing these systems because security cannot compromise the reliable operation of the control system.

The goal of a control systems security program is to balance security while operating within resource limits. When developing a security policy to address control systems, these characteristics must be considered. Security is not meant to impede operation and should be as transparent as possible. The most successful security program is one that integrates seamlessly and becomes a common aspect of daily operation. The intent of this document is to help facilitate such a program.

2. RECOMMENDATIONS FOR STANDARDS DEVELOPERS

This section contains a detailed listing of recommended controls from several sources. The organization of each recommendation is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, but modified to convey control system language. The recommended controls are organized into families primarily based on NIST SP 800-53 and include contributions from "Key Elements to a Cyber Security Management System," (Clause 5) found in the Draft Instrumentation, Systems, and Automation Society (ISA)-d9900.02 document. The families have been realigned from the format of NIST SP 800-53, Revision 3 to facilitate the security management of the control system environments. However, all the families addressed in NIST SP 800-53, Revision 3 are also addressed in this document. A cross-reference of the subsections below in Section 2 and the NIST SP 800-53, Revision 3 families is provided in Table 1. Table 1 demonstrates that this document expands on the NIST SP 800-53, Revision 3 families by adding subsections addressing *Security Policy*, *Organizational Security*, *Information and Document Managemen*t, and *Monitoring and Reviewing Control System Security Policy* to provide a comprehensive catalog of control systems security recommendations.

Table 1. Catalog of Recommendations and NIST SP 800-53 comparison.

Catalog of Recommendations Subsections	NIST SP 800-53 Revision 3 Families
2.1 Security Policy	Each of the 18 control family initial elements relates to its own policy and procedures (e.g., AC- 1 through PM-1)
2.2 Organizational Security	Access Control—AC Program Management—PM
2.3 Personnel Security	Access Control—AC Personnel Security—PS
2.4 Physical and Environmental Security	Access Control—AC Physical and Environmental Security—PE
2.5 System and Services Acquisition	System and Services Acquisition—SA
2.6 Configuration Management	Configuration Management—CM
2.7 Strategic Planning	Planning—PL
2.8 System and Communication Protection	Access Control—AC System and Communication Protection—SC
2.9 Information and Document Management	Contingency Planning—CP Media Protection—MP
2.10 System Development and Maintenance	Maintenance—MA
2.11 Security Awareness and Training	Awareness and Training—AT
2.12 Incident Response	Incident Response—IR
2.13 Media Protection	Media Protection—MP
2.14 System and Information Integrity	System and Information Integrity—SI
2.15 Access Control	Access Control—AC Identification Authentication—IA
2.16 Audit and Accountability	Audit and Accountability—AU

Table 1. (continued).

Catalog of Recommendations Subsections	NIST SP 800-53 Revision 3 Families
2.17 Monitoring and Reviewing Control System Security Policy	Security Assessment and Authorization—CA
2.18 Risk Management and Assessment	Assessment and Authorization—CA Risk Assessment—RA
2.19 Security Program Management	Program Management—PM

This DHS catalog contains 250 recommended controls compared to 347 controls defined in NIST SP 800-53 Revision 3. Of these controls, seven catalog of recommendation controls are not specifically addressed in NIST SP 800-53 Revision 3. NIST SP 800-53 Revision 3 does not ignore these seven controls; rather, they are implied within several other control families. This change is reflective of the increased granularity for each control element within the NIST document. The new consensus audit guidelines (CAG) and regulatory guide (RG) 5.71 guidelines also follow this trend. As an example, catalog of recommendation control element 2.9.8, “Document Destruction,” addresses document retention and destruction. However, areas, such as visitor control, incident management, and configuration management, require different document retention and destruction requirements and policies. Other areas, such as roles and responsibilities and access control, are also broken down and inserted as needed into control elements to assist the user to understand and effectively deploy the security control being discussed.

The “Requirement” section for each security control includes detailed recommended security practices and mechanisms. The “Supplemental Guidance” section provides additional information that may be beneficial for understanding and implementing the recommendation. The last section, “Requirement Enhancements,” includes supplementary security constraints for the recommendation that will result in a more secure environment based on the organization’s predetermined level of protection required for the control system used for the critical process. Not all the recommendations are appropriate for all applications, so it will be necessary to determine the level of protection needed and only apply the guidance as appropriate. Industrial controls have an availability requirement that may require compensating controls instead of following the recommendations (see Appendix I of NIST SP 800-53 Revision 3, “Industrial Control Systems”). A few examples of these areas may be password, multiple session, and patch management controls where interference with operations becomes unacceptable because of operational requirements, testing, and certification requirements (e.g., substation automation, certain refinery operations, flight controls). The following recommendations were obtained from a review of the controls found in various industry standards. Similar controls were identified, and a single recommendation was prepared that addressed the intent of the original controls. Appendix A presents a cross reference of standards and guidelines used to develop these recommendations.

2.1 Security Policy

Security policies are the specific controls and behavior expectations that each member of the organization’s staff is required to meet in the daily operation of the control system. The development of the organization’s security policy is the first and most important step in developing an organizational security program. Security policies lay the groundwork for securing the organization’s physical, enterprise, and control system assets. Security procedures define how an organization implements the security policy. Using a predefined security policy best practices guide can help the organization to develop a cogent security policy.

2.1.1 Security Policy and Procedures

2.1.1.1 Requirement

The organization develops, implements, and periodically reviews and updates:

1. A formal, documented, control system security policy that addresses:
    a. The purpose of the security program as it relates to protecting the organization’s personnel and assets
    b. The scope of the security program as it applies to all organizational staff and third-party contractors
    c. The roles, responsibilities, management commitment, and coordination among organizational entities of the security program to ensure compliance with the organization’s security policy and other regulatory commitments.
2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each family contained in this document.

2.1.1.2 Supplemental Guidance

The security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the control system in particular, when required.

2.1.1.3 Requirement Enhancements

None

2.1.1.4 References

NIST SP 800-53r3	AC-1, SC-14, PM-1
CAG	CC-9
API 1164r2	4, 5.5, 7.1.3, Annex A, Annex B.4.1.2
NERC CIPS	CIP 003-3, B.R1
NRC RG 5.71	App. A.2, App. B.1.1

2.2 Organizational Security

Organizational security involves setting organization-wide policies and procedures that define acceptable behavior and practices concerning security. Organizational security includes management accountability, physical controls, and cyber-related functions. Organizational policies and procedures specify direction, commitment, responsibility, and oversight and define the security posture for the control system. These policies and procedures also apply to third-party contractors, integrators, and vendors used by the organization.

2.2.1 Management Policy and Procedures

2.2.1.1 Requirement

The organization establishes policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program.

2.2.1.2 Supplemental Guidance

The scope and responsibilities of the security program include management accountability, physical security, and information security for the enterprise and control systems. This program applies to third-party contractors, outsourcing partners, and the supply chain components of the organization.

2.2.1.3 Requirement Enhancements

None

2.2.1.4 References

NIST SP 800-53r3	PM-1
API 1164r2	1.2, Annex A, Annex B.4.1.2
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. B.3.11

2.2.2 Management Accountability

2.2.2.1 Requirement

The organization defines a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cybersecurity policy, assign security roles, and coordinate the implementation of cybersecurity across the organization.

2.2.2.2 Supplemental Guidance

This framework is not limited to traditional IT systems but also extends to control systems and the organization’s supply chain.

2.2.2.3 Requirement Enhancements

None

2.2.2.4 References

NIST SP 800-53r3	PM-1
API 1164r2	1.2
NERC CIPS	CIP 003-3, B.R2, B.R5

2.2.3 Baseline Practices

2.2.3.1 Requirement

Baseline practices that organizations employ for organizational security include, but are not limited to:

1. Executive management accountability for the security program.
2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization’s security policy.
3. The organization’s security policies and procedures that provide clear direction, accountability, and oversight for the organization’s security team. The security team assigns roles and responsibilities in accordance with the organization’s policies and confirms that processes are in place to protect company assets and critical information.
4. The organization’s contracts with external entities that address the organization’s security policies and procedures with business partners, third-party contractors, and outsourcing partners.

5. The organization’s security policies and procedures that ensure coordination or integration with the organization’s physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.

2.2.3.2 Supplemental Guidance

None

2.2.3.3 Requirement Enhancements

None

2.2.3.4 References

NIST SP 800-53r3	PM-1
API 1164r2	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8
NRC RG 5.71	App. C.11.3

2.2.4 Coordination of Threat Mitigation

2.2.4.1 Requirement

The organization’s security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers, and other relevant organizations in the event of a security incident.

2.2.4.2 Supplemental Guidance

The organization expands relationships with local emergency response personnel to include information sharing and coordination of contingency plans as well as coordinated response to cybersecurity incidents. Entities, such as US-CERT and ICS-CERT, are available for threat assistance.

2.2.4.3 Requirement Enhancements

None

2.2.4.4 References

NIST SP 800-53r3	PM-9
API 1164r2	Section 3, Annex B and B.3
NERC CIPS	CIP 003-3, B.R1

2.2.5 Security Policies for Third Parties

2.2.5.1 Requirement

The organization holds external suppliers and contractors that have an impact on the security of the control center to the same security policies and procedures as the organization’s own personnel. The organization ensures security policies and procedures of second and third-tier suppliers comply with corporate cybersecurity policies and procedures if they will impact control system security.

2.2.5.2 Supplemental Guidance

The organization considers the increased security risk associated with outsourcing as part of the decision-making process to determine what to outsource and what outsourcing partner to select. Contracts with external suppliers govern physical as well as logical access. The organization clearly defines confidentiality or nondisclosure agreements and intellectual property rights. The organization also clearly defines change management procedures.

2.2.5.3 Requirement Enhancements

None

2.2.5.4 References

NIST SP 800-53r3	PS-7
API 1164r2	3.4, 7.3.4, Annex A
NERC CIPS	CIP 004-3, B.R4, B.R4.1
NRC RG 5.71	App. B.1.21

2.2.6 Termination of Third-Party Access

2.2.6.1 Requirement

The organization establishes procedures to remove external supplier physical and electronic access at the conclusion/termination of the contract in a timely manner.

2.2.6.2 Supplemental Guidance

The organization clearly defines the timeliness for removal of external supplier access in the contract.

2.2.6.3 Requirement Enhancements

The organization periodically reviews existing authorized physical and electronic access permissions to ensure they are current. This check provides validation that terminated entities have been removed from physical and electronic access.

2.2.6.4 References

NIST SP 800-53r3	AC-2, PS-4
CAG	CC-9, CC-11
API 1164r2	7.3.4, Annex A
NERC CIPS	CIP 004-3, B.R4, B.4.2
NRC RG 5.71	App. B.1.21, App. C.2.2

2.3 Personnel Security

Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the control system. The organization trains personnel when they are hired and provides subsequent refresher training on their job tasks, responsibilities, and behavioral expectations concerning the security of the control system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of control system facilities must sign before being granted access to the control system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.

2.3.1 Personnel Security Policy and Procedures

2.3.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, personnel security policy that addresses:
    a. The purpose of the security program as it relates to protecting the organization’s personnel and assets
    b. The scope of the security program as it applies to all the organizational staff and third-party contractors
    c. The roles, responsibilities, management commitment, and coordination among organizational entities of the security program to ensure compliance with the organization’s security policy and other regulatory commitments
2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls
3. Formal procedures to review and document the list of approved personnel with access to control systems.

2.3.1.2 Supplemental Guidance

The organization ensures the personnel security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular control system, when required.

2.3.1.3 Requirement Enhancements

None

2.3.1.4 References

NIST SP 800-53r3	PS-1
API 1164r2	3.1
NERC CIPS	CIP 003-3, A, B.R1, B.1.1-1.3
NRC RG 5.71	App. B.1.21, App. C.2.1

2.3.2 Position Categorization

2.3.2.1 Requirement

The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations periodically based on the organization’s requirements or regulatory commitments.

2.3.2.2 Supplemental Guidance

Designated officials within the organization assign a risk level for every position within the control system as determined by the position's potential for adverse impact to the integrity and efficiency of the control system.

2.3.2.3 Requirement Enhancements

None

2.3.2.4 References

NIST SP 800-53r3	PS-2
API 1164r2	3.1
NERC CIPS	CIP 003-3, B.R5.1, B.5.1.1
NRC RG 5.71	App. B.1.21

2.3.3 Personnel Screening

2.3.3.1 Requirement

The organization screens individuals requiring access to the control system before access is authorized.

2.3.3.2 Supplemental Guidance

The organization maintains consistency between the screening process and organizational policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.

Basic screening requirements include:

1. Past 5 years of employment
2. Past 5 years of education, with verification of the highest degree received
3. Past 3 years of residency
4. References
5. Past 5 years of law enforcement records.

2.3.3.3 Requirement Enhancements

The organization rescreens individuals with access to organizational control systems based on a defined list of conditions requiring rescreening and the frequency of such rescreening.

2.3.3.4 References

NIST SP 800-53r3	PS-3
API 1164r2	Annex A
NERC CIPS	CIP 004-3, B.R5.1, B.R5.1.2
NRC RG 5.71	App. B.1.21

2.3.4 Personnel Termination

2.3.4.1 Requirement

When an employee is terminated, the organization revokes logical and physical access to control systems and facilities and ensures all organization-owned property is returned and that organization-owned documents and data files relating to the control system that are in the employee’s possession are transferred to the new authorized owner within the organization. Complete execution of this control occurs within 24 hours for employees or contractors terminated for cause.

2.3.4.2 Supplemental Guidance

Organization-owned property includes system administration manuals, keys, identification cards, building passes, computers, cell phones, and personal data assistants. Organization-owned documents include field device configuration and operational information, control system network documentation.

Exit interviews ensure that individuals understand any security constraints imposed by being a former employee and that proper accountability is achieved for all system-related property.

2.3.4.3 Requirement Enhancements

The organization implements automated processes to revoke access permissions that are initiated by the termination. Periodic reviews of physical and electronic access are conducted to validate that terminated account access was completed.

2.3.4.4 References

NIST SP 800-53r3	PS-4
API 1164r2	Annex A
NERC CIPS	CIP 004-3, B.R4, B.4.2
NRC RG 5.71	App. B.1.2, App. C.2.2

2.3.5 Personnel Transfer

2.3.5.1 Requirement

The organization reviews electronic and physical access permissions to control systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. Complete execution of this control occurs within 7 days for employees or contractors who no longer need to access control system resources.

2.3.5.2 Supplemental Guidance

Appropriate actions may include:

1. Returning old and issuing new keys, identification cards, and building passes
2. Closing old accounts and establishing new accounts
3. Changing system access authorizations
4. Providing access to official records created or managed by the employee at the former work location and in the former accounts.

2.3.5.3 Requirement Enhancements

The organization periodically reviews existing authorized physical and electronic access permissions to ensure they are current. This check is to provide validation that transferred entities have been added, changed, or removed correctly from necessary physical and electronic access.

2.3.5.4 References

NIST SP 800-53r3	PS-5
API 1164r2	Annex A
NERC CIPS	CIP 004-3, B.R4, B.4.2
NRC RG 5.71	App. C.2.2

2.3.6 Access Agreements

2.3.6.1 Requirement

The organization completes appropriate agreements for control system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the control system. The organization reviews and updates access agreements periodically.

2.3.6.2 Supplemental Guidance

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the control system to which access is authorized. Electronic signatures are acceptable for acknowledging access agreements unless specifically prohibited by organizational policy or applicable government regulations.

2.3.6.3 Requirement Enhancements

None

2.3.6.4 References

NIST SP 800-53r3	PS-6
API 1164r2	2.4.2, 2.4.3
NERC CIPS	CIP 004-3, B.R4, B.R.4.1, B.4.2
NRC RG 5.71	App. B.1.1, App. B.1.21

2.3.7 Third-Party Personnel Security

2.3.7.1 Requirement

The organization enforces security controls for third-party personnel and monitors service provider behavior and compliance.

2.3.7.2 Supplemental Guidance

Third-party providers include service bureaus, contractors, and other organizations providing control system operation and maintenance, development, IT services, outsourced applications, and network and security management. The organization explicitly includes personnel security controls in acquisition-related contract and agreement documents.

2.3.7.3 Requirement Enhancements

None

2.3.7.4 References

NIST SP 800-53r3	PS-7
API 1164r2	3.1
NERC CIPS	CIP 004-3, A-3, B.R2.1
NRC RG 5.71	App. B.1.1, App. B.1.21, App. B.1.22, App. B.3.11, App. C.3.5

2.3.8 Personnel Accountability

2.3.8.1 Requirement

The organization employs a formal accountability process for personnel failing to comply with established control system security policies and procedures and clearly documents potential disciplinary actions for failing to comply.

2.3.8.2 Supplemental Guidance

The organization ensures that the accountability process is consistent with applicable federal and local government statutory requirements (directives, policies, and regulations), standards, and guidance. The accountability process can be included as part of the organization’s general personnel policies and procedures.

2.3.8.3 Requirement Enhancements

None

2.3.8.4 References

NIST SP 800-53r3	PS-8
API 1164r2	1.2
NERC CIPS	CIP 003-3, B.R2.1-2.4
NRC RG 5.71	App. B.1.11, App. B.3.11

2.3.9 Personnel Roles

2.3.9.1 Requirement

The organization provides employees and contractors with complete job descriptions and unambiguous and detailed expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.

2.3.9.2 Supplemental Guidance

None

2.3.9.3 Requirement Enhancements

Employees and contractors acknowledge understanding by signature.

2.3.9.4 References

API 1164r2	1.2, 3.1, Annex A
NERC CIPS	CIP 003-3, B.R2, R2.1-2.4
NRC RG 5.71	App. B.1.1, App. C.10.10

2.4 Physical and Environmental Security

Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical security addresses the physical security mechanisms used to create secure areas around hardware. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access control system equipment. Environmental security addresses the safety of assets from damage from environmental concerns. Control system equipment can be very expensive and may ensure human safety; therefore, protection is important from fire, water, and other possible environmental threats.

2.4.1 Physical and Environmental Security Policy and Procedures

2.4.1.1 Requirement

The organization develops, implements, and periodically reviews and updates:

1. A formal, documented physical security policy that addresses:
    a. The purpose of the physical security program as it relates to protecting the organization’s personnel and assets
    b. The scope of the physical security program as it applies to all the organizational staff and third-party contractors

    c. The roles, responsibilities, management commitment, and coordination among organizational entities of the physical security program to ensure compliance with the organization's security policy and other regulatory commitments.

2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

2.4.1.2 Supplemental Guidance

The organization ensures the physical and environmental protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The organization includes the physical and environmental protection policy as part of the general control system security policy for the organization. The organization develops physical and environmental protection procedures for the security program in general and for a particular control system's components when required.

2.4.1.3 Requirement Enhancements

None

2.4.1.4 References

NIST SP 800-53r3	PE-1
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, A, B, R1
NRC RG 5.71	App. B.1.1, App. C.5.1

2.4.2 Physical Access Authorizations

2.4.2.1 Requirement

The organization develops and maintains lists of personnel with authorized access to facilities containing control systems (except for areas within facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

2.4.2.2 Supplemental Guidance

The organization promptly removes from the access list personnel no longer requiring access to facilities containing control system assets or who are denied access based on organizationally defined accountability procedures.

2.4.2.3 Requirement Enhancements

1. The organization authorizes physical access to the facility where the control system resides based on position or role.

2. The organization requires two forms of identification to gain access to the facility where the control system resides.

2.4.2.4 References

NIST SP 800-53r3	PE-2
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, B.R1, R1.5
NRC RG 5.71	C.3.3.1.1, App. C.5.4

2.4.3 Physical Access Control

2.4.3.1 Requirement

Control: The organization:

1. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the control system resides (excluding those areas within the facility officially designated as publicly accessible)
2. Verifies individual access authorizations before granting access to the facility
3. Controls entry to facilities containing control systems using physical access devices and guards
4. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk
5. Secures keys, combinations, and other physical access devices
6. Inventories physical access devices on a periodic basis
7. Changes combinations and keys on an organization-defined frequency and when keys are lost, combinations are compromised, or individuals are transferred or terminated
8. Controls and verifies physical access to information system distribution and transmission lines of communications within the organizational facilities
9. Controls physical access to information system output devices (e.g., monitors, speakers, printers) to prevent unauthorized individuals from observing and obtaining information access.

2.4.3.2 Supplemental Guidance

Physical access devices include keys, locks, combinations, and card readers. Workstations and associated peripherals (monitors, speakers, and printing devices) connected to (and part of) an organizational system should be located in areas designated as limited access such as secure control rooms with access to such devices being safeguarded. This may include protecting, identifying, and inspecting information and communication lines for evidence of tampering. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of Federal Information Processing Standard (FIPS) 201. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76.

2.4.3.3 Requirement Enhancements

1. The organization limits physical access to control system assets independent of the physical access security mechanisms for the facility.
2. The organization performs security checks at physical boundaries for unauthorized removal of information or system components.
3. The organization ensures that every physical access point to the facility where the system resides is guarded or alarmed and monitored 24 hours per day, 7 days per week.
4. The organization employs lockable physical casings to protect internal components of the system from unauthorized physical access.
5. The organization identifies and inspects information and communication lines for evidence of tampering.

2.4.3.4 References

NIST SP 800-53r3	PE-3, PE-4, PE-5
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.4
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. B.1.22, App. C.5.5, App. C.5.6

2.4.4 Monitoring Physical Access

2.4.4.1 Requirement

The organization:

1. Monitors physical access to the control system to detect and respond to physical security incidents
2. Reviews physical access logs on an organization-defined frequency
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

2.4.4.2 Supplemental Guidance

Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities are part of the organization’s incident response capability.

2.4.4.3 Requirement Enhancements

1. The organization monitors real-time physical intrusion alarms and surveillance equipment.
2. The organization implements automated mechanisms to recognize potential intrusions and initiates designated response actions.

2.4.4.4 References

NIST SP 800-53r3	PE-6
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.6
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. C.5.8

2.4.5 Visitor Control

2.4.5.1 Requirement

The organization controls physical access to the system by authenticating visitors before authorizing access to the facility where the system resides other than areas designated as publicly accessible.

2.4.5.2 Supplemental Guidance

Contractors and others with permanent authorization credentials are not considered visitors.

2.4.5.3 Requirement Enhancements

The organization escorts visitors and monitors visitor activity as required according to security policies and procedures.

The organization requires two forms of identification for access to the facility.

2.4.5.4 References

NIST SP 800-53r3	PE-7
API 1164r2	Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.6
NRC RG 5.71	C.3.3.1.1, App. B.1.1

2.4.6 Visitor Records

2.4.6.1 Requirement

The organization maintains visitor access records to the control system facility (except for those areas within the facility officially designated as publicly accessible) that include:

1. Name and organization of the person visiting
2. Signature of the visitor
3. Form of identification
4. Date of access
5. Time of entry and departure
6. Purpose of visit
7. Name and organization of person visited.

2.4.6.2 Supplemental Guidance

Designated officials within the organization review the access logs after close-out and periodically review access logs based on an organization-approved frequency.

2.4.6.3 Requirement Enhancements

The organization employs automated mechanisms to facilitate the maintenance and review of access records.

2.4.6.4 References

NIST SP 800-53r3	PE-8
API 1164r2	Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.6, R1.6.1
NRC RG 5.71	App. B.1.1, App. C.5.9

2.4.7 Physical Access Log Retention

2.4.7.1 Requirement

The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.

2.4.7.2 Supplemental Guidance

None

2.4.7.3 Requirement Enhancements

None

2.4.7.4 References

NIST SP 800-53r3	PE-8
API 1164r2	Annex A
NERC CIPS	CIP 006-3c, A, B, R7
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. C.5, App. C5.9

2.4.8 Emergency Shutoff

2.4.8.1 Requirement

The organization, for specific locations within a facility containing concentrations of control system resources, protects emergency power shutoff capability from unauthorized activation.

2.4.8.2 Supplemental Guidance

The design of the control systems facility includes an emergency shutoff to cut power to critical control system resources outside any area prone to flooding.

2.4.8.3 Requirement Enhancements

The organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.

2.4.8.4 References

NIST SP 800-53r3	PE-10
API 1164r2	Annex A
NRC RG 5.71	C.3.2, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.9 Emergency Power

2.4.9.1 Requirement

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of noncritical control system components in the event of a primary power source loss.

2.4.9.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.9.3 Requirement Enhancements

1. The organization provides a long-term alternate power supply for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
2. The organization provides a long-term alternate power supply for the system that is self-contained and not reliant on external power generation.

2.4.9.4 References

NIST SP 800-53r3	PE-11
API 1164r2	4, Annex A
NRC RG 5.71	C.3.2, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.10 Emergency Lighting

2.4.10.1 Requirement

The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and includes lighting for emergency exits and evacuation routes.

2.4.10.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.10.3 Requirement Enhancements

None

2.4.10.4 References

NIST SP 800-53r3	PE-12
API 1164r2	4, Annex A
NRC RG 5.71	C.3.2, App. C.9

2.4.11 Fire Protection

2.4.11.1 Requirement

The organization implements and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

2.4.11.2 Supplemental Guidance

Fire suppression and detection devices/systems include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.11.3 Requirement Enhancements

1. The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.
2. The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.
3. The organization employs an automatic fire suppression capability in facilities that are not staffed continuously.

2.4.11.4 References

NIST SP 800-53r3	PE-13
API 1164r2	Annex A
NRC RG 5.71	C.3.2

2.4.12 Temperature and Humidity Controls

2.4.12.1 Requirement

The organization regularly monitors the temperature and humidity within facilities containing control system assets and ensures they are maintained within acceptable levels.

2.4.12.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.12.3 Requirement Enhancements

None

2.4.12.4 References

NIST SP 800-53r3	PE-14
NRC RG 5.71	C.3.2

2.4.13 Water Damage Protection

2.4.13.1 Requirement

The organization protects the control systems from damage resulting from water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.

2.4.13.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.13.3 Requirement Enhancements

The organization implements automated mechanisms to close shutoff valves and provide notification to key personnel in the event of a water leak within facilities containing control systems.

2.4.13.4 References

NIST SP 800-53r3	PE-15
NRC RG 5.71	C.3.2, C.9

2.4.14 Delivery and Removal

2.4.14.1 Requirement

The organization authorizes and limits the delivery and removal of control system components (i.e., hardware, firmware, software) from control system facilities and maintains appropriate records and control of that equipment. The organization documents policies and procedures governing the delivery and removal of control system assets in the control system security plan.

2.4.14.2 Supplemental Guidance

The organization secures delivery areas and, if possible, isolates delivery areas from the control system to avoid unauthorized physical access.

2.4.14.3 Requirement Enhancements

None

2.4.14.4 References

NIST SP 800-53r3	PE-16

2.4.15 Alternate Work Site

2.4.15.1 Requirement

The organization establishes an alternate control center with proper equipment and communication infrastructure to compensate for the loss of the primary control system work site. The organization implements appropriate management, operational, and technical security measures at alternate control centers.

2.4.15.2 Supplemental Guidance

Alternate work sites may include government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

2.4.15.3 Requirement Enhancements

The organization provides methods for employees to communicate with control system security staff in case of security problems.

2.4.15.4 References

NIST SP 800-53r3	PE-17
API 1164r2	3.4
NERC CIPS	CIP 002-3, B.R1.2.1, R3
NRC RG 5.71	C.3.2, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.16 Portable Media

2.4.16.1 Requirement

The organization:

1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices
2. Authorizes connection of mobile devices to organizational control systems
3. Monitors for unauthorized connections of mobile devices to organizational control systems
4. Enforces requirements for the connection of mobile devices to organizational control systems
5. Disables control system functionality that provides the capability for automatic execution of code on removable media without user direction
6. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures
7. Applies specified measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

2.4.16.2 Supplemental Guidance

Mobile devices include portable storage media (e.g., USB [Universal Serial Bus] memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Usage restrictions and implementation guidance related to mobile devices can include configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of control system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

2.4.16.3 Requirement Enhancements

1. The organization restricts the use of writable, removable media in organizational control systems.
2. The organization prohibits the use of personally owned, removable media in organizational control systems.
3. The organization prohibits the use of removable media in organizational control systems when the media have no identifiable owner.

2.4.16.4 References

NIST SP 800-53r3	MP-2
API 1164r2	Annex A
NERC CIPS	CIP 007-3, B.R7.1, R7.2
CAG	CC-15

2.4.17 Personnel and Asset Tracking

2.4.17.1 Requirement

The organization implements asset location technologies to track and monitor the movements of personnel and vehicles within the organization’s controlled areas to ensure they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.

2.4.17.2 Supplemental Guidance

None

2.4.17.3 Requirement Enhancements

Electronic monitoring mechanisms alert control system personnel when unauthorized access or an emergency occurs.

2.4.17.4 References

None

2.4.18 Location of Control System Assets

2.4.18.1 Requirement

The organization locates control system assets to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

2.4.18.2 Supplemental Guidance

Physical and environmental hazards include flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Where a completely enclosed (six-wall) border cannot be established, the organization implements and documents alternate measures to control physical access to the control system assets. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.18.3 Requirement Enhancements

The organization considers the risks associated with physical and environmental hazards when planning new control system facilities or reviewing existing facilities. Risk mitigation strategies are documented in the control system security plan.

2.4.18.4 References

NIST SP 800-53r3	PE-18
API 1164r2	Annex A
NERC CIPS	CIP 002-3, B.R1-R4, CIP 006-3, B.R1.1
NRC RG 5.71	C.2, C.3.1, C.3.1.3, C.3.3.3, C.3.3.2.9, C.3.14, C.4

2.4.19 Information Leakage

2.4.19.1 Requirement

The organization protects the control system from information leakage.

2.4.19.2 Supplemental Guidance

The organization considers all forms of information leakage such as removable media, official documents, remote access, misconfigured perimeter security devices, and electromagnetic signals emanations. This requirement supports confidentiality more than availability and, hence, is not as critical for control system applications.

The FIPS 199 security categorization (for confidentiality) of the system and organizational security policy guides the application of safeguards and countermeasures employed to protect the system against information leakage because of electromagnetic signals emanations.

2.4.19.3 Requirement Enhancements

None

2.4.19.4 References

NIST SP 800-53r3	PE-19
API 1164r2	Annex A
NRC RG 5.71	C.3.1.3 , C.3.2, App. B.2.5, App. B.5.1, App. C.2.1, App. C.3.4, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.20 Power Equipment and Power Cabling

2.4.20.1 Requirement

The organization protects control system power equipment and power cabling from damage and destruction.

2.4.20.2 Supplemental Guidance

None

2.4.20.3 Requirement Enhancements

The organization employs redundant power equipment and parallel power cabling paths for the control system.

2.4.20.4 References

NIST SP 800-53r3	PE-9
API 1164r2	4, Annex A
NRC RG 5.71	C.2, C.3.1, C.3.3.2.9

2.4.21 Physical Device Access Control

2.4.21.1 Requirement

The organization employs hardware (cages, locks, cases, etc.) to detect and deter unauthorized physical access to control system devices.

2.4.21.2 Supplemental Guidance

Tamper-evident hardware includes, but is not limited to: (1) metal or hard plastic production-grade enclosures, (2) opaque enclosures with tamper-evident seals or pick-resistant locks for doors or removable covers, and (3) tamper detection/response envelopes with tamper response.

2.4.21.3 Requirement Enhancements

The organization ensures that the ability to respond appropriately in the event of an emergency is not hindered by using tamper-evident hardware.

2.4.21.4 References

NIST SP 800-53r3	PE-3, PE-4, PE-5
API 1164r2	5.9, 8.1
NRC RG 5.71	C.3.3.2.5, App. B.1.1, App. B.1.11, App. B.1.15, App. B.1.19, App. B.4.2, App. B.4.5, App. C.3.1, App. C.5.5, App. C.5.6

2.5 System and Services Acquisition

Systems and services acquisition covers the contracting and acquiring of control system components, software, and services from third parties. The organization includes security as part of the acquisition process to ensure that the products received fit into the organization's security plan and have associated risk commensurate with defined risk acceptance levels. A strong policy with detailed procedures for reviewing acquisitions helps to eliminate the introduction of additional or unknown vulnerabilities into the control system.

2.5.1 System and Services Acquisition Policy and Procedures

2.5.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, system and services acquisition policy that includes control system security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

2.5.1.2 Supplemental Guidance

The organization ensures the system and services acquisition policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular control system when required.

2.5.1.3 Requirement Enhancements

None

2.5.1.4 References

NIST SP 800-53r3	SA-1
CAG	CC-3
API 1164r2	3.1
NRC RG 5.71	C.3.4, C.3.3.3, C.3.3.3.1

2.5.2 Allocation of Resources

2.5.2.1 Requirement

The organization:

1. Includes a determination of control system security requirements for the system in mission/business case planning
2. Determines, documents, and allocates the resources required to protect the control system as part of its capital planning and investment control process.

2.5.2.2 Supplemental Guidance

The organization determines the security controls for the control systems in mission/business case planning and establishes a discrete line item for control system security in its programming and budgeting documentation.

2.5.2.3 Requirement Enhancements

None

2.5.2.4 References

NIST SP 800-53r3	SA-2
API 1164r2	3.6
NRC RG 5.71	C.3.1.1, C.3.1.3, App. B.3.5

2.5.3 Life-Cycle Support

2.5.3.1 Requirement

The organization manages the control system using a system development life-cycle methodology that includes control system security considerations.

2.5.3.2 Supplemental Guidance

None

2.5.3.3 Requirement Enhancements

None

2.5.3.4 References

NIST SP 800-53r3	SA-3
CAG	CC-7
NRC RG 5.71	C.4, C.4.1, C.4.2.1

2.5.4 Acquisitions

2.5.4.1 Requirement

The organization includes the following requirements and specifications, explicitly or by reference, in control system acquisition contracts based on an assessment of risk and in accordance with applicable laws, directives, policies, regulations, and standards:

- Security functional requirements/specifications
- Security-related documentation requirements
- Developmental and evaluation-related assurance requirements.

2.5.4.2 Supplemental Guidance

The acquisition documents for control systems and services include, either explicitly or by reference, security requirements that describe: (1) required security capabilities (security needs and, as necessary, specific security controls), (2) required design and development processes, (3) required test and evaluation procedures, and (4) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

2.5.4.3 Requirement Enhancements

1. The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls employed within the control system.
2. The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls employed within the control system (including functional interfaces among control components).
3. The organization limits the acquisition of commercial technology products with security capabilities to products that have been evaluated and validated through a government-approved process.

2.5.4.4 References

NIST SP 800-53r3	SA-4
CAG	CC-3, CC-7
NRC RG 5.71	C.3.3.3, App. B.5.4, App. C.12.4

2.5.5 Control System Documentation

2.5.5.1 Requirement

The organization:

1. Obtains, protects as required, and makes available to authorized personnel, administrator and user guidance for the control system that includes information on: (a) configuring, installing, and operating the system and (b) using the system’s security features

2. Documents attempts to obtain control system documentation when such documentation is either unavailable or nonexistent (e.g., because of the age of the system or lack of support from the vendor/contractor) and provides compensating security controls, if needed.

2.5.5.2 Supplemental Guidance

Administrator and user guides need to include information on:

- The configuration, installation, operation, and trouble-shooting of the control system
- The operation and trouble-shooting of the control system's security features.

2.5.5.3 Requirement Enhancements

1. The organization obtains, if available from the vendor/contractor, information describing the functional properties of the security controls employed within the control system.
2. The organization obtains, if available from the vendor/contractor, information describing the design and implementation details of the security controls employed within the control system (including functional interfaces among control components).
3. The organization obtains, if available from the vendor/contractor, information that describes the security-relevant external interfaces to the control system.

2.5.5.4 References

NIST SP 800-53r3	SA-5
API 1164r2	Annex A, Annex B.1
NERC CIPS	CIP 002-3, B.R1-R4
NRC RG 5.71	C.4.2, C.4.2.1, C.5, App. A.3

2.5.6 Software License Usage Restrictions

2.5.6.1 Requirement

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws
2. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution
3. Controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

2.5.6.2 Supplemental Guidance

The organization uses software and associated documentation in accordance with the software licensing agreement and applicable copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization limits and documents the use of publicly accessible peer-to-peer file-sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

2.5.6.3 Requirement Enhancements

None

2.5.6.4 References

NIST SP 800-53r3	SA-6
CAG	CC-2
API 1164r2	3.8
NRC RG 5.71	App. B.1.1, App. B.1.16, App. B.1.17, App. B.1.19, App. B.3.14, App. C.11.6

2.5.7 User-Installed Software

2.5.7.1 Requirement

The organization implements policies and procedures to enforce explicit rules and management expectations governing user installation of software.

2.5.7.2 Supplemental Guidance

If provided the necessary privileges, users have the ability to install software. The organization's security program identifies the types of software permitted to be downloaded and installed (e.g., updates and security patches to existing software) and types of software prohibited (e.g., software that is free only for personal, not government or corporate use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

2.5.7.3 Requirement Enhancements

None

2.5.7.4 References

NIST SP 800-53r3	SA-7
CAG	CC-2
API 1164r2	3.8, Annex A
NRC RG 5.71	App. C.3.7, App. C.13.1

2.5.8 Security Engineering Principles

2.5.8.1 Requirement

The organization applies control system security engineering principles in the specification, design, development, and implementation of the system.

2.5.8.2 Supplemental Guidance

The application of security engineering principles is primarily targeted at new development control systems or control systems undergoing major upgrades and is integrated into the system development life cycle. For legacy control systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

2.5.8.3 Requirement Enhancements

1. The organization adopts software development standards and practices for trustworthy software throughout the development life cycle.
2. Trustworthy software reduces common design and coding errors that affect security, such as:
   a. Unsafe buffer and string management
   b. Languages that have unsafe buffer operations.

3 Trustworthy software development employs commercially available tools including a robust set of data validation and software quality assurance.

2.5.8.4 References

NIST SP 800-53r3	SA-8
CAG	CC-7, CC-16
API 1164r2	Annex A
NRC RG 5.71	C.C.8.1, C.8.4, C.10.2, C.10.3, C.12.3

2.5.9 Outsourced Control System Services

2.5.9.1 Requirement

The organization:

1. Requires that providers of external control system services employ security controls in accordance with applicable laws, directives, policies, regulations, standards, guidance, and established service-level agreements
2. Defines government oversight and user roles and responsibilities with regard to external control system services
3. Monitors security control compliance by external service providers.

2.5.9.2 Supplemental Guidance

Third-party providers are subject to the same control system security policies and procedures of the organization. All the contractors' equipment conforms to the same requirements as the organization's internal systems. Appropriate organizational officials need to approve outsourcing of control system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced control system services' documentation includes service provider and end-user security roles, responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

2.5.9.3 Requirement Enhancements

None

2.5.9.4 References

NIST SP 800-53r3	PS-7, SA-9
API 1164r2	1.2, Annex A
NRC RG 5.71	App. B.1.1, App. B.1.2, App. B.1.21, App. B.1.22, App. C.5.2

2.5.10 Developer Configuration Management

2.5.10.1 Requirement

The organization requires that control system developers/integrators implement and document a configuration management process that (1) manages and controls changes to the system during design, development, implementation, and operation; (2) tracks security flaws; and (3) includes organizational approval of changes.

2.5.10.2 Supplemental Guidance

None

2.5.10.3 Requirement Enhancements

1. The organization requires that information system developers/integrators provide an integrity check of software to facilitate user verification of software integrity after delivery.
2. The organization provides an alternative configuration management process with organizational personnel in the absence of dedicated developer/integrator configuration management team.
3. Enhancement Supplemental Guidance: The configuration management process includes key organizational personnel that are responsible for reviewing and approving proposed changes to the informational system and security personnel that conduct impact analyses prior to the implementation of any changes to the system.

2.5.10.4 References

NIST SP 800-53r3	SA-4, SA-10
CAG	CC-3, CC-7
API 1164r2	3.7, Annex A
NRC RG 5.71	C.3.1.3, C.4.2, App. B.5.2

2.5.11 Developer Security Testing

2.5.11.1 Requirement

The control system developer/integrator:

1. Develops a security test and evaluation plan
2. Implements a verifiable error remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process
3. Documents the result of the security testing/evaluation and error remediation processes.

2.5.11.2 Supplemental Guidance

The organization does not perform developmental security tests on the production control system network. Functional acceptance and security verification checks need to be conducted on a representative testbed environment with issues documented, resolved, and retested before operational acceptance can be given. Once accepted, deployment needs to be in a controlled manner to mitigate inadvertent system upsets.

2.5.11.3 Requirement Enhancements

1. The organization requires that control system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.
2. The organization requires that control system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.
3. The organization requires that information system developers/integrators create a security test and evaluation plan and implement this plan under independent verification and validation.

2.5.11.4 References

NIST SP 800-53r3	SA-11
API 1164r2	Annex A
NRC RG 5.71	App. C.12.5

2.5.12 Supply Chain Protection

2.5.12.1 Requirement

The organization protects against supply chain vulnerabilities employing controls defined to protect the products and services from threats initiated against organizations, people, information, and resources, possibly international in scope, that provides products or services to the organization.

2.5.12.2 Supplemental Guidance

A supply chain is a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Products and services in the domestic and international supply chain include hardware, software, and firmware components for systems, data management services, telecommunications service providers, and Internet service providers. Domestic and international supply chains are becoming increasingly important to the national and economic security interests of the United States because of the growing dependence on products and services produced or maintained in worldwide markets. Uncertainty in the supply chain and the growing sophistication and diversity of international cyber threats increase the potential for a range of adverse effects on organizational operations and assets, individuals, other organizations, and the nation. Global commercial supply chains provide adversaries with opportunities to manipulate control system technology products that are routinely used by public and private sector organizations (e.g., suppliers, contractors) in the control systems that support U.S. critical infrastructure applications. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those control systems. To mitigate risk from the supply chain, a comprehensive security strategy should be considered that employs a strategic, organization-wide *defense-in-breadth* approach. A defense-in-breadth approach helps to protect control systems (including the technology products that compose those systems) throughout the System Development Life Cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). The identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk are important components of a successful defense-in-breadth approach.

2.5.12.3 Requirement Enhancements

1. The organization purchases all anticipated control system components and spares in the initial acquisition.
2. The organization employs trusted intermediaries for purchasing contract services, acquisitions, or logistical activities during the control system life cycle.
3. The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire control system hardware, software, firmware, or services.
4. The organization uses trusted shipping and warehousing for control systems, control system components, and technology products.
5. The organization uses a diverse set of suppliers for control systems, control system components, technology products, and control system services.
6. The organization uses standard configurations for control systems, control system components, and technology products.
7. The organization minimizes the time between purchase decisions and delivery of control systems, control system components, and technology products.
8. The organization employs independent analysis and penetration testing against delivered control systems, control system components, and technology products.

2.5.12.4 References

NIST SP 800-53r3	SA-12
CAG	CC-17
NRC RG 5.71	App. C.12.2

2.5.13 Trustworthiness

2.5.13.1 Requirement

The organization requires that the control system meet an organization-defined level of trustworthiness.

2.5.13.2 Supplemental Guidance

The level of trustworthiness for organizational control systems is defined in terms of degree of correctness for intended functionality and of degree of resilience to attack by explicitly identified levels of adversary capability. In addition, but not as a replacement for this expression of degree of correctness and resilience, the level of trustworthiness may also be described in terms of levels of developmental assurance, that is, actions taken in the specification, design, development, implementation, and operation/maintenance of the control system that impact the degree of correctness and resilience achieved. Trustworthiness may be defined as different levels on the basis of component-by-component, subsystem-by-subsystem, function-by-function, or a combination of the above. However, typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and, at a minimum, something that likely requires careful attention in order to achieve practically useful results.

2.5.13.3 Requirement Enhancements

The organization requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

2.5.13.4 References

NIST SP 800-53r3	SA-13
NRC RG 5.71	App. C.12.3

2.5.14 Critical Information System Components

2.5.14.1 Requirement

The organization:

1. Defines and documents all critical hardware and software system components that are in service
2. Upgrade existing limited legacy equipment with current or custom developed information system components.

2.5.14.2 Supplemental Guidance

The assumption is that information technology products defined by the organization cannot be trusted due to unacceptable threat potential from the supply chain. Examples would be legacy systems with no viable alternatives, or existing components that cannot be hardened or enhanced to the required level of high security assurance. The organization can deploy custom developed or compensating controls to achieve high assurance security requirements.

2.5.14.3 Requirement Enhancements

The organization:

1. Identifies information system components for which alternative sourcing is not possible

2. Employs compensating measures to ensure that critical security controls for the information system components are not compromised.

2.5.14.4 References

NIST SP 800-53r3	SA-14
API 1164r2	Annex A, Annex B.3.1.1
NRC RG 5.71	C.3.1.3, App. C.3.7, App. C.11.9

2.6 Configuration Management

The organization's security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the control system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the control system configuration. Control systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a control system. Vendor updates and patches need to be thoroughly tested on a nonproduction control system setup before being introduced into the production environment to ensure no adverse effects occur.

2.6.1 Configuration Management Policy and Procedures

2.6.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented configuration management policy that addresses:
   a. The purpose of the configuration management policy as it relates to protecting the organization's personnel and assets
   b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors
   c. The roles, responsibilities, management accountability structure, and coordination among organizational entities contained in the configuration management policy to ensure compliance with the organization's security policy and other regulatory commitments.
2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.

2.6.1.2 Supplemental Guidance

The organization ensures the configuration management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general control system security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular control system component when required. Configuration management should include hardware, software, versions, patches deployed, operational applications, security components, conduit schedules (for data and security items). Barcodes and RFID are commonplace means of tracking hardware and supporting elements (conduits).

2.6.1.3 Requirement Enhancements

None

2.6.1.4 References

NIST SP 800-53r3	CM-1
CAG	CC-2, CC-3, CC-4
API 1164r2	Annex A, Annex B.3.1.1
NERC CIPS	CIP 002-3, B.R6, CIP 007-3, B.R1, B.R3
NRC RG 5.71	C.3.1.4, C.4.2, App. C.11.2

2.6.2 Baseline Configuration

2.6.2.1 Requirement

The organization develops, documents, and maintains a current baseline configuration of the control system and an inventory of the system's constituent components.

2.6.2.2 Supplemental Guidance

This control establishes a baseline configuration for the control system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the control system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the control system is built, and deviations, if required, are documented in support of mission needs/objectives. The configuration of the control system component should be consistent with the organization's control system architecture and documentation policy. The inventory of control system components includes information (e.g., manufacturer, type, serial number, version number, and location) that uniquely identifies each component. Modern inventory control systems are frequently using radio-frequency identification (RFID) for ease of use and accuracy. Maintaining the baseline configuration involves creating a new baseline as the control system changes over time and keeping old baselines available for possible rollback.

2.6.2.3 Requirement Enhancements

1. The organization reviews and updates the baseline configuration as an integral part of control system component installations.
2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the control system.
3. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.
4. The organization employs a deny-all, permit-by-exception authorization policy to identify software allowed on organizational control systems.

2.6.2.4 References

NIST SP 800-53r3	CM-2
CAG	CC-2, CC-3, CC-4
API 1164r2	3.6, Annex B.1.1
NERC CIPS	CIP 007-3, B.R1, B.R3
NRC RG 5.71	C.4.2, App. C.11.3

2.6.3 Configuration Change Control

2.6.3.1 Requirement

The organization:

1. Authorizes and documents changes to the control system
2. Retains and reviews records of configuration-managed changes to the system
3. Audits activities associated with configuration-managed changes to the system.

2.6.3.2 Supplemental Guidance

The organization manages configuration changes to the control system using an organizationally approved process (e.g., a Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the control system, including upgrades and modifications. Because of the convergence of IT and control systems, configuration change control includes changes to the configuration settings for the control system and those IT products (e.g., operating systems, firewalls, routers) that are components of the control system. Each device on the control system contains a unique identifier (e.g., serial number, device name, tag number, RFID tag) that is referenced in the configuration management process. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the control system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the control system.

A production control system may need to be taken offline, or replicated to the extent feasible, before the testing can be conducted. If a control system must be taken offline for tests, tests are scheduled to occur during planned control system outages whenever possible. In situations where the organization determines it is not feasible or advisable (e.g., adversely impacting performance, safety, reliability) to implement the live testing of the production control system, the organization documents the rationale for using a replicated system.

2.6.3.3 Requirement Enhancements

1. The organization employs automated mechanisms to:
   a. Document proposed changes to the control system
   b. Notify appropriate approval authorities
   c. Highlight approvals that have not been received in a timely manner
   d. Inhibit change until necessary approvals are received
   e. Document completed changes to the control system.
2. The organization tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational control system. The organization ensures that testing does not interfere with control system operations. The tester fully understands the corporate cyber and control system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process.

2.6.3.4 References

NIST SP 800-53r3	CM-3
CAG	CC-2, CC-3, CC-4
API 1164r2	3.6, Annex A, Annex B.3.1
NERC CIPS	CIP 002-3 B.R6, CIP 007-3. B.R1, B.R3

NRC RG 5.71	C.3.1.3, C.4.2, App. B.5.4, App. B.5.5, App. C.11.4

2.6.4 Monitoring Configuration Changes

2.6.4.1 Requirement

The organization implements a process to monitor changes to the control system and conducts security impact analyses to determine the effects of the changes.

2.6.4.2 Supplemental Guidance

Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the control system for potential security impacts. After the control system is changed, the organization should check the security features to ensure that the features are still functioning properly. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. Security impact analysis is an important activity in the ongoing monitoring of security controls in the control system. The organization should audit activities associated with configuration changes to the control system. The organization considers control system safety and security interdependencies.

2.6.4.3 Requirement Enhancements

None

2.6.4.4 References

NIST SP 800-53r3	CM-4
CAG	CC-4
API 1164r2	3.6, Annex A, Annex B.3.1.1.1
NERC CIPS	CIP 007-3. B.R1, B.R3
NRC RG 5.71	C.4.3, App. C.3.4, B.5.4, App. C.11.7, App. C.11.8

2.6.5 Access Restrictions for Configuration Change

2.6.5.1 Requirement

The organization:

1. Defines, documents, and approves individual access privileges and enforces physical and logical access restrictions associated with configuration changes to the control system
2. Generates, retains, and reviews records reflecting all such changes.

2.6.5.2 Supplemental Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the control system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to control system components for purposes of initiating changes, including upgrades, and modifications. The organization establishes strict terms and conditions for installing any hardware or software on control system devices (e.g., modems, wireless adapters, multi-function printers, games, word processing software).

In addition, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the control system. Access restrictions for change also include software libraries. Examples of access restrictions include physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the control system component), and change windows (e.g., changes occur only during specified times making unauthorized changes outside the window, easy to discover). Some or all the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the control system, auditing changes, and retaining and review records of changes.

2.6.5.3 Requirement Enhancements

1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
2. The organization conducts audits of control system changes at a defined frequency and when indications so warrant to determine whether unauthorized changes have occurred.
3. The control system prevents the installation of device drivers that are not signed with an organizationally recognized and approved certificate.
4. Physical security to restrict data devices (compact disc [CD]/digital video disc [DVD], tape, serial ports, network ports, USB/secure digital memory card [SD] configuration devices) is required. Security authorization including two-man policies is required.

2.6.5.4 References

NIST SP 800-53r3	CM-5
CAG	CC-2, CC-3, CC-4
API 1164r2	Annex A, Annex B.5
NERC CIPS	CIP 007-3. B.R1, B.R3
NRC RG 5.71	C.4.2.1, C.4.3, App. B.1.1, App. B.5.4, App. B.5.5, App. C.11.6

2.6.6 Configuration Settings

2.6.6.1 Requirement

The organization:

1. Establishes mandatory configuration settings for products employed within the control system
2. Configures the security settings of control systems technology products to the most restrictive mode consistent with control system operational requirements
3. Documents the changed configuration settings
4. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the control system based on explicit operational requirements
5. Enforces the configuration settings in all components of the control system
6. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

2.6.6.2 Supplemental Guidance

Configuration settings are the configurable parameters of the products that compose the control system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. In some industries, a mandated testing period is required, with separate approval needed before the test configuration settings can be deployed.

This control applies to remote assets (e.g., remote assets used to access the control system) as well as assets onsite.

2.6.6.3 Requirement Enhancements

1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings.
3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

2.6.6.4 References

NIST SP 800-53r3	CM-6
CAG	CC-3, CC-4, CC-13
NERC CIPS	CIP 007-3. B.R1, B.R3
NRC RG 5.71	App. C.11.7

2.6.7 Configuration for Least Functionality

2.6.7.1 Requirement

The organization configures the control system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list.

2.6.7.2 Supplemental Guidance

Control systems provide a wide variety of functions and services. Some of the default functions and services may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services (e.g., voice-over internet protocol [VoIP], instant messaging, file transfer protocol, hypertext transfer protocol [HTTP], file sharing) provided by control systems should be carefully reviewed to determine which are candidates for elimination.

The organization considers disabling unused or unnecessary physical and logical ports (e.g., USB, Personal System/2, file transfer protocol [FTP]) on control system components to prevent unauthorized connection of devices (e.g., thumb drives, keystroke loggers). Organizations can use network scanning tools, intrusion detection and prevention systems, and end-point protections, such as firewalls and host intrusion detection systems, to identify and prevent the use of prohibited ports, protocols, and services. This can be third-party software or physical methods to control access.

2.6.7.3 Requirement Enhancements

1 The organization reviews the control system periodically or as deemed necessary to identify and eliminate unnecessary functions, ports, protocols, and/or services.

2. The organization employs automated mechanisms to prevent program execution in accordance with defined lists.
3. Use of configuration laptops and or removable electronic media sometimes cannot be avoided. In such cases, approved and authorized devices need to be documented, secured, and available only to specified and approved entities for use.
4. Six wall bordering requirements such as special equipment vaulting, two-man rules, and enhanced inventory control and authorization will be used.

5. In high security situations, it is necessary to separate the duties and access between the system administrator and the cybersecurity officer such that neither can make the changes by themselves. In this case, while the system administrator may have server permission, the security officer maintains and controls physical access to the server and/or dataport locking mechanisms.

2.6.7.4 References

NIST SP 800-53r3	CM-7
CAG	CC-2, CC-3, CC-4, CC-7, CC-13
API 1164r2	5.7, Annex A
NERC CIPS	CIP 007-3. B.R2, B.R2.1-2.3
NRC RG 5.71	App. 5.3, App. B.5.4, App. C.11.8

2.6.8 Configuration Assets

2.6.8.1 Requirement

The organization develops, documents, and maintains an inventory of the components of the control system that:

1. Accurately reflects the current control system
2. Is consistent with the authorization boundary of the control system
3. Is at the level of granularity deemed necessary for tracking and reporting
4. Includes defined information deemed necessary to achieve effective property accountability.

2.6.8.2 Supplemental Guidance

Before a configuration management program can operate, all configurable items should first be uniquely identified and recorded. The organization determines the appropriate level of granularity for any control system component included in the inventory that is subject to management control (e.g., tracking, and reporting). The inventory of control system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner, and for a networked component/device, the machine name and network address). In addition, configuration files, setpoints, alarm points, security filter rules, authorized and approved white lists, and permission files need to be documented and securely stored and backed up. This includes the current operational application files for the operational PLC elements. These files are crucial to effective disaster/incident recovery. The organization's maintenance program is responsible for configuration management tasks. Personnel performing maintenance on a control system should refer to and update the configurable assets list to ensure that all control system components are maintained and configured appropriately.

2.6.8.3 Requirement Enhancements

1. The organization updates the inventory of control system components and programming as an integral part of component installation, replacement and system updates.
2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of control system components, configuration files and setpoints, alarm settings and other required operational settings.
3. The organization employs automated mechanisms to detect the addition of unauthorized components/devices/component settings into the control system.

4. The organization disables network access by such components/devices or notifies designated organizational officials.

5. The organization includes in property accountability information for control system components, the names of the individuals responsible for administering those components.

2.6.8.4 References

NIST SP 800-53r3	CM-8
CAG	CC-1, CC-2, CC-4
API 1164r2	Annex A
NERC CIPS	CIP 007-3. B.R1
NRC RG 5.71	App. 5.3, App. B.5.4, App. B5.5, App. C.11.8, App. C.11.9

2.6.9 Addition, Removal, and Disposal of Equipment

2.6.9.1 Requirement

The organization implements policy and procedures to address the addition, removal, and disposal of all control system equipment. All control system assets and information are documented, identified, and tracked so that the location and function are known.

2.6.9.2 Supplemental Guidance

The organization sanitizes control system media, both paper and digital, before disposal or reuse. All control system media need to be tracked, documented, and verified as sanitized. The organization periodically verifies the media sanitization process.

2.6.9.3 Requirement Enhancements

1. Specialized critical digital assets must require internal registration, configuration and usage plan, and secure storage before, during and after usage.
2. Critical Digital Assets in security arenas, such as laptop and desktop computers, network gear, hard drives, removable electronic media (e.g., CD/DVD/Tape/USB/SD), must be destroyed on removal from operations, or inspected and undergo approved, documented, de-sanitization procedures (deep formatting or destruction) on being removed from service.

2.6.9.4 References

CAG	CC-2
NERC CIPS	CIP 007-3, B.R7, R7.1, R7.2, R7.3
NRC RG 5.71	App. B.5.1, App. B.5.5, App. C.1.6, App. C.11.2, App. C.11.9

2.6.10 Factory Default Authentication Management

2.6.10.1 Requirement

The organization changes all factory default authentication credentials on control system components and applications upon installation.

2.6.10.2 Supplemental Guidance

Many control system devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory defaults are often well known or easily discoverable. They present an obvious security risk and, therefore, should be changed prior to the device being put into service. In addition, do not embed passwords into tools, source code, scripts, aliases, or shortcuts. Known legacy components with these deficiencies need to be identified and targeted for higher priority in upgrade/replacement during the next maintenance/upgrade cycle.

2.6.10.3 Requirement Enhancements

Known legacy operational equipment needs compensatory access restrictions to protect against loss of authentication. In addition, these components need to be identified, tested, and documented to verify that proposed compensatory measures are effective.

2.6.10.4 References

NIST SP 800-53r3	IA-5
CAG	CC-4
API 1164r2	5.5, 5.6, Annex A
NERC CIPS	CIP 007-3. B.R5.1
NRC RG 5.71	C.3.3.1.4, App. B.1.20, App. B.4.1, App. B.4.7

2.6.11 Configuration Management Plan

2.6.11.1 Requirement

The organization develops and implements a configuration management plan for the control system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures
2. Defines the configuration items for the control system
3. Defines when (in the system development life cycle) the configuration items are placed under configuration management
4. Defines the means for uniquely identifying configuration items throughout the system development life cycle
5. Defines the process for managing the configuration of the controlled items.

2.6.11.2 Supplemental Guidance

Configuration items are the control system items (hardware, software, firmware, and documentation). Configuration management is the management of planned changes to those items. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual control system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life-cycle activities at the control system level. It includes the steps for moving a change through the change management process; how configuration settings and configuration baselines are updated; how the control system component inventory is maintained; how development, test, and operational environments are controlled; and how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

2.6.11.3 Requirement Enhancements

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Enhanced Supplemental Guidance—In the absence of a dedicated configuration management team, the system integrator may be tasked with developing a configuration management process.

2.6.11.4 References

NIST SP 800-53r3	CM-9
API 1164r2	Annex A
NERC CIPS	CIP 003-3. B.R6
NRC RG 5.71	C.3.1.4, C.4.2, App. B.5.3, App. B.5.4, App. B.5.5, App. C.11.2

2.7 Strategic Planning

Strategic planning maintains optimal operations and prevents or recovers from undesirable interruptions to control system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain system operation during and after an interruption), and planning to identify mitigation strategies. The continuity of operations planning may also be designated as incident response planning. The planning process is the same for each type of plan. The following items should be considered when developing a plan.

2.7.1 Strategic Planning Policy and Procedures

2.7.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, planning policy that addresses:
   a. The purpose of the strategic planning program as it relates to protecting the organization’s personnel and assets
   b. The scope of the strategic planning program as it applies to all the organizational staff and third-party contractors
   c. The roles, responsibilities, coordination among organizational entities, and management accountability structure of the strategic planning program to ensure compliance with the organization’s security policy and other regulatory commitments.

2 Formal, documented procedures to facilitate the implementation of the strategic planning policy and associated strategic planning controls.

2.7.1.2 Supplemental Guidance

The strategic planning policy may be included as part of the general information security policy for the organization. Strategic planning procedures may be developed for the security program in general and a control system in particular, when required.

2.7.1.3 Requirement Enhancements

None

2.7.1.4 References

NIST SP 800-53r3	PL-1
NERC CIPS	CIP 002-3. through CIP 009-3
NRC RG 5.71	C.3.1, C.3.1.1, C.3.3.3, App. C.13

2.7.2 Control System Security Plan

2.7.2.1 Requirement

The organization:

1. Develops a security plan for the system that:
   a. Aligns with the organization's enterprise architecture
   b. Explicitly defines the authorization boundary for the system
   c. Describes relationships with or connections to other systems
   d. Provides an overview of the security requirements for the system
   e. Describes the security controls in place or planned for meeting those requirements
   f. Specifies the authorizing official or authorizing official designated representative who reviews and approves the control system security plan prior to implementation.
2. Reviews the security plan for the system on an organization-defined frequency, at least annually
3. Revises the plan to address changes to the system/environment of operation or problems identified during plan implementation or security control assessments.

2.7.2.2 Supplemental Guidance

The security plan is aligned with the organization's control system architecture and information security architecture. To develop properly the control system security plan, it is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experience to evaluate and mitigate risk in the control system. The cybersecurity team considers control system safety and security interdependencies. The cybersecurity team includes members of the organization's IT staff, control system engineers, control system operators, members with network and system security expertise, members of the management staff, and members of the physical security department, at a minimum. In some smaller organizations, it may be necessary for personnel to perform multiple roles. For continuity and completeness, the cybersecurity team consults with the control system vendor(s) as well.

2.7.2.3 Requirement Enhancements

Secure control system operations require more in-depth and specialized security plans, which limit data ports, physical access, specific data technology (Fiber), additional physical and electronic inspections and physical separation requirements.

2.7.2.4 References

NIST SP 800-53r3	PL-2
API 1164r2	3, Annex B
NERC CIPS	CIP 003-3. B.R1
NRC RG 5.71	C.2, C.3, App. B.1.2, App. C.10.4

2.7.3 Interruption Identification and Classification

2.7.3.1 Requirement

The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."

2.7.3.2 Supplemental Guidance

The various types of incidents that might be caused by system intrusion need to be identified and classified as to their effects and likelihood so that a proper response can be formulated for each potential incident. The organization determines the impact to each system and the consequences associated with loss of one or more of the control systems. Proactive measurements are determined automatically to identify attacks during their early stages. The organization fully identifies any potential links between the corporate mission, safety, and the control system and incorporates this understanding into integrated security incident response procedures.

During postinterruption analysis activities, previously unforeseen consequences, especially those that may affect future application of the plan, need to be identified. Incidents may include risk events, near misses, and malfunctions. Also included should be any observed or suspected weaknesses in the control system or risks that may not have been previously recognized.

2.7.3.3 Requirement Enhancements

None

2.7.3.4 References

NIST SP 800-53r3	IR-8, PM-9
CAG	CC-10, CC-17
NERC CIPS	CIP 008-03 B.R1.1
NRC RG 5.71	C.2, C.3.1.2, App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8

2.7.4 Roles and Responsibilities

2.7.4.1 Requirement

The organization’s control system security plan defines and communicates the specific roles and responsibilities in relation to various types of incidents.

2.7.4.2 Supplemental Guidance

The organization’s control system security plan defines the roles and responsibilities of the various employees and contractors in the event of an incident. The plan identifies responsible personnel to lead the response effort if an incident occurs. Response teams need to be formed, including control system and other process owners, to reestablish operations. The response teams have a major role in the interruption identification and planning process. Several other standards and guidelines have begun separating out roles and responsibilities to separate control elements as necessary. Examples of differing roles and responsibilities would be Security Training versus Incident Management versus Patch Management.

2.7.4.3 Requirement Enhancements

None

2.7.4.4 References

NIST SP 800-53r3	AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9
CAG	CC-18
API 1164r2	1.2, 3.1, Annex A, Annex B.5
NERC CIPS	CIP 008-3. B.R1.2
NRC RG 5.71	C.2, C.3.1.2, App. C.3.4, App. C.8, App. C.8.1, App. C.8.8, App. C.10.10

2.7.5 Planning Process Training

2.7.5.1 Requirement

The organization includes training on the implementation of the control system security plans for employees, contractors, and stakeholders into the organization's planning process.

2.7.5.2 Supplemental Guidance

Advanced training, documentation and testing requirements and certifications are to be provided to individuals in the control system community to understand the content, purpose, and implementation of the security plans, procedures and funtionality. The organization's planning process must account for training in the implementation of the organization's security plan. Different levels of training may be prepared for personnel with different levels of roles and responsibility. Cross-training might also be considered. Additional training controls are addressed in individual families.

2.7.5.3 Requirement Enhancements

None

2.7.5.4 References

NIST SP 800-53r3	AC-5, CP-1, CP-3
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B.5
NERC CIPS	CIP 008-3. B.R1.2
NRC RG 5.71	App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8, App. C.10.4, App. C.10.6

2.7.6 Testing

2.7.6.1 Requirement

The organization regularly tests security plans to validate the control system objectives.

2.7.6.2 Supplemental Guidance

Following the preparation of the various plans, a schedule is developed to review and test each of the plans and ensure that it continues to meet the objectives. Additional testing requirements are addressed in individual families.

2.7.6.3 Requirement Enhancements

None

2.7.6.4 References

NIST SP 800-53r3	CP-2, CP-4, IR-3, SA-11, SI-4, SI-6
CAG	CC-17
API 1164r2	3.5, 3.7, Annex A, Annex B.4
NERC CIPS	CIP 008-3. B.R1, C, M1
NRC RG 5.71	App. B.4.9, App. C.8.3, App. C.9.3, App. C.13.1, App. C.13.2

2.7.7 Investigation and Analysis

2.7.7.1 Requirement

The organization includes investigation and analysis of control system incidents in the planning process.

2.7.7.2 Supplemental Guidance

The organization develops an incident investigation and analysis program, either internally or externally, to investigate incidents. These investigations need to consider incidents based on the potential outcome as well as the actual outcome, recognizing that the cyber and control system incident may include intentional and/or unintentional incidents. The organization develops, tests, deploys, and fully documents an incident investigation process. The incident and analysis investigation program specifies the roles and responsibilities of local law enforcement and/or other critical stakeholders in an internal and shared incident investigation program. Incidents need to be analyzed in light of trends and recorded so they can be used for subsequent trend analyses.

2.7.7.3 Requirement Enhancements

None

2.7.7.4 References

NIST SP 800-53r3	IR-4
API 1164r2	3.5, Annex A, Annex B.2
NRC RG 5.71	App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8, App. C.10.10

2.7.8 Corrective Action

2.7.8.1 Requirement

The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cybersecurity and control system incidents are fully implemented.

2.7.8.2 Supplemental Guidance

The organization reviews investigation results and determines corrective actions needed to ensure that similar events do not reoccur. The organization encourages and promotes cross-industry exchange of incident information and cooperation to learn corrective actions from the experiences of others.

2.7.8.3 Requirement Enhancements

None

2.7.8.4 References

NIST SP 800-53r3	IR-4
API 1164r2	3.5, Annex B.4
NERC CIPS	CIP 009-3. B.R3
NRC RG 5.71	App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8

2.7.9 Risk Mitigation

2.7.9.1 Requirement

Risk-reduction mitigation measures are planned and implemented, and the results are monitored to ensure effectiveness of the organization’s risk management plan.

2.7.9.2 Supplemental Guidance

The organization's planning process develops step-by-step actions to be taken by the various organizations to implement the organization's risk mitigation plan. Risk mitigation measures need to be implemented, and the results need to be monitored against planned metrics to ensure the effectiveness of the risk management plan. The reasons for selecting or rejecting certain security mitigation mechanisms and the risks they address need to be documented by the organization's planning process.

2.7.9.3 Requirement Enhancements

None

2.7.9.4 References

NIST SP 800-53r3	PL-2, PM-9
API 1164r2	Annex B.3
NERC CIPS	CIP 007-3. B.R8
NRC RG 5.71	App. C.13.2

2.7.10 System Security Plan Update

2.7.10.1 Requirement

The organization regularly, at prescribed frequencies, reviews the security plan for the control system and revises the plan to address system/organizational changes or problems identified during system security plan implementation or security controls assessment.

2.7.10.2 Supplemental Guidance

Significant changes need to be defined in advance by the organization and identified in the configuration management process.

2.7.10.3 Requirement Enhancements

None

2.7.10.4 References

NIST SP 800-53r3	PL-2
API 1164r2	3, Annex B.4
NERC CIPS	CIP 008-3. B.R1.3, R4.3
NRC RG 5.71	C.4.1, C.4.2.2, App. B.3.1, App. C.3.1, App. C.7

2.7.11 Rules of Behavior

2.7.11.1 Requirement

The organization establishes and makes readily available to all control system users a set of rules that describes their responsibilities and expected behavior with regard to control system usage. The organization obtains signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the control system.

2.7.11.2 Supplemental Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy.

2.7.11.3 Requirement Enhancements

The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial web sites, and sharing system account information.

2.7.11.4 References

NIST SP 800-53r3	PL-4
API 1164r2	3. Annex A, Annex B.5
NERC CIPS	CIP 005-3. B.R2, R2.5, R2.6
NRC RG 5.71	C.3.3.2, C.3.3.2.7, App. C.9.1

2.7.12 Security-Related Activity Planning

2.7.12.1 Requirement

The organization plans and coordinates security-related activities affecting the control system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals.

2.7.12.2 Supplemental Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advanced planning and coordination include both emergency and nonemergency (i.e., routine) situations.

2.7.12.3 Requirement Enhancements

None

2.7.12.4 References

NIST SP 800-53r3	PL-6
API 1164r2	3.5, 3.7, Annex A, Annex B.2
NERC CIPS	CIP 008-3. B.R1
NRC RG 5.71	C.3.3.2, C.3.3.2.7, App. C.9.1, App. C.10.3, App. C.10.4

2.8 System and Communication Protection

System and communication protection consists of steps taken to protect the control system and the communication links between system components from cyber intrusions. Although control system and communication protection might logically include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in Section 2.4.

2.8.1 System and Communication Protection Policy and Procedures

2.8.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented system and communication protection policy that addresses:
   a. The purpose of the system and communication protection policy as it relates to protecting the organization’s personnel and assets
   b. The scope of the system and communication protection policy as it applies to all the organizational staff and third-party contractors

c. The roles, responsibilities, coordination among organizational entities, and management accountability structure of the security program to ensure compliance with the organization's system and communications protection policy and other regulatory commitments

2. Formal, documented procedures to facilitate the implementation of the control system and communication protection policy and associated systems and communication protection controls.

2.8.1.2 Supplemental Guidance

The organization ensures the system and communication protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communication protection policy needs to be included as part of the general information security policy for the organization. System and communication protection procedures can be developed for the security program in general and a control system in particular, when required.

2.8.1.3 Requirement Enhancements

None

2.8.1.4 References

NIST SP 800-53r3	SC-1
API 1164r2	Annex A, Annex B
NERC CIPS	CIP 005-3. B.R1 through R5
NRC RG 5.71	C.3.3.1.3, App. B.3.1, App. C.1.1, App. C.5.1

2.8.2 Management Port Partitioning

2.8.2.1 Requirement

The control system components separate telemetry/data acquisition services from management port functionality.

2.8.2.2 Supplemental Guidance

The control system management port needs to be physically or logically separated from telemetry/data acquisition services and information storage and management services (e.g., database management) of the system. Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses, combinations of these methods, or other methods as appropriate.

2.8.2.3 Requirement Enhancements

In situations where the ICS cannot separate user functionality from information system management functionality, the organization employs compensating controls (e.g., providing increased auditing measures).

2.8.2.4 References

NIST SP 800-53r3	SC-2
API 1164r2	8.2, Annex B.3.1.4.4
NERC CIPS	CIP 005-3. B.R2
NRC RG 5.71	App. B.3.2, App. B.3.6, App. B.5.1, App. B.5.4, App. C.3.3, App. C.7, App. C.11

2.8.3 Security Function Isolation

2.8.3.1 Requirement

The control system isolates security functions from nonsecurity functions.

2.8.3.2 Supplemental Guidance

The control system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions, domains) that controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. The control system maintains a separate execution domain (e.g., address space) for each executing process.

Some legacy control systems may not implement this capability. In situations where it is not implemented, the organization details its risk acceptance and mitigation in the control system security plan.

2.8.3.3 Requirement Enhancements

The control system employs the following underlying hardware separation mechanisms to facilitate security function isolation.

1 The control system isolates security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

2. The control system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

3. The control system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

4. The control system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

2.8.3.4 References

NIST SP 800-53r3	SC-3
CAG	CC-4, CC-5, CC-13, CC-15, CC-16
API 1164r2	5.1, Annex B.3.1.3
NERC CIPS	CIP 005-3. B.R1.1 through R1.5, R2
NRC RG 5.71	C.3.2.1, App. B.1.20, App. B.3.2

2.8.4 Information in Shared Resources

2.8.4.1 Requirement

The control system prevents unauthorized or unintended information transfer via shared system resources.

2.8.4.2 Supplemental Guidance

Control of system remnants, sometimes referred to as object reuse or data remnants, prevents information, including cryptographically protected representations of information previously produced by the control system, from being available to any current user/role/process that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the system. This control does not address: (1) information remnants that refer to residual representation of data that have been in some way nominally erased or removed, (2) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions, or (3) components in the control system for which only a single user/role exists.

2.8.4.3 Requirement Enhancements

The information system does not share resources that are used to interface with systems operating at different security levels.

2.8.4.4 References

NIST SP 800-53r3	SC-4
API 1164r2	Annex B.3.1.3
NERC CIPS	CIP 005-3. B.R2
NRC RG 5.71	App. B.3.3

2.8.5 Denial-of-Service Protection

2.8.5.1 Requirement

The control system protects against or limits the effects of denial-of-service attacks based on an organization’s defined list of types of denial-of-service attacks.

2.8.5.2 Supplemental Guidance

A variety of technologies exists to limit, or in some cases, eliminate the effects of denial-of-service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization’s internal network from being directly affected by denial-of-service attacks.

2.8.5.3 Requirement Enhancements

1. The control system restricts the ability of users to launch denial-of-service attacks against other control systems or networks.
2. The control system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

2.8.5.4 References

NIST SP 800-53r3	SC-5
API 1164r2	Annex A, Annex B.2
NRC RG 5.71	App. B.3.4

2.8.6 Resource Priority

2.8.6.1 Requirement

The control system limits the use of resources by priority.

2.8.6.2 Supplemental Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the control system servicing any higher-priority process. This control does not apply to components in the system for which only a single user/role exists.

2.8.6.3 Requirement Enhancements

None

2.8.6.4 References

NIST SP 800-53r3	SC-6
NRC RG 5.71	App. B.3.5

2.8.7 Boundary Protection

2.8.7.1 Requirement

The organization defines the external boundaries of the control system. Procedural and policy security functions define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The control system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.

2.8.7.2 Supplemental Guidance

Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective, organization-defined security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone). Control system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services commonly are based on network components and consolidated management systems shared by all attached commercial customers and may include third-party-provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.

Generally, public access to ICS information is not permitted. Allowing telecommunication and business IT traffic (e-mail, Internet access) on ICS systems is not recommended.

2.8.7.3 Requirement Enhancements

1. The organization physically allocates publicly accessible control system components to separate subnetworks with separate, physical network interfaces. Publicly accessible control system components include public web servers. Generally, no control system information should be publicly accessible.

2. The organization prevents public access into the organization’s internal control system networks except as appropriately mediated.

3. The organization limits the number of access points to the control system to allow for better monitoring of inbound and outbound network traffic.

4. The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted.

5. The control system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
6. The organization prevents the unauthorized release of information outside the control system boundary or any unauthorized communication through the control system boundary when an operational failure occurs of the boundary protection mechanisms.
7. The organization prevents the unauthorized release of information across managed interfaces.
8. The control system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
9. The control system at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external systems.
10. The control system prevents remote devices that have established connections with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks.
11. The control system routes all internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices.
12. The organization selects an appropriate failure mode (e.g., fail open or fail close), depending on the critical needs of system availability.

2.8.7.4 References

NIST SP 800-53r3	SC-7
CAG	CC-4, CC-5, CC-13, CC-15, CC-16
API 1164r2	4, Annex A, Annex B
NERC CIPS	CIP 005-3. A, B.R1
NRC RG 5.71	C.3.2.1, App. B.1.20

2.8.8 Communication Integrity

2.8.8.1 Requirement

The control system design and implementation protects the integrity of electronically communicated information.

2.8.8.2 Supplemental Guidance

If the organization is relying on a commercial service provider for communication services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security measures for transmission integrity. When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization either implements appropriate compensating security measures or explicitly accepts the additional risk.

2.8.8.3 Requirement Enhancements

1. The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).
2. The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety.

3. Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.
4. The control system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

2.8.8.4 References

NIST SP 800-53r3	SC-8
API 1164r2	8, Annex A, Annex B.3.1.1
NRC RG 5.71	App. B.3.6

2.8.9 Communication Confidentiality

2.8.9.1 Requirement

The control system design and implementation protects the confidentiality of communicated information where necessary.

2.8.9.2 Supplemental Guidance

The use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within a control system could introduce communications latency because of the additional time and computing resources required to encrypt, decrypt, and authenticate each message. Any latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the control system.

2.8.9.3 Requirement Enhancements

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.
2. The control system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

2.8.9.4 References

NIST SP 800-53r3	SC-9
CAG	CC-4, CC-14
API 1164r2	8
NRC RG 5.71	App. B.1.17, App. B.3.7

2.8.10 Trusted Path

2.8.10.1 Requirement

The control system establishes a trusted communications path between the user and the system.

2.8.10.2 Supplemental Guidance

A trusted path is employed for high-confidence connections between the security functions of the control system and the user (e.g., for login).

Login-to-operator interface should be protected by trusted path or a compensating control. A trusted path is a mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base (TCB) that provides the security functions of the system. This mechanism can only be activated by the person or the TCB and cannot be imitated by untrusted software. The TCB is the totality of protection mechanisms within a computer system—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

2.8.10.3 Requirement Enhancements

None

2.8.10.4 References

NIST SP 800-53r3	SC-11
API 1164r2	8.1, Annex A
NRC RG 5.71	App. B.1.22, App. B.3.9

2.8.11 Cryptographic Key Establishment and Management

2.8.11.1 Requirement

When cryptography is required and employed within the control system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

2.8.11.2 Supplemental Guidance

Organizations need to select cryptographic protection that matches the value of the information being protected and the control system operating constraints. A formal written policy needs to be developed to document the practices and procedures relating to cryptographic key establishment and management. These policies and procedures need to address, under key establishment, such items as key generation process in accordance with a specified algorithm and key sizes based on an assigned standard. Key generation must be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards.

2.8.11.3 Requirement Enhancements

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

2.8.11.4 References

NIST SP 800-53r3	SC-12
NRC RG 5.71	App. B.3.9

2.8.12 Use of Validated Cryptography

2.8.12.1 Requirement

The organization develops and implements a policy governing the use of cryptographic mechanisms for the protection of control system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.

2.8.12.2 Supplemental Guidance

Any cryptographic modules deployed within a control system, at a minimum, must be able to meet the FIPS 140-2. Assessment of the modules must include validation of the cryptographic modules operating in approved modes of operation. The most effective safeguard is to use a cryptographic module validated by the Cryptographic Module Validation Program. Additional information on the use of validated cryptography can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html.

2.8.12.3 Requirement Enhancements

1. The organization protects cryptographic hardware from physical tampering and uncontrolled electronic connections.
2. The organization selects cryptographic hardware with remote key management capabilities.

2.8.12.4 References

NIST SP 800-53r3	SC-13
CAG	CC-15
NRC RG 5.71	App. B.3.10

2.8.13 Collaborative Computing Devices

2.8.13.1 Requirement

The use of collaborative computing devices on the control system is strongly discouraged. If use is authorized and allowed by the organization, explicit indication of use is provided to users physically present at the devices.

2.8.13.2 Supplemental Guidance

Collaborative computing devices include video and audio conferencing capabilities, networked information boards, or instant messaging technologies. Explicit indication of use includes signals to local users when cameras and microphones are activated.

2.8.13.3 Requirement Enhancements

1. If collaborative computing devices are used on the control system, they are disconnected and powered down when not in use.
2. The control system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.
3. The organization disables or removes collaborative computing devices from control systems in organization-defined secure work areas.

2.8.13.4 References

NIST SP 800-53r3	SC-15
API 1164r2	7.15, 7.3, Annex B.3.1.4.3
NRC RG 5.71	App. B.3.11

2.8.14 Transmission of Security Attributes

2.8.14.1 Requirement

The control system reliably associates security attributes (e.g., security labels and markings) with information exchanged between the enterprise systems and the control system.

2.8.14.2 Supplemental Guidance

Security attributes may be explicitly or implicitly associated with the information contained within the control system. For example, security labels are often used in data structures to associated attributes with specific information objects such as user access privileges, nationality, or affiliation as a contractor.

2.8.14.3 Requirement Enhancements

The control system validates the integrity of security parameters exchanged between systems.

2.8.14.4 References

NIST SP 800-53r3	SC-16
NRC RG 5.71	App. B.3.12

2.8.15 Public Key Infrastructure Certificates

2.8.15.1 Requirement

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

2.8.15.2 Supplemental Guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

2.8.15.3 Requirement Enhancements

Any latency induced from the use of public key certificates must not degrade the operational performance of the control system.

2.8.15.4 References

NIST SP 800-53r3	SC-17
NRC RG 5.71	App. B.1.22, App. B.3.13

2.8.16 Mobile Code

2.8.16.1 Requirement

The organization:

1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the control system if used maliciously
2. Documents, monitors, and manages the use of mobile code within the control system. Appropriate organizational officials authorize the use of mobile code.

2.8.16.2 Supplemental Guidance

Mobile code technologies include Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures need to prevent the development, acquisition, or introduction of unacceptable mobile code within the control system. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at http://iase.disa.mil/mcp/index.html. This link to the Mobile Code Policy and Guidance has been moved to the Department of Defense Public Key Infrastructure (PKI)-certified protected area of Information Assurance Support Environment (IASE) A person must have the proper authority for access to this document.

2.8.16.3 Requirement Enhancements

The control system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

2.8.16.4 References

NIST SP 800-53r3	SC-18
CAG	CC-5, CC-12
NRC RG 5.71	App. B.1.22, App. B.3.14

2.8.17 Voice-Over Internet Protocol

2.8.17.1 Requirement

The organization: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the system if used maliciously and (2) authorizes, monitors, and controls the use of VoIP within the control system.

2.8.17.2 Supplemental Guidance

Generally, VoIP technologies should not be employed on control systems. Usage should be determined after careful consideration and after verification that it does not adversely impact the operational parameters of the ICS.

2.8.17.3 Requirement Enhancements

None

2.8.17.4 References

NIST SP 800-53r3	SC-19
API 1164r2	7.3.6

2.8.18 System Connections

2.8.18.1 Requirement

All external control system and communication connections are identified and protected from tampering or damage.

2.8.18.2 Supplemental Guidance

External access point connections to the control system need to be secured to protect the system. Access points include any externally connected communication end point (for example, dialup modems) terminating at any device within the electronic security perimeter. The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information needs to be documented, tracked, and audited periodically. After identifying these connection points, the extent of their protection needs to be determined. Policies and procedures need to be developed and implemented to protect the connection to the business or enterprise system. This might include disabling the connection except when specific access is requested for a specific need, automatic timeout for the connection, etc.

2.8.18.3 Requirement Enhancements

None

2.8.18.4 References

NIST SP 800-53r3	CA-3
CAG	CC-5
API 1164r2	3.6, Annex B.1, B.2, B.3
NERC CIPS	CIP 005-3. B.R1 through R1.3

NRC RG 5.71	C.3.1.3, C.3.1.4, App. B.1.1, App. B.1.22, App. B.4.5, App. B.5.2, App. C.3.4, App. C.7, App. C.9.1, App. C.11.3

2.8.19 Security Roles

2.8.19.1 Requirement

The control system design and implementation specifies the security roles and responsibilities for the users of the system.

2.8.19.2 Supplemental Guidance

Security roles and responsibilities for control system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals.

2.8.19.3 Requirement Enhancements

None

2.8.19.4 References

NIST SP 800-53r3	AC-5, PS-2
API 1164r2	1.2, Annex A
NERC CIPS	CIP 002-3. through CIP 009-3
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. B.1.22, App. C.10.10

2.8.20 Session Authenticity

2.8.20.1 Requirement

The control system provides mechanisms to protect the authenticity of device-to-device communications sessions.

2.8.20.2 Supplemental Guidance

Message authentication provides protection from malformed traffic from misconfigured devices and malicious entities. The intent is to establish confidence at each end of a communications session with respect to the validity of the data and the identity of the sender. This is to address man-in-the middle attacks, which can include session hijacking, insertion of fake information, or instruction sets in the middle of a session.

In situations where the ICS cannot protect the authenticity of communications sessions, the organization employs compensating controls (e.g., auditing measures, isolation/segmented architecture, additional physical isolation). Enhanced auditing measures or encryption mechanisms designed to enhance session authenticity must not impact ICS operations by consuming too many available resources or by slowing down communications to an unacceptable level as to constitute a self-inflicted denial-of-service attack.

2.8.20.3 Requirement Enhancements

Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

2.8.20.4 References

NIST SP 800-53r3	SC-23
API 1164r2	5.9, 7.2.2, 8.1, Annex A, Annex B.1, B.2, B.3

NRC RG 5.71	App. 3.1.1, App. B.3.6, App. B.3.18

2.8.21 Architecture and Provisioning for Name/Address Resolution Service

2.8.21.1 Requirement

The control system devices that collectively provide name/address resolution services for an organization are fault tolerant and implement address space separation.

2.8.21.2 Supplemental Guidance

In general, do not use domain name system (DNS) services on a control system. Host-based name resolution solutions are the recommended practice. However, if DNS services are implemented, deploy at least two authoritative DNS servers. The DNS configuration on the host will reference one DNS server as the primary source and the other as the secondary source. In addition, locate the two DNS servers on different network subnets and separate geographically. If control system resources are accessible from external networks, establish authoritative DNS servers with separate address space views (internal and external) to the control system resources. The DNS server with the internal view provides name/address resolution services within the control system boundary. The DNS server with the external view only provides name/address resolution information pertaining to control system resources accessible from external resources. The list of clients who can access the authoritative DNS server with a particular view is also specified.

2.8.21.3 Requirement Enhancements

The use of secure name/address resolution services must not adversely impact the operational performance of the control system.

2.8.21.4 References

NIST SP 800-53r3	SC-22
CAG	CC-16
NRC RG 5.71	App. B.3.6, App. B.3.17

2.8.22 Secure Name/Address Resolution Service (Authoritative Source)

2.8.22.1 Requirement

The control system resource (i.e., authoritative DNS server) that provides name/address resolution service provides additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.

2.8.22.2 Supplemental Guidance

In general, do not use DNS services on a control system. Host-based name resolution solutions are best practice. This requirement enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A DNS server is an example of control system resource that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data.

2.8.22.3 Requirement Enhancements

The control system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

2.8.22.4 References

NIST SP 800-53r3	SC-20
CAG	CC-16
NRC RG 5.71	App. B.3.15

2.8.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

2.8.23.1 Requirement

The control system resource (i.e., resolving or caching name server) that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative DNS servers when requested by client systems.

2.8.23.2 Supplemental Guidance

In general, do not use DNS services on a control system. Host-based name resolution solutions are best practice. A resolving or caching DNS server is an example of a control system resource that provides name/address resolution service for local clients, and authoritative DNS servers are examples of authoritative sources.

2.8.23.3 Requirement Enhancements

The control system resource that implements DNS services performs data origin authentication and data integrity verification on all resolution responses whether local DNS clients (i.e., stub resolvers) explicitly request this function.

2.8.23.4 References

NIST SP 800-53r3	SC-21
CAG	CC-16
NRC RG 5.71	App. B.3.16, App. B.3.18, App. B.4.4

2.8.24 Fail in Known State

2.8.24.1 Requirement

The control system fails to a known state for defined failures.

2.8.24.2 Supplemental Guidance

Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization's mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the control system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property.

2.8.24.3 Requirement Enhancements

The control system preserves defined system state information in failure.

2.8.24.4 References

NIST SP 800-53r3	SC-24
CAG	CC-14
NRC RG 5.71	App. B.1.17, App. B.3.22

2.8.25 Thin Nodes

2.8.25.1 Requirement

The control system employs processing components that have minimal functionality and data storage.

2.8.25.2 Supplemental Guidance

The deployment of control system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, control systems, and services to a successful attack.

2.8.25.3 Requirement Enhancements

Use secure data transmission media, such as fiber optic technology, to minimize data loss from eavesdropping and data tapping.

2.8.25.4 References

NIST SP 800-53r3	SC-25
NRC RG 5.71	App. B.3.19

2.8.26 Honeypots

2.8.26.1 Requirement

The control system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

2.8.26.2 Supplemental Guidance

Not all ICS users should use honeypots. Only specialized entities using nonoperational equipment in highly isolated and protected zones should attempt deployment of honeypots. Created honeypots determine if active entities are attacking/probing the particular configuration the honeypot is mimicking. If deployed incorrectly, this technique can lead to a direct shortcut of established cybersecurity measures. This is a very specialized and limited application and should not be widely used.

2.8.26.3 Requirement Enhancements

The control system includes components that proactively seek to identify web-based malicious code.

2.8.26.4 References

NIST SP 800-53r3	SC-26
CAG	CC-12

2.8.27 Operating System-Independent Applications

2.8.27.1 Requirement

The control system includes organization-defined applications that are independent of the operating system.

2.8.27.2 Supplemental Guidance

Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system.

2.8.27.3 Requirement Enhancements

None

2.8.27.4 References

NIST SP 800-53r3	SC-27
NRC RG 5.71	App. C.12.5

2.8.28 Confidentiality of Information at Rest

2.8.28.1 Requirement

The control system protects the confidentiality of information at rest. Examples of data at rest are: configuration files and settings, alarm point setting, password files, and security filter rules.

2.8.28.2 Supplemental Guidance

This control is intended to address the confidentiality of information in nonmobile devices.

2.8.28.3 Requirement Enhancements

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures.

2.8.28.4 References

NIST SP 800-53r3	SC-28
CAG	CC-15
API 1164r2	Annex A
NRC RG 5.71	App. B.3.20

2.8.29 Heterogeneity

2.8.29.1 Requirement

The organization employs diverse technologies in the implementation of the control system.

2.8.29.2 Supplemental Guidance

Increasing the diversity of technologies within the control system reduces the impact from the exploitation of a specific technology.

2.8.29.3 Requirement Enhancements

None

2.8.29.4 References

NIST SP 800-53r3	SC-29
NRC RG 5.71	App. B.3.21

2.8.30 Virtualization Techniques

2.8.30.1 Requirement

The organization employs virtualization techniques to present gateway components into control systems environments as other types of components or components with differing configurations.

2.8.30.2 Supplemental Guidance

Virtualization techniques provide organizations with the ability to disguise gateway components into control systems environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

2.8.30.3 Requirement Enhancements

1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications.
2. The organization changes the diversity of operating systems and applications on an organization-defined frequency.
3. The organization employs randomness in the implementation of the virtualization.

2.8.30.4 References

NIST SP 800-53r3	SC-30
CAG	CC-5

2.8.31 Covert Channel Analysis

2.8.31.1 Requirement

The organization requires that control system developers/integrators perform covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

2.8.31.2 Supplemental Guidance

Control system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when the potential exists for unauthorized information flows across security domains in the case of control systems containing export controlled information and having connections to the Internet.

2.8.31.3 Requirement Enhancements

The organization tests a subset of the vendor identified covert channel avenues to determine if they are exploitable.

2.8.31.4 References

NIST SP 800-53r3	SC-31
CAG	CC-5

2.8.32 Information System Partitioning

2.8.32.1 Requirement

The organization partitions the information system into components residing in separate physical domains (or environments) as necessary.

2.8.32.2 Supplemental Guidance

Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning when system components can be associated with different system impact levels derived from the categorizations. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

2.8.32.3 Requirement Enhancements

None

2.8.32.4 References

NIST SP 800-53r3	SC-32
NRC RG 5.71	App. B.3.2.2

2.8.33 Transmission Preparation Integrity

2.8.33.1 Requirement

The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

2.8.33.2 Supplemental Guidance

Information can be subjected to unauthorized changes (i.e., malicious and unintentional modification) at information aggregation or protocol transformation points.

2.8.33.3 Requirement Enhancements

None

2.8.33.4 References

NIST SP 800-53r3	SC-33
NRC RG 5.71	App. B.3.6

2.8.34 Non-Modifiable Executable Programs

2.8.34.1 Requirement

The information system:

1. Loads and executes the operating system software from hardware-enforced, read-only media
2. Loads and executes authorized applications from hardware-enforced, read-only media.

2.8.34.2 Supplemental Guidance

In this control, operating system software is defined as the base code on which applications are hosted. Hardware-enforced, read-only media include CD-R/DVD-Rs. The use of nonmodifiable storage media ensures the integrity of the software from the point of creation as a read-only image.

2.8.34.3 Requirement Enhancements

1. The organization employs system components with no writable storage that is persistent across component restart or power on/off cycles.

   Enhanced Supplemental Guidance—This control enhancement eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system component and requires that no removable storage be employed.

2. The Organization protects the integrity of the information on read-only media.

   Enhanced Supplemental Guidance—This control enhancement covers protection of the integrity of information placed on read-only media, controlling the media after information has been recorded onto the media. Measures may include a combination of prevention and detection/response.

2.8.34.4 References

NIST SP 800-53r3	SC-34

2.9 Information and Document Management

Information and document management is generally a part of the company records retention and document management system. Digital and hardcopy information associated with the development and execution of a control system is important and sensitive and needs to be managed. Control system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive company information and need to be protected. Security measures, philosophy, and implementation strategies are other examples. In addition, business conditions change and require updated analyses and studies. Care is given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

The following are the controls for Information and Document Management that need to be supported and implemented by the organization to protect the control system.

2.9.1 Information and Document Management Policy and Procedures

2.9.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, control system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the control system information and document management policy and associated system maintenance controls.

2.9.1.2 Supplemental Guidance

The organization ensures the control system information and document management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system information and document management policy can be included as part of the general information security policy for the organization. System information and document management procedures can be developed for the security program in general and for a particular control system when required.

2.9.1.3 Requirement Enhancements

None

2.9.1.4 References

NIST SP 800-53r3	SI-1
API 1164r2	Annex A
NERC CIPS	CIP 002-3. through CIP 009-3
NRC RG 5.71	App. C.3.1, App. C.11

2.9.2 Information and Document Retention

2.9.2.1 Requirement

The organization manages control system-related data, including establishing retention policies and procedures for both electronic and paper data and manages access to the data based on formally assigned roles and responsibilities.

2.9.2.2 Supplemental Guidance

The organization develops policies and procedures detailing the retention of company information. These procedures address retention/destruction issues for all applicable information media. Any legal or regulatory requirements are considered when developing these policies and procedures. Information associated with the development and execution of a control system is important, sensitive, and needs to be appropriately managed. The National Archives and Records Administration provides guidance on records retention.

2.9.2.3 Requirement Enhancements

The organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations.

2.9.2.4 References

NIST SP 800-53r3	SI-12
API 1164r2	Annex A
NERC CIPS	CIP 003-3.B.R4
NRC RG 5.71	C.5, App. B.2.11, App. C.3.4, App. C.3.10

2.9.3 Information Handling

2.9.3.1 Requirement

Organization implemented policies and procedures detailing the handling of information are developed and periodically reviewed and updated.

2.9.3.2 Supplemental Guidance

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of control system information. These policies or procedures include the periodic review of all information to ensure it is properly handled. The organization protects information against unauthorized access, misuse, or corruption during transportation or transmission. The organization distributes or shares information on a need-to-know basis and considers legal and regulatory requirements when developing these policies and procedures.

2.9.3.3 Requirement Enhancements

None

2.9.3.4 References

NIST SP 800-53r3	MP-1, SI-12
API 1164r2	Annex A
NERC CIPS	CIP 002-3. B.R4.1
NRC RG 5.71	App. B.3.1, App. C.1.2

2.9.4 Information Classification

2.9.4.1 Requirement

All information is classified to indicate the protection required commensurate with its sensitivity and consequence.

2.9.4.2 Supplemental Guidance

A minimum of three levels of classification should be defined for control system information to indicate the protection required commensurate with its sensitivity and consequence. These levels may be company proprietary, restricted, or public, indicating the need, priority, and level of protection required for that information. These information classification levels provide guidance for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.

2.9.4.3 Requirement Enhancements

None

2.9.4.4 References

NIST SP 800-53r3	RA-2
CAG	CC-9
API 1164r2	6, Annex A
NERC CIPS	CIP 003-3. B.R4.2
NRC RG 5.71	App. C.8.4

2.9.5 Information Exchange

2.9.5.1 Requirement

Formal contractual and confidentiality agreements are established for the exchange of information and software between the organization and external parties.

2.9.5.2 Supplemental Guidance

When it is necessary for the control system to communicate information to another organization or external party system, the operators need to mutually develop a formal contractual and confidentiality agreement and use a secure method of communication. These formal exchange policies, procedures, and security controls need to be in place to protect the exchange of information using all types of communication facilities.

2.9.5.3 Requirement Enhancements

If a specific device needs to communicate with another device outside the control system network, communications need to be limited to only the devices that need to communicate. All other ports and routes need to be locked down or disabled.

2.9.5.4 References

NIST SP 800-53r3	SC-16
API 1164r2	Annex A
NERC CIPS	CIP 003-3. B.R5
NRC RG 5.71	App. B.3.12

2.9.6 Information and Document Classification

2.9.6.1 Requirement

The organization develops policies and procedures to classify data, including establishing:

1. Retention policies and procedures for both electronic and paper media
2. Classification policies and methods (e.g., restricted, classified, general)

3. Access and control policies, to include sharing, copying, transmittal, and distribution appropriate for the level of protection required
4. Access to the data based on formally assigned roles and responsibilities for the control system.

2.9.6.2 Supplemental Guidance

Companies use both comprehensive information and document management policies for their cybersecurity management system. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection. The organization defines information classification levels (e.g., restricted, classified, general) for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required. The organization also classifies all information (i.e., control system design information, network diagrams, process programs, vulnerability assessments) to indicate the need, priority, and level of protection required commensurate with its sensitivity and consequence.

2.9.6.3 Requirement Enhancements

The organization periodically reviews information that requires special control or handling to determine whether such special handling is still required.

2.9.6.4 References

NIST SP 800-53r3	AC-1, AC-3, MP-1, MP-3
CAG	CC-9
API 1164r2	6, Annex A
NERC CIPS	CIP 003-3. B.R4.2
NRC RG 5.71	App. B.3.1, App. C.1.3

2.9.7 Information and Document Retrieval

2.9.7.1 Requirement

The organization develops policies and procedures that provide details of the retrieval of written and electronic records, equipment, and other media for the control system in the overall information and document management policy.

2.9.7.2 Supplemental Guidance

The organization employs appropriate measures to ensure long-term records information can be retrieved (i.e., converting the data to a newer format, retaining older equipment that can read the data). Any legal or regulatory requirements are considered when developing these policies and procedures. The organization takes special care to confirm the security, availability, and usability of the control system configuration, which includes the logic used in developing the configuration or programming for the life of the control system.

2.9.7.3 Requirement Enhancements

None

2.9.7.4 References

NIST SP 800-53r3	AC-1
API 1164r2	Annex A
NRC RG 5.71	App. C.1.2

2.9.8 Information and Document Destruction

2.9.8.1 Requirement

The organization develops policies and procedures detailing the destruction of written and electronic records, equipment, and other media for the control system, without compromising the confidentiality of the data.

2.9.8.2 Supplemental Guidance

The organization develops policies and procedures detailing the destruction and disposal of written and electronic records, equipment, and other media in the overall information and document management policy. This also includes the method of disposal such as shredding of paper records, erasing of disks or other electronic media, or physical destruction. All legal or regulatory requirements need to be considered when developing these policies and procedures.

2.9.8.3 Requirement Enhancements

None

2.9.8.4 References

API 1164r2	Annex A
NRC RG 5.71	App. C.1.2

2.9.9 Information and Document Management Review

2.9.9.1 Requirement

The organization performs periodic reviews of compliance with the control system information and document security management policy to ensure compliance with any laws and regulatory requirements.

2.9.9.2 Supplemental Guidance

The organization periodically reviews compliance in the information and document management security policy. The compliance review procedure needs to consider all legal and regulatory documentation requirements applicable to the control system.

2.9.9.3 Requirement Enhancements

None

2.9.9.4 References

API 1164r2	1.2, Annex A
NERC CIPS	CIP 003-3. D
NRC RG 5.71	App. B.2.3, App. C.1.2

2.9.10 Media Marking

2.9.10.1 Requirement

The organization:

1. Marks, in accordance with organizational policies and procedures, removable system media and system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information

2. Exempts an organization-defined list of media types or hardware components from marking as long as the exempted items remain within the organization-defined protected environment (e.g., controlled areas).

2.9.10.2 Supplemental Guidance

The term marking is distinguished from the term labeling. Marking is used in security controls when referring to information that is human-readable. The term labeling is used in the context of marking internal data structures within the system for access control purposes for information in process, in storage, or in transit. Removable system media include both digital media (e.g., magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs, diskettes) and nondigital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, marking is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations may require marking for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information including monitors and printers. Marking of removable media and information system output is consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance.

2.9.10.3 Requirement Enhancements

None

2.9.10.4 References

NIST SP 800-53r3	MP-3
CAG	CC-9
API 1164r2	Annex A
NRC RG 5.71	App. C.1.3

2.9.11 Security Attributes

2.9.11.1 Requirement

The control system supports and maintains the binding of user-defined security attributes to information in storage, in process, and in transmission in accordance with:

1. Access control requirements
2. Special dissemination, handling, or distribution instructions
3. Otherwise, as required by the system security policy.

2.9.11.2 Supplemental Guidance

Security attributes are specified characteristics used on internal data structures to enable the implementation of access control, flow control, special dissemination, handling, or distribution instructions or to support other aspects of the information security policy. The term security label is often used to associate a set of security attributes with a specific information object as part of the data structure for that object (e.g., user access privileges, nationality, and contractor affiliation). Such labels are often used to implement access control and flow control policies.

2.9.11.3 Requirement Enhancements

1. The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.
2. The information system allows authorized entities to change security attributes.

3. The information system maintains the binding of security attributes to information with sufficient assurance that the information attribute association can be used as the basis for automated policy actions.

   Enhanced Supplemental Guidance—Examples of automated policy actions include automated access control decisions (e.g., mandatory Access Control decisions) or decisions to release/or not release information (e.g., information flows via cross domain systems).

4. The information system allows authorized users to associate security attributes with information

   Enhanced Supplemental Guidance—The support provided by the information system can vary from prompting users to select security attributes to be associated with specific information objects, to ensure that the combination of attributes selected is valid.

5. The information system displays security attributes in human-readable form on each object-output from the system-to-system output devices to identify special dissemination, handling, or distribution instructions.

   Enhanced Supplemental Guidance—Objects output from the information system include pages, screens, or equivalent. Output devices include printers, video displays on computer terminals, monitors, screens on HMIs, notebooks/laptop computer, and personal digital assistants.

2.9.11.4 References

NIST SP 800-53r3	AC-16
NRC RG 5.71	App. C.1.3

2.10 System Development and Maintenance

Security is most effective when it is designed into the control system and sustained, through effective maintenance, throughout the life cycle of the system and through all future configurations. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a control system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

2.10.1 System Maintenance Policy and Procedures

2.10.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, control system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the control system maintenance policy and associated system maintenance controls.

2.10.1.2 Supplemental Guidance

The organization ensures the control system maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular control system when required.

2.10.1.3 Requirement Enhancements

None

2.10.1.4 References

NIST SP 800-53r3	MA-1
API 1164r2	3.6, Annex A
NERC CIPS	CIP 007-3. A
NRC RG 5.71	C.3.3.2.4, C.4, App. C.4.1

2.10.2 Legacy System Upgrades

2.10.2.1 Requirement

The organization develops policies and procedures to upgrade existing legacy control systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the system and processes controlled.

2.10.2.2 Supplemental Guidance

Legacy systems are those control systems currently in place for control of the organization's processes. In some cases, these systems were installed before a concern about system security existed, and hence, security mitigation measures were not included. The organization determines the current configuration of the control system and then provides system upgrades as required to meet the organization's security requirements.

2.10.2.3 Requirement Enhancements

None

2.10.2.4 References

NIST SP 800-53r3	SA-8
CAG	CC-7, CC-16
API 1164r2	Annex B.3.1.6.2
NRC RG 5.71	App. C.12.4

2.10.3 System Monitoring and Evaluation

2.10.3.1 Requirement

The organization conducts periodic security vulnerability assessments according to the risk management plan. The control system is then updated to address any identified vulnerabilities in accordance with organization's control system maintenance policy.

2.10.3.2 Supplemental Guidance

Control systems need to be monitored and evaluated according to the risk management plan periodically to identify vulnerabilities or conditions that might affect the security of a control system. The frequency of these evaluations needs to be based on the organization's risk mitigation policy. Changing security requirements and vulnerabilities necessitate a system review. These reviews need to be carefully planned and documented in accordance with the organization configuration management policy to identify any changes to the system. The organization maintains contact with other organizations that have similar systems to determine changing vulnerabilities.

2.10.3.3 Requirement Enhancements

None

2.10.3.4 References

NIST SP 800-53r3	CA-2
CAG	CC-17
API 1164r2	3.3, Annex B.2.1
NERC CIPS	CIP 007-3. B.R6
NRC RG 5.71	C.4.1.2

2.10.4 Backup and Recovery

2.10.4.1 Requirement

The organization makes and secures backups of critical system software, applications, and data for use if the control system operating system software becomes corrupted or destroyed.

2.10.4.2 Supplemental Guidance

Control system operating software may be compromised due to an incident or disaster. A copy of the operating system software needs to be made, updated regularly, and stored in a secure environment so that it can be used to restore the control system to normal operations. In many instances, a backup control site can serve this purpose.

2.10.4.3 Requirement Enhancements

None

2.10.4.4 References

NIST SP 800-53r3	CP-6, CP-10
CAG	CC-13
API 1164r2	3.4, Annex A
NERC CIPS	CIP 009-3 B.R4
NRC RG 5.71	App. C.8.1, App. C.9.1, App. C.9.5, App. C.9.6, App. C.9.7

2.10.5 Unplanned System Maintenance

2.10.5.1 Requirement

The organization reviews and follows security requirements for a control system before undertaking any unplanned maintenance activities of control system components (including field devices). Documentation includes the following:

1. The date and time of maintenance
2. The name of the individual(s) performing the maintenance
3. The name of the escort, if necessary
4. A description of the maintenance performed
5. A list of equipment removed or replaced (including identification numbers, if applicable).

2.10.5.2 Supplemental Guidance

Unplanned maintenance is required to support control system operation in the event of system/component malfunction or failure. Security requirements necessitate that all unplanned maintenance activities use approved contingency plans and document all actions taken to restore operability to the system.

2.10.5.3 Requirement Enhancements

The organization documents the decision and justification should unplanned maintenance not be performed on a control system after the identification of a security vulnerability.

2.10.5.4 References

API 1164r2	3.4, 3.8, Annex A, Annex B.3.1
NRC RG 5.71	App. C.3.11, App. C.4.1

2.10.6 Periodic System Maintenance

2.10.6.1 Requirement

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on system components in accordance with manufacturer or vendor specifications and/or organizational requirements
2. Explicitly approves the removal of the system or system components from organizational facilities for offsite maintenance or repairs
3. Sanitizes the equipment to remove all information from associated media prior to removal from organizational facilities for offsite maintenance or repairs
4. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

2.10.6.2 Supplemental Guidance

The control is intended to address the security aspects of the organization’s system maintenance program. All maintenance activities to include routine, scheduled maintenance and repairs are controlled whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Maintenance procedures that require the physical removal of any control system component need to be documented, listing the date, time, reason for removal, estimated date of reinstallation, and name personnel removing components. These activities need to be approved by the appropriate organization officials. If the control system or component requires offsite repair, the organization removes all critical/sensitive information from associated media using approved procedures. After maintenance is performed on the control system, the organization checks the security features to ensure that they are still functioning properly.

2.10.6.3 Requirement Enhancements

1. The organization maintains maintenance records for the system that include (a) the date and time of maintenance; (b) name of the individual performing the maintenance; (c) name of escort, if necessary; (d) a description of the maintenance performed; and (e) a list of equipment removed or replaced (including identification numbers, if applicable).
2. The organization employs automated mechanisms to schedule and document maintenance and repairs as required, producing up-to-date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

2.10.6.4 References

NIST SP 800-53r3	MA-2

NRC RG 5.71	App. C.4.1

2.10.7 Maintenance Tools

2.10.7.1 Requirement

The organization approves and monitors the use of system maintenance tools.

2.10.7.2 Supplemental Guidance

The intent of this control is to address the security-related issues arising from the hardware and software brought into the system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and software components that may support system maintenance, yet are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch), are not covered by this control.

2.10.7.3 Requirement Enhancements

1. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.
2. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the system.
3. The organization prevents the unauthorized removal of maintenance equipment by one of the following: (a) verifying that no organizational information is contained on the equipment, (b) sanitizing or destroying the equipment, (c) retaining the equipment within the facility, or (d) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.
4. The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.
5. Maintenance tools are used with care on control system networks to ensure that control system operations will not be degraded by their use.

2.10.7.4 References

NIST SP 800-53r3	MA-3
API 1164r2	5.8, Annex B.4.11
NRC RG 5.71	App. C.4.2

2.10.8 Maintenance Personnel

2.10.8.1 Requirement

The organization documents authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the control system. Only authorized and qualified organization or vendor personnel perform maintenance on the control system.

2.10.8.2 Supplemental Guidance

Maintenance personnel need to have appropriate access authorization to the control system when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the control system.

2.10.8.3 Requirement Enhancements

None

2.10.8.4 References

NIST SP 800-53r3	MP-5
API 1164r2	3.1, Annex A
NRC RG 5.71	App. B.1.22, App. C.4.3

2.10.9 Non-Local (Remote) Maintenance

2.10.9.1 Requirement

The organization:

1. Authorizes and monitors and controls remotely executed maintenance and diagnostic activities
2. Allows the use of remote maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system
3. Maintains records for remote maintenance and diagnostic activities
4. Terminates all sessions and remote connections when remote maintenance is completed
5. Changes passwords following each remote maintenance session, if password-based authentication is used to accomplish remote maintenance.

2.10.9.2 Supplemental Guidance

Individuals communicating through an external, nonorganization-controlled network (e.g., the Internet) conduct remote maintenance and diagnostic activities. Identification and authentication techniques used in remote maintenance and diagnostic sessions are consistent with Section 2.15.1, “Access Control Policy and Procedures.” Strong authentication and enforcement requirements are in other controls in Section 2.8, “System and Communications Protection”; Section 2.10, “System Development and Maintenance”; Section 2.14, “System and Information Integrity”; and Section 2.15, “Access Controls.”

2.10.9.3 Requirement Enhancements

1. The organization audits remote maintenance and diagnostic sessions, and designated organizational personnel review the maintenance records of the remote sessions.
2. The organization documents the installation and use of remote maintenance and diagnostic links.
3. The organization:
   a. Requires that remote maintenance or diagnostic services be performed from a system that implements a level of security at least as high as that implemented on the system being serviced or
   b. Removes the component to be serviced from the system and prior to remote maintenance or diagnostic services, sanitizes the component (e.g., clearing of set points, embedded network addresses and embedded security validation information) before removal from organizational facilities. After the service is performed and the component is returned to the facility, the organization should check or reinstall the authorized firmware code as specified by the configuration management plan and reset all authorized embedded configuration settings. This should remove potentially malicious software that may have been added via “new” firmware. This should be done before reconnecting the component to the system.

4. The organization requires that remote maintenance sessions be protected by a strong authenticator tightly bound to the user.
5. The organization requires that
   a. Maintenance personnel notify the system administrator when remote maintenance is planned (i.e., date/time)
   b. A designated organizational official with specific security/system knowledge approves the remote maintenance.
6. The organization employs cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.
7. The organization employs remote disconnect verification at the termination of remote maintenance and diagnostic sessions.

2.10.9.4 References

NIST SP 800-53r3	MA-4
API 1164r2	5, 8.1, 8.2.4, Annex A
NRC RG 5.71	App. B.1.22, App. B.3.11

2.10.10 Timely Maintenance

2.10.10.1 Requirement

The organization obtains maintenance support and spare parts for organization-defined list of security-critical system components within organization-defined period of failure.

2.10.10.2 Supplemental Guidance

The organization specifies those system components that, when not operational, result in increased risk to organizations, individuals, or the nation because the security functionality intended by that component is not being provided. Security-critical components include firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

2.10.10.3 Requirement Enhancements

None

2.10.10.4 References

NIST SP 800-53r3	MA-6
API 1164r2	Annex A
NERC CIPS	CIP 008-3 B.R8, CIP 009-3 B.R4
NRC RG 5.71	C.3.3.2.4, App. C.4.1

2.11 Security Awareness and Training

Physical and cyber control system security awareness is a critical part of control system incident prevention, particularly with regard to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information such as passwords. This information can then be used to compromise otherwise secure systems. Implementing a control system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals’ roles and responsibilities. Communication vehicles need to be developed to help employees understand why new access and control methods are required and how they can reduce risks and impacts to the organization. Training programs also need to demonstrate management's commitment to cyber and control system security programs. Feedback from staff can be valuable for refining the security program.

Following are the controls for awareness and training that need to be supported and implemented by the organization to protect the control system.

2.11.1 Security Awareness and Training Policy and Procedures

2.11.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

2.11.1.2 Supplemental Guidance

The organization ensures the security awareness and training policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular control system when required.

2.11.1.3 Requirement Enhancements

None

2.11.1.4 References

NIST SP 800-53r3	AT-1
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B
NERC CIPS	CIP 004-3 A, B, C, D
NRC RG 5.71	C.3.3.2.8, App. C.10.1, App. C.10.2, App. C.10.4, App. C.10.6

2.11.2 Security Awareness

2.11.2.1 Requirement

The organization provides basic security awareness training to all control system users (including managers, senior executives, and contractors) before authorizing access to the system, when required by system changes, and at least annually thereafter. The effectiveness of security awareness training, at the organization level, needs to be reviewed once a year at a minimum.

2.11.2.2 Supplemental Guidance

The organization determines the content of security awareness training and security awareness techniques based on the specific requirements of the organization and the systems to which personnel have authorized access. Security awareness techniques can include displaying posters, offering security-messaged items, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting security awareness events. The security awareness training program is consistent with the requirements contained in CFR Part 5 Subpart C (5 CFR 930.301).

2.11.2.3 Requirement Enhancements

1. All control system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training.
2. The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

2.11.2.4 References

NIST SP 800-53r3	AT-2
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B
NERC CIPS	CIP 004-3 A, B.R1
NRC RG 5.71	App. C.10.1

2.11.3 Security Training

2.11.3.1 Requirement

The organization:

1. Defines and documents system security roles and responsibilities throughout the system development life cycle
2. Identifies individuals having system security roles and responsibilities
3. Provides security-related technical training: (a) before authorizing access to the system or performing assigned duties, (b) when required by system changes, and (c) on an organization-defined frequency, thereafter.

2.11.3.2 Supplemental Guidance

The organization determines the content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, security-related technical training to perform their assigned duties. The organization’s security training program is consistent with the requirements contained in CFR Part 5 Subpart C (5 CFR 930.301).

2.11.3.3 Requirement Enhancements

None

2.11.3.4 References

NIST SP 800-53r3	AT-3
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B
NERC CIPS	CIP 004-3 B.R2
NRC RG 5.71	C.3.3.2.8, App. C.10.2, App. C.10.4, App. C.10.6

2.11.4 Security Training Records

2.11.4.1 Requirement

The organization documents, maintains, and monitors individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization's records retention policy.

2.11.4.2 Supplemental Guidance

The organization maintains a record of training requirements for each user in accordance with the provisions of the organization training and records retention policy.

2.11.4.3 Requirement Enhancements

None

2.11.4.4 References

NIST SP 800-53r3	AT-4
API 1164r2	3.1
NERC CIPS	CIP 004-3 B.R2.3
NRC RG 5.71	App. C.10.8

2.11.5 Contact with Security Groups and Associations

2.11.5.1 Requirement

The organization establishes and maintains contact with security groups and associations to stay up-to-date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.

2.11.5.2 Supplemental Guidance

Security groups and associations can include special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to systems are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

2.11.5.3 Requirement Enhancements

None

2.11.5.4 References

NIST SP 800-53r3	AT-5
API 1164r2	3.4
NERC CIPS	CIP 008-3 B.R1.3
NRC RG 5.71	App. C.10.9

2.11.6 Security Responsibility Testing

2.11.6.1 Requirement

The organization documents and tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the control system.

2.11.6.2 Supplemental Guidance

The organization maintains a list of security responsibilities for each user. These need to be used to test each user in accordance with the provisions of the organization training policy. Users must be notified when their testing is scheduled, informed as to how it will be conducted, and notified of the results. The security responsibility testing needs to be conducted at least annually and/or as warranted by technology/procedural changes.

2.11.6.3 Requirement Enhancements

None

2.11.6.4 References

NIST SP 800-53r3	MA-6
API 1164r2	3.5
NRC RG 5.71	App. C.3.6, App. C.12.5, App. C.12.6, App. C.13.1

2.12 Incident Response

Incident response addresses the capability to continue or resume operations of a control system in the event of disruption of normal system operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the control system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters, such as earthquakes, tornados, floods, or from manmade events like riots, terrorism, or vandalism. The ability for the control system to function after such an event is directly dependent on implementing policies, procedures, training, and resources in place ahead of time using the organizations planning process. The security controls recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the control systems for an organization.

2.12.1 Incident Response Policy and Procedures

2.12.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

2.12.1.2 Supplemental Guidance

The organization ensures the incident response policy and procedures are consistent with applicable laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular system, when required.

2.12.1.3 Requirement Enhancements

None

2.12.1.4 References

NIST SP 800-53r3	IR-1
CAG	CC-18
API 1164r2	3.5
NERC CIPS	CIP 008-3
NRC RG 5.71	App. C.8.1

2.12.2 Continuity of Operations Plan

2.12.2.1 Requirement

The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or re-establishing production in case of an undesirable interruption for a control system. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan.

2.12.2.2 Supplemental Guidance

A continuity of operations plan addresses both business continuity planning and recovery of control system operations. Development of a continuity of operations plan is a process to identify procedures for safe control system operation while recovering from a significant system disruption. The plan requires documentation of critical control system functions that need to be recovered.

2.12.2.3 Requirement Enhancements

1. The continuity of operations plan delineates that at the time of the disruption to normal system operations, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities.
2. The organization initiates a root cause analysis for the event and submits any findings from the analysis to the organizations corrective action program.
3. The organization then resumes normal operation of the system in accordance with its policies and procedures.

2.12.2.4 References

NIST SP 800-53r3	CP-2
API 1164r2	3.4, Annex A
NERC CIPS	CIP 003-3 B.R4.1, CIP 009-3
NRC RG 5.71	App. C.9.2

2.12.3 Continuity of Operations Roles and Responsibilities

2.12.3.1 Requirement

The organization’s continuity of operations plan defines and communicates the specific roles and responsibilities for each part of the plan in relation to various types of control system incidents.

2.12.3.2 Supplemental Guidance

The continuity of operations plan defines the roles and responsibilities of the various employees and contractors in the event of a significant incident. The plans identify responsible personnel to lead the recovery and response effort if an incident occurs.

2.12.3.3 Requirement Enhancements

None

2.12.3.4 References

NIST SP 800-53r3	CP-3
API 1164r2	3.5
NERC CIPS	CIP 009-3 B.R1.2
NRC RG 5.71	App. C.9.4

2.12.4 Incident Response Training

2.12.4.1 Requirement

The organization:

1. Trains personnel in their incident response roles and responsibilities with respect to the system
2. Provides refresher training on an organization-defined frequency, at least annually.

2.12.4.2 Supplemental Guidance

Training needs to be provided to individuals in the control system community so that all users of the control system understand the content, purpose, and implementation of the plans. The organization provides continuity of operations training and refresher sessions annually.

2.12.4.3 Requirement Enhancements

1. The organization incorporates control system simulated events into continuity of operations training to facilitate effective response by personnel in crisis situations.
2. The organization employs automated mechanisms to provide a thorough and realistic control system training environment.

2.12.4.4 References

NIST SP 800-53r3	IR-2
CAG	CC-18
API 1164r2	3.5, Annex A, Annex B.5.1.2.4
NERC CIPS	CIP 008-3 B.R1.6
NRC RG 5.71	App. C.8.2

2.12.5 Continuity of Operations Plan Testing

2.12.5.1 Requirement

The organization tests the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization review the documented test results and initiate corrective actions if necessary. The organization tests the continuity of operations plan for the control system at least annually, using organization prescribed tests and exercises to determine the plan’s effectiveness and the organization’s readiness to execute the plan.

2.12.5.2 Supplemental Guidance

The organization maintains a list of incident response activities and mitigations for each user in accordance with the provisions of the organization incident response policy and procedures. Users need to be notified when their testing is scheduled and informed as to how it will be conducted. Several methods for testing and/or exercising continuity of operations plans exist for identifying potential weaknesses (e.g., full-scale business continuity plan testing, functional/tabletop exercises). Following the preparation of the various plans, a schedule needs to be developed to review and test each plan and ensure that each still meets the objectives.

2.12.5.3 Requirement Enhancements

1. The organization coordinates continuity of operations plan testing and exercises with organizational elements responsible for related plans.
2. The organization tests and exercises the continuity of operations plan at the alternate processing site to familiarize control system operations personnel with the facility and available resources and to evaluate the site's capabilities to support continuity of operations.
3. The organization employs automated mechanisms to thoroughly and effectively test and exercise the continuity of operations plan by providing complete coverage of operational issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the control system and supported missions.

2.12.5.4 References

NIST SP 800-53r3	CP-4, IR-3
API 1164r2	3.5, Annex A
NERC CIPS	CIP 008-3 B.R1.6
NRC RG 5.71	App. C.9.3, App. C.9.7

2.12.6 Continuity of Operations Plan Update

2.12.6.1 Requirement

The organization reviews the continuity of operations plan for the control system at least annually and updates the plan to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.

2.12.6.2 Supplemental Guidance

Organizational changes include changes in mission, functions, or business processes supported by the control system. The organization communicates the changes to appropriate organizational elements responsible for related plans.

2.12.6.3 Requirement Enhancements

None

2.12.6.4 References

NIST SP 800-53r3	CP-2
API 1164r2	3.4, Annex A
NRC RG 5.71	App. C.9.3, App. C.9.7

2.12.7 Incident Handling

2.12.7.1 Requirement

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
2. Coordinates incident handling activities with contingency planning activities

3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures and implements the procedures accordingly.

2.12.7.2 Supplemental Guidance

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Incidents need to be analyzed in light of trends and recorded so they can be used for subsequent trend analyses.

2.12.7.3 Requirement Enhancements

The organization employs automated mechanisms to administer and support the incident handling process.

2.12.7.4 References

NIST SP 800-53r3	IR-4
CAG	CC-16, CC-18
API 1164r2	3.5, Annex A, Annex B.2.1.3.5
NERC CIPS	CIP 008-3 B.R1.2
NRC RG 5.71	App. C.8.4

2.12.8 Incident Monitoring

2.12.8.1 Requirement

The organization tracks and documents control system network security incidents on an ongoing basis.

2.12.8.2 Supplemental Guidance

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

2.12.8.3 Requirement Enhancements

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

2.12.8.4 References

NIST SP 800-53r3	IR-5
CAG	CC-18
API 1164r2	3.5, Annex B.2.1.3.5
NERC CIPS	CIP 008-3 B.R1.2
NRC RG 5.71	App. C.8.5

2.12.9 Incident Reporting

2.12.9.1 Requirement

The organization promptly reports cyber and system security incident information to designated authorities.

2.12.9.2 Supplemental Guidance

The organization develops guidance to determine what is a reportable incident and the granularity of the information reported (e.g., aggregation of common malicious activity) and who to report to (e.g., management, IT security, process safety, control systems engineering, law enforcement agencies). Reporting documents include the details of the incident, the lessons learned, and the course of action to prevent it from occurring again. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, directives, policies, regulations, standards, and guidance. In addition to incident information, weaknesses and vulnerabilities in the control system need to be reported to appropriate organizational officials in a timely manner to prevent security incidents. Each organization establishes reporting criteria, to include sharing information through appropriate channels. Current federal policy requires that organizational officials report security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within specified timeframes designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. The US-CERT phone number is 1-888-282-0870.

A sister organization, the Industrial Control System Computer Emergency Response Team (ICS-CERT) at http://www.us-cert.gov/control_systems/ics-cert/ provides free assistance specifically for ICS issues. This is a manned 24-hour center designed to receive and transmit ICS Alerts, pertaining to potential adverse cyber effects (malware and 0-day infections). It is equipped with trained specialists to assist ICS users in determining whether they are experiencing a system upset or potential malware infection effects. The phone number for this watch floor is 1-877-776-7585.

2.12.9.3 Requirement Enhancements

The organization employs automated mechanisms to assist in the reporting of security incidents. The Einstein network monitoring device from DHS is an example of an automated mechanism.

2.12.9.4 References

NIST SP 800-53r3	IR-6
CAG	CC-18
API 1164r2	3.5
NERC CIPS	CIP 008-3 B.R1.3
NRC RG 5.71	App. C.8.5

2.12.10 Incident Response Assistance

2.12.10.1 Requirement

The organization provides an incident response support resource that offers advice and assistance to users of the control system for the handling and reporting of security incidents.

2.12.10.2 Supplemental Guidance

Possible implementations of incident response support resources in an organization include a help desk and/or an assistance group and access to forensics services when required. The incident response procedures allow for an effective response to any attack on the control system up to and including assigning qualified personnel to manipulate manually control system functions if necessary.

The ICS-CERT at http://www.us-cert.gov/control_systems/ics-cert/ provides free assistance specifically for ICS issues. This is a manned 24-hour center designed to receive and transmit ICS Alerts, pertaining to potential adverse cyber effects (malware and 0-day infections). It is equipped with trained specialists to assist ICS users in determining whether they are experiencing a system upset or potential malware infection effects. This assistance can be in the form of support for incident response and forensic analysis. The phone number for this watch floor is 1-877-776-7585.

2.12.10.3 Requirement Enhancements

1. The organization employs automated mechanisms to increase the availability of incident response-related information and support.

   Enhanced Supplemental Guidance—Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to websites to query the assistance capability, or the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

2. The organization:

   a. Establishes a direct, coorperative relationship between its incident response capability and external providers of information system protection capability

   Identifies organizational incident response team members to the external providers.

   Enhanced Supplemental Guidance—External providers of information system protection capability include the Computer Network Defense program within the US Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

2.12.10.4 References

NIST SP 800-53r3	IR-7
NRC RG 5.71	App. C.8.7

2.12.11 Incident Response Plan

2.12.11.1 Requirement

The organization:

1. Develops an incident response plan that

   a. Provides the organization with a roadmap for implementing its incident response capability

   b. Describes the structure and organization of the incident response capability

   c. Provides a high-level approach for how the incident response capability fits into the overall organization

   d. Meets the unique requirements of the organization with respect to mission, function, size, and structure

   e. Defines reportable incidents

   f. Provides metrics for measuring the incident response capability within the organization

2. Distributes copies of the incident response plan to identified active incident response personnel

2. Reviews the incident response plan on a periodic frequency for relevance, changes to configuration and processes and the result of incident plan test exercises

3. Revises the incident response plan to address system/organizational/operational changes or problems encountered during plan implementation, execution, or testing

4. Communicates incident response plan changes to identified active incident response personnel.

2.12.11.2 Supplemental Guidance

The organization should have a formal, focused, and coordinated approach to responding to incidents. The time to develop an incident response investigation and analysis plans, either internally or externally, is not during such incidents, but beforehand, where calm, calculated actions and responses can be developed and tested for effectiveness. These investigations should consider incidents based on the potential outcome as well as the actual outcome, recognizing that the cyber incident may include intentional and unintentional incidents. Immediate response that is not well thought-out has the potential to be more harmful than no alternative action.

2.12.11.3 Requirement Enhancements

1. The organization develops, tests, deploys, and fully documents an incident response investigation and analysis process.
2. The program specifies roles and responsibilities with respect to local law enforcement and/or other critical stakeholders in an internal and shared incident response investigation and analysis program.

2.12.11.4 References

NIST SP 800-53r3	IR-8
API 1164r2	3.5, Annex A
NERC CIPS	CIP 008-3
NRC RG 5.71	App. C.8.8

2.12.12 Corrective Action

2.12.12.1 Requirement

The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cybersecurity incident are fully implemented.

2.12.12.2 Supplemental Guidance

The organization reviews investigation results and determines corrective actions needed to ensure that similar events do not happen again. The organization encourages and promotes cross-industry incident information exchange and cooperation to learn from the experiences of others.

2.12.12.3 Requirement Enhancements

None

2.12.12.4 References

NIST SP 800-53r3	CP-4, IR-4
API 1164r2	3.5, Annex A
NERC CIPS	CIP 008-3 C, M1
NRC RG 5.71	C2, App. C.3.2, App. C.3.9, App. C.3.11, App. C.8.1, App. C.13.3

2.12.13 Alternate Storage Sites

2.12.13.1 Requirement

The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of control system configuration information.

2.12.13.2 Supplemental Guidance

The frequency of control system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization’s recovery time objectives and recovery point objectives.

2.12.13.3 Requirement Enhancements

1. The organization identifies potential accessibility problems at the alternative storage site in the event of an areawide disruption or disaster and outlines explicit mitigation actions.
2. The organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards.
3. The organization configures the alternate storage site to facilitate timely and effective recovery operations.

2.12.13.4 References

NIST SP 800-53r3	CP-6
API 1164r2	3.4, Annex A, Annex B.2.1.3.5
NRC RG 5.71	App. B.1.22

2.12.14 Alternate Command/Control Methods

2.12.14.1 Requirement

The organization identifies alternate command/control methods for the control system and initiates necessary agreements to permit the resumption of operations for the safe operation of the control system within an organization-defined time period when the primary system capabilities are unavailable.

2.12.14.2 Supplemental Guidance

Alternate command/control methods required to resume operations within the organization-defined time period are either available at alternate organization sites or contracts with vendors need to be in place to support alternate command/control methods for the control system. Timeframes to resume system operations need to be consistent with organization-established recovery time objectives.

2.12.14.3 Requirement Enhancements

1. Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization’s availability requirements.
2. Alternate telecommunications services do not share a single point of failure with primary telecommunications services.
3. Alternate telecommunications service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards.
4. Primary and alternate telecommunications service providers need to have adequate contingency plans.

2.12.14.4 References

NIST SP 800-53r3	CP-4, CP-8
API 1164r2	3.4, Annex A, Annex B.2.1.3.5
NRC RG 5.71	C.3.3, App. B.1.22, App. B.4.5

2.12.15 Alternate Control Center

2.12.15.1 Requirement

The organization identifies an alternate control center, necessary telecommunications, and initiates necessary agreements to permit the resumption of control system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable.

2.12.15.2 Supplemental Guidance

Equipment, telecommunications, and supplies required to resume operations within the organization-prescribed time period need to be available at the alternative control center or by a contract in place to support delivery to the site.

2.12.15.3 Requirement Enhancements

1. The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards.
2. The organization identifies potential accessibility problems to the alternate control center in the event of an areawide disruption or disaster and outlines explicit mitigation actions.
3. The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.
4. The organization fully configures the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability.
5. The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

2.12.15.4 References

NIST SP 800-53r3	CP-7
API 1164r2	3.4, Annex A
NERC CIPS	CIP 002-3 B.R1.2.1, CIP 002-3 R3
NRC RG 5.71	App. B.1.22

2.12.16 Control System Backup

2.12.16.1 Requirement

The organization:

1. Conducts backups of user-level information contained in the system on an organization-defined frequency
2. Conducts backups of system-level information (including system state information) contained in the system on an organization-defined frequency
3. Protects the confidentiality and integrity of backup information at the storage location.

2.12.16.2 Supplemental Guidance

The frequency of system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the recovery time and recovery point objectives for the organization. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of system backups. Protecting backup information from unauthorized disclosure also is an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control.

2.12.16.3 Requirement Enhancements

1. The organization tests backup information periodically to verify media reliability and information integrity.
2. The organization selectively uses backup information in the restoration of control system functions as part of contingency plan testing.
3. The organization stores backup copies of the operating system and other critical control system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

2.12.16.4 References

NIST SP 800-53r3	CP-9
CAG	CC-19
API 1164r2	3.4, Annex A, Annex B.3.1.1.1
NERC CIPS	CIP 008-3 B.R4
NRC RG 5.71	App. C.8.1, App. C.9.5, App. C.9.6

2.12.17 Control System Recovery and Reconstitution

2.12.17.1 Requirement

The organization provides the capability to recover and reconstitute the system to a known secure state after a disruption, compromise, or failure.

2.12.17.2 Supplemental Guidance

System recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. The recovery and reconstitution capability employed by the organization can be a combination of automated mechanisms and manual procedures.

2.12.17.3 Requirement Enhancements

1. The organization implements transaction recovery for systems that are transaction-based (e.g., database management systems).
2. The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state.
3. The organization provides the capability to re-image system components in accordance with organization defined restoration time periods from configuration controlled and integrity protected disk images representing a secure, operational state for the components.

2.12.17.4 References

NIST SP 800-53r3	CP-10
CAG	CC-19
API 1164r2	3.4, Annex A

NERC CIPS	CIP 009-3 B.R1 through R5
NRC RG 5.71	App. C.9.3, App. C.9.7

2.12.18 Fail-Safe Response

2.12.18.1 Requirement

The system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with the system or the loss of the control system itself.

2.12.18.2 Supplemental Guidance

In the event of a loss of communication between the system and the operational facilities, the onsite instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric industry, this may be to alert the operator of the failure and then do nothing (e.g., let the electric grid continue to operate). For the chemical or manufacturing industry, the fail-safe process may be to alert the operator but then safely shut down the process. For the natural gas industry, this may be to maintain the last operational setting before communication failure. The organization defines what “loss of communications” means (i.e., 5 seconds or 5 minutes without communications). The organization then defines the appropriate fail-safe process for its industry.

2.12.18.3 Requirement Enhancements

The system preserves the organization-defined system state information in failure.

2.12.18.4 References

API 1164r2	8.1

2.13 Media Protection

The security controls under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for labeling media for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media.

Media assets include CDs; DVDs; erasable, programmable read-only memory; tapes; printed reports; and documents. Physical security controls need to address specific requirements for the safe maintenance of these assets and provide specific guidance for transporting, handling, and destroying these assets. Security requirements could include safe storage from fire, theft, unintentional distribution, or environmental damage. If an attacker gains access to unencrypted system backup media associated with a control system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an attacker to run password-cracking tools and extract usable passwords. In addition, the backups typically contain machine names, Internet Protocol (IP) addresses, software version numbers, usernames, and other data useful in planning an attack. The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media on any node that is part of, or connected to, the control system should not be allowed.

2.13.1 Media Protection Policy and Procedures

2.13.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

2.13.1.2 Supplemental Guidance

The media protection policy and procedures need to be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular control system when required.

2.13.1.3 Requirement Enhancements

None

2.13.1.4 References

NIST SP 800-53r3	MP-1
API 1164r2	Annex A
NERC CIPS	CIP 003-3 B.R4, CIP 009-3 B.R5, CIP 007-3 B.R7
NRC RG 5.71	App. B.3.1

2.13.2 Media Access

2.13.2.1 Requirement

The organization ensures that only authorized users have access to information in printed form or on digital media, whether integral to or removed from the control system.

2.13.2.2 Supplemental Guidance

The organization implements stringent access and authentication techniques for portable storage media to ensure the validity of connection. The security measures allow organizations to protect data files against unauthorized internal or semi-internal access.

System media include both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, and DVDs) and nondigital media (e.g., paper, microfilm). This requirement also applies to portable and mobile computing and communications device with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

2.13.2.3 Requirement Enhancements

The organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted. Note: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media are stored.

2.13.2.4 References

NIST SP 800-53r3	MP-2
CAG	CC-15
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R7
NRC RG 5.71	App. C.1.2

2.13.3 Media Classification

2.13.3.1 Requirement

The organization reviews and classifies all removable information storage media and the control system output to determine distribution limitations (public, confidential, or classified).

2.13.3.2 Supplemental Guidance

The organization reviews and classifies all removable information storage media using written and approved classification guides. The classification applied to the information storage indicates the level of sensitivity of the information contained on the media.

2.13.3.3 Requirement Enhancements

None

2.13.3.4 References

NIST SP 800-53r3	MP-3
CAG	CC-9
API 1164r2	6, Annex A
NERC CIPS	CIP 003-3 B.R4.2
NRC RG 5.71	App. B.1.13, App. C.1.3

2.13.4 Media Marking

2.13.4.1 Requirement

The organization:

1. Marks, in accordance with organizational policies and procedures, removable system media and system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information
2. Exempts an organization-defined list of media types or hardware components from marking as long as the exempted items remain within the organization-defined protected environment.

2.13.4.2 Supplemental Guidance

The term marking is distinguished from the term labeling. Marking is used in security controls when referring to information that is human-readable. The term labeling is used in the context of marking internal data structures within the system for access control purposes for information in process, in storage, or in transit. Removable system media include both digital media (e.g., magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs, diskettes) and nondigital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, marking is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

2.13.4.3 Requirement Enhancements

The system marks output on external media including video display devices, to identify any of the organization-identified set of special dissemination, handling, or distribution instructions that apply to system output using organization-identified human readable, standard naming conventions. Note: System markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the system). External markings are distinguished from internal markings (i.e., the labels used on internal data structures within the system). Video display devices include computer terminals, monitors, screens on notebook computers, and personal digital assistants.

2.13.4.4 References

NIST SP 800-53r3	MP-3
CAG	CC-9
API 1164r2	Annex A
NRC RG 5.71	App. B.1.13, App. C.1.3

2.13.5 Media Storage

2.13.5.1 Requirement

The organization physically manages and securely stores control system media within protected areas. The sensitivity of the material delineates how the media are stored.

2.13.5.2 Supplemental Guidance

System media include both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and nondigital media (e.g., paper, microfilm). This control applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered systems and may have the capability to store information on internal media (e.g., on voicemail systems). Because telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, the physical access controls to the facility where the media reside provide adequate protection. The organization protects system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

2.13.5.3 Requirement Enhancements

None

2.13.5.4 References

NIST SP 800-53r3	MP-4
CAG	CC-15

API 1164r2	Annex A
NERC CIPS	CIP 009-3 B.R4
NRC RG 5.71	App. C.1.4

2.13.6 Media Transport

2.13.6.1 Requirement

The organization:

1. Protects organization-defined types of digital and nondigital media during transport outside controlled areas using organization-defined security measures
2. Maintains accountability for system media during transport outside controlled areas

3 Restricts the activities associated with transport of such media to authorized personnel.

2.13.6.2 Supplemental Guidance

System media include both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, CDs, DVDs) and nondigital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside controlled areas. Telephone systems also are considered systems and may have the capability to store information on internal media (e.g., on voicemail systems). Because telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other systems, organizational personnel exercise caution in the types of information stored on telephone voicemail systems that are transported outside controlled areas. A controlled area is any space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and system.

Physical and technical security measures for the protection of digital and nondigital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and nondigital media during transport. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms used. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of storage containers for transporting nondigital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

2.13.6.3 Requirement Enhancements

1. The organization documents activities associated with the transport of system media using organization-defined system of records. Note: Organizations establish documentation requirements for activities associated with the transport of system media in accordance with the organizational assessment of risk.
2. The organization employs an identified custodian throughout the transport of system media. Note: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

3. In situations where the ICS cannot support cryptographic mechanisms, the organization employs compensating controls.

2.13.6.4 References

NIST SP 800-53r3	MP-5
NRC RG 5.71	App. C.1.5

2.13.7 Media Sanitization and Disposal

2.13.7.1 Requirement

The organization sanitizes system digital and nondigital media, before disposal or release for reuse.

2.13.7.2 Supplemental Guidance

This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from system media such that reasonable assurance exists, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media are reused or disposed of. The organization employs sanitization mechanisms with strength and integrity commensurate with the security category of the information. FIPS 199 provides standards and guidance on security categories of information and systems. The organization uses its discretion on the use of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

2.13.7.3 Requirement Enhancements

1. The organization tracks, documents, and verifies media sanitization and disposal actions.
2. The organization periodically tests sanitization equipment and procedures to verify correct performance.

2.13.7.4 References

NIST SP 800-53r3	MP-6
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R7
NRC RG 5.71	App. C.1.6

2.14 System and Information Integrity

Maintaining a control system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security controls described under the system and information integrity family provide policy and procedure for identifying, reporting, and correcting control system flaws. Controls exist for malicious code detection, spam protection, and tools and techniques. Also provided are controls for receiving security alerts and advisories and the verification of security functions on the control system. In addition, controls within this family detect and protect against unauthorized changes to software and data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

2.14.1 System and Information Integrity Policy and Procedures

2.14.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. Formal, documented, system and control integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

2.14.1.2 Supplemental Guidance

The organization ensures the system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general control security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular control system when required.

2.14.1.3 Requirement Enhancements

None

2.14.1.4 References

NIST SP 800-53r3	SI-1
NERC CIPS	CIP 007-3 A, B, C, D
NRC RG 5.71	App. C.3.1

2.14.2 Flaw Remediation

2.14.2.1 Requirement

The organization:

1. Identifies, reports, and corrects system flaws
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational systems before installation
3. Incorporates flaw remediation into the organizational configuration management process as an emergency change.

2.14.2.2 Supplemental Guidance

The organization identifies control systems containing software affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Proprietary software can be found either in commercial/government off-the-shelf component products or in custom-developed applications. The organization (or the software developer/vendor for software developed and maintained by a vendor/contractor) promptly evaluates newly released security-relevant patches, service packs, and hot fixes and tests them for effectiveness and potential impacts on the organization's control system before installation. Flaws discovered during security assessments, continual monitoring, or under incident response activities also need to be addressed expeditiously. It is generally not recommended to shut down and restart control system components when an anomaly is identified.

2.14.2.3 Requirement Enhancements

1. The organization centrally manages the flaw remediation process and installs updates automatically. Organizations consider the risk of employing automated flaw remediation processes on a control system.
2. The organization employs automated mechanisms to determine periodically and on demand the state of system components with regard to flaw remediation.
3. The organization measures the time between flaw identification and flaw remediation, comparing with organization-defined benchmarks.
4. The organization employs automated patch management tools to facilitate flaw remediation to organization-defined system components.
5. The use of automated flaw remediation processes must not degrade the operational performance of the control system.

2.14.2.4 References

NIST SP 800-53r3	SI-2
API 1164r2	3.7, 7.2, Annex B.3
NERC CIPS	CIP 007-3 B.R1
NRC RG 5.71	App. C.3.2

2.14.3 Malicious Code Protection

2.14.3.1 Requirement

The organization:

1. Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means or (b) inserted through the exploitation of system vulnerabilities
2. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures
3. Configures malicious code protection mechanisms to: (a) perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed and (b) disinfect and quarantine infected files
4. Considers using malicious code protection software products from multiple vendors as part of defense-in-depth
5. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

2.14.3.2 Supplemental Guidance

The organization employs malicious code protection mechanisms at critical control system entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware). The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the control system.

Updates are scheduled to occur during planned control system outages. The organization considers control system vendor recommendations for malicious code protection. To reduce malicious code, organizations remove the functions and services that should not be employed on the control system (e.g., VoIP, Instant Messaging, file transfer protocol, HTTP, electronic mail, file sharing).

2.14.3.3 Requirement Enhancements

1. The organization centrally manages malicious code protection mechanisms.
2. The system automatically updates malicious code protection mechanisms (including signature definitions).
3. The system prevents users from circumventing host-based malicious code protection capabilities.
4. The system updates malicious code protection mechanisms only when directed by a privileged user.
5. The organization does not allow users to introduce removable media into the system.
6. The system implements malicious code protection mechanisms to identify data containing malicious code and responds accordingly (i.e., block, quarantine, send alert to administrator) when the system encounters data not explicitly allowed by the security policy.
7. The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the system.

2.14.3.4 References

NIST SP 800-53r3	SI-3
CAG	CC-2, CC-4, CC-5, CC-7, CC-10, CC-12, CC-13, CC-15, CC-16, CC-17
API 1164r2	5.7, 5.8, 5.8, Annex B.3.1.2
NERC CIPS	CIP 007-3 B.R4, R4.1, R4.2
NRC RG 5.71	App. B.1.16, App. B.1.20, App. B.3.11, App. B.5.2, App. C.3.3

2.14.4 System Monitoring Tools and Techniques

2.14.4.1 Requirement

The organization:

1. Monitors events on the system
2. Detects system attacks
3. Identifies unauthorized use of the system
4. Deploys monitoring devices (a) strategically within the system to collect organization-determined essential information and (b) at ad hoc locations within the system to track specific types of transactions of interest to the organization
5. Heightens the level of system monitoring activity whenever an indication of increased risk exists to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information
6. Consults legal counsel with regard to system monitoring activities.

2.14.4.2 Supplemental Guidance

Control system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools). It is paramount that the use of monitoring tools and techniques does not adversely impact the operation performance of the ICS. Monitoring devices can be strategically deployed within the control system (e.g., at selected perimeter locations and/or near server farms supporting critical applications) to collect essential information. Monitoring devices also can be deployed at ad hoc locations within the system to track specific transactions. In addition, these devices can be used to track the impact of security changes to the control system. The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the control system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is HTTP traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Organizations need to consult with appropriate legal counsel with regard to all system monitoring activities. The level of system monitoring activity is heightened by organizations whenever an indication of increased risk exists to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

2.14.4.3 Requirement Enhancements

1. The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.
2. In situations where the ICS cannot support the use of automated tools to support near real-time analysis of events, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.
3. The organization employs automated tools to support near real-time analysis of events.
4. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
5. The control system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions include the presence of malicious code, the unauthorized export of information, or signaling to an external control system.
6. The control system provides a real-time alert when indications of compromise or potential compromise occur.
7. The system prevents users from circumventing host-based intrusion detection and prevention capabilities.
8. In situations where the ICS cannot prevent nonprivileged users from circumventing intrusion detection and prevention capabilities, the organization employs appropriate compensating controls (e.g., enhanced auditing) in accordance with the general tailoring guidance.
9. The system notifies a defined list of incident response personnel of suspicious events and takes a defined list of least disruptive actions to terminate suspicious events. Note: The least disruptive actions may include initiating request for human response.
10. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.
11. The organization tests/exercises intrusion monitoring tools on a defined time-period. Note: The frequency of tests/exercises is dependent on the type and method of deployment of the intrusion monitoring tools.

12. The organization makes provisions so that encrypted traffic is visible to system monitoring tools. Note: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount, for others the mission assurance concerns are greater.

13. The system analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. Note: Anomalies within the system include large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

14. The use of monitoring tools and techniques must not adversely impact the operational performance of the control system.

2.14.4.4 References

NIST SP 800-53r3	SI-4
CAG	CC-5, CC-6, CC-14, CC-15
API 1164r2	3.5, Annex B.0, Annex B.3.1.2
NERC CIPS	CIP 007-3 B.R4, R6
NRC RG 5.71	App. B.1.17, App. B.5.2, App. C.3.4

2.14.5 Security Alerts and Advisories and Directives

2.14.5.1 Requirement

The organization:

1. Receives system security alerts, advisories, and directives from designated external organizations on an ongoing basis
2. Generates internal security alerts, advisories, and directives as deemed necessary
3. Disseminates security alerts, advisories, and directives to an organization-defined list of personnel
4. Implements security directives in accordance with timeframes established by the directives, or notifies the issuing organization of the degree of noncompliance. Shutting down and restarting the ICS on the identification of an anomaly are not recommended because the event logs can be erased.

2.14.5.2 Supplemental Guidance

The US-CERT generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential because of the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the nation should the directives not be implemented in a timely manner. Preplanned segmentation and limited operational plans should be enacted to maximize operational availability if immediate untested compliance represents a greater detrimental threat to the ICS.

2.14.5.3 Requirement Enhancements

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

2.14.5.4 References

NIST SP 800-53r3	SI-5

API 1164r2	Annex B.5.1.1.5
NERC CIPS	CIP 007-3 B.R4, R6
NRC RG 5.71	App. C.3.5

2.14.6 Security Functionality Verification

2.14.6.1 Requirement

The organization verifies the correct operation of security functions within the control system upon system startup and restart, upon command by user with appropriate privilege, periodically, and at defined time periods. The control system notifies the system administrator when anomalies are discovered.

2.14.6.2 Supplemental Guidance

The need to verify security functionality applies to all security functions. For security functions that are not able to execute automated self-tests, the organization either implements compensating security measures or explicitly accepts the risk of not performing the verification as required. Generally, the control system resources should not be shut down and restarted upon the identification of an anomaly.

2.14.6.3 Requirement Enhancements

1. The organization employs automated mechanisms to provide notification of failed automated security tests.
2. The organization employs automated mechanisms to support management of distributed security testing.

2.14.6.4 References

NIST SP 800-53r3	SI-6
API 1164r2	7.2, Annex B.4.1.2
NERC CIPS	CIP 007-3 B.R4, R6
NRC RG 5.71	App. B.3.2, App. B.4.9

2.14.7 Software and Information Integrity

2.14.7.1 Requirement

The system monitors and detects unauthorized changes to software and information.

2.14.7.2 Supplemental Guidance

The organization employs integrity verification techniques on the system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial-off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to monitor automatically the integrity of the IT systems, control systems, and the applications it hosts. The organization uses automated tools with extreme caution on designated high-availability systems.

2.14.7.3 Requirement Enhancements

1. The organization reassesses the integrity of software and information by performing on an organization-defined frequency integrity scans of the system and uses the scans with extreme caution on designated high-availability systems.
2. The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification and uses automated tools with extreme caution on designated high-availability systems.

3. The organization employs centrally managed integrity verification tools and uses such tools with extreme caution on designated high-availability systems.

4. The organization requires use of tamper-evident packaging for organization-defined system components during transportation from vendor to operational site, during operation, or both.

2.14.7.4 References

NIST SP 800-53r3	SI-7
CAG	CC-3
API 1164r2	3.6, 7.2.2.2, Annex A
NRC RG 5.71	App. B.1.16, App. B.3.2

2.14.8 Spam Protection

2.14.8.1 Requirement

The organization:

1. Employs spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means
2. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures
3. Considers using spam protection software products from multiple vendors as part of defense-in-depth.

2.14.8.2 Supplemental Guidance

The organization employs spam protection mechanisms at critical control system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, and mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet access, or other common means. The organization considers using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another for workstations).

The organization removes unused and unnecessary functions and services (e.g., electronic mail, Internet access). Because of differing operational characteristics between control system and general IT systems, control systems do not generally employ spam protection mechanisms. Unusual traffic flow, such as during crisis situations, may be misinterpreted and caught as spam, which can cause issues with the system and possible failure of the system.

2.14.8.3 Requirement Enhancements

1. The organization centrally manages spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on a control system. The use of mechanisms to centrally managed spam protection must not degrade the operational performance of the system.

2. The control system automatically updates spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on designated high-availability systems. The use of mechanisms to centrally managed spam protection must not degrade the operational performance of the system.

2.14.8.4 References

NIST SP 800-53r3	SI-8

API 1164r2	7.2.2.1, 7.3.7
NERC CIPS	CIP 007-3 B.R4
NRC RG 5.71	App. C.3.3

2.14.9 Information Input Restrictions

2.14.9.1 Requirement

The organization implements security measures to restrict information input to the control system to authorized personnel only.

2.14.9.2 Supplemental Guidance

Restrictions on personnel authorized to input information to the control system may extend beyond the typical access requirements employed by the system and include limitations based on specific operational or project responsibilities.

2.14.9.3 Requirement Enhancements

None

2.14.9.4 References

NIST SP 800-53r3	SI-9
API 1164r2	6.1, Annex A
NERC CIPS	CIP 003-3 B.R5
NRC RG 5.71	App. C.3.8

2.14.10 Information Input Validation

2.14.10.1 Requirement

The control system checks the validity of information inputs by employing mechanisms to check for accuracy, completeness, validity, and authenticity.

2.14.10.2 Supplemental Guidance

Rules for checking accuracy, completeness, validity, and authenticity of information inputs should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax and semantics of control system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to ensure the content is not unintentionally interpreted as commands. The extent the control system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

2.14.10.3 Requirement Enhancements

None

2.14.10.4 References

NIST SP 800-53r3	SI-10
CAG	CC-7
API 1164r2	5, 8.1, Annex A
NRC RG 5.71	App. B.3.6, App. C.3.8

2.14.11 Error Handling

2.14.11.1 Requirement

The system:

1. Identifies error conditions
2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries
3. Reveals error messages only to authorized personnel
4. Prohibits inclusion of sensitive information in error logs or associated administrative messages.

2.14.11.2 Supplemental Guidance

The structure and content of error messages need to be carefully considered by the organization. Error messages generated by the control system need to provide timely and useful information without providing potentially harmful information that could be exploited by adversaries. System error messages are revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, passwords, and personnel ID numbers) is not to be listed in error logs or associated administrative messages. The extent the control system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

2.14.11.3 Requirement Enhancements

None

2.14.11.4 References

NIST SP 800-53r3	SI-11
API 1164r2	7.2
NRC RG 5.71	App. C.3.9

2.14.12 Information Output Handling and Retention

2.14.12.1 Requirement

The organization handles and retains output from the control system in accordance with applicable laws, regulations, standards, and organizational policy as well as operational requirements of the control process.

2.14.12.2 Supplemental Guidance

The National Archives and Records Administration provides guidance on records retention.

2.14.12.3 Requirement Enhancements

None

2.14.12.4 References

NIST SP 800-53r3	SI-12
API 1164r2	3.1, 6, Annex A
NERC CIPS	CIP 005-3 B.R5 to R5.3
NRC RG 5.71	App. C.3.10

2.14.13 Predictable Failure Prevention

2.14.13.1 Requirement

The organization:

1. Protects the system from harm by considering mean time to failure for an organization-defined list of system components in specific environments of operation
2. Provides substitute system components, when needed, and a mechanism to exchange active and standby roles of the components.

2.14.13.2 Supplemental Guidance

Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry average. The transfer of responsibilities between active and standby system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress, or for maintenance reasons.

2.14.13.3 Requirement Enhancements

1. The organization takes the system component out of service by transferring component responsibilities to a substitute component no later than an organization-defined fraction or percentage of mean time to failure.
2. The organization does not allow a process to execute without supervision for more than an organization-defined time period.
3. The organization manually initiates a transfer between active and standby system components at least once per a defined frequency if the mean time to failure exceeds the defined time period.
4. The organization, if a system component failure is detected, (a) ensures that the standby system component successfully and transparently assumes its role within a defined time period and (b) activates an alarm and/or automatically shuts down the system. Note: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.

2.14.13.4 References

NIST SP 800-53r3	SI-13
API 1164r2	3.4, 6, Annex A, Annex B.3, Annex B.5
NRC RG 5.71	App. B.3.22, App. C.3.11, App. C.9.2

2.15 Access Control

The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need to be in place to monitor access activities for inappropriate activity. The access control lists need to be managed through adding, altering, and removing access rights as necessary.

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a control system. Identification could be a password, a token, or a fingerprint. Authentication is the challenge process to prove (validate) the identification provided. An example would be using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.

2.15.1 Access Control Policy and Procedures

2.15.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

2.15.1.2 Supplemental Guidance

The organization ensures the access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular control system when required.

2.15.1.3 Requirement Enhancements

1. Public access to ICS is not permitted.
2. Business IT and general corporation access to the ICS is not permitted.

2.15.1.4 References

NIST SP 800-53r3	AC-1, SC-14
CAG	CC-9
API 1164r2	4, 5, Annex A
NERC CIPS	CIP 003-3 B.R5, CIP 005-3 B.R2
NRC RG 5.71	C.3.3.1.1, App. B.1.1

2.15.2 Identification and Authentication Policy and Procedures

2.15.2.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

2.15.2.2 Supplemental Guidance

The organization ensures the identification and authentication policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular control system when required.

2.15.2.3 Requirement Enhancements

None

2.15.2.4 References

NIST SP 800-53r3	IA-1

API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R2.5
NRC RG 5.71	App. B.4.1

2.15.3 Account Management

2.15.3.1 Requirement

The organization manages system accounts, including:

1. Identifying account types (i.e., individual, group, and system)
2. Establishing conditions for group membership
3. Identifying authorized users of the system and specifying access rights and privileges
4. Requiring appropriate approvals for requests to establish accounts
5. Authorizing, establishing, activating, modifying, disabling, and removing accounts
6. Reviewing accounts on a defined frequency
7. Specifically authorizing and monitoring the use of guest/anonymous accounts
8. Notifying account managers when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes
9. Granting access to the system based on a valid need-to-know or need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage.

2.15.3.2 Supplemental Guidance

The identification of authorized users of the system and the specification of access rights and privileges are consistent with the requirements in other security controls in the security plan.

2.15.3.3 Requirement Enhancements

1. The organization employs automated mechanisms to support the management of system accounts.
2. The system automatically terminates temporary and emergency accounts after a defined time period for each type of account.
3. The system automatically disables inactive accounts after a defined time period.
4. The system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.
5. The organization reviews currently active system accounts on a defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.
6. The organization prohibits the use of system account identifiers as the identifiers for user electronic mail accounts.

2.15.3.4 References

NIST SP 800-53r3	AC-2
CAG	CC-9, CC-11
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R5

NRC RG 5.71	App. B.1.2

2.15.4 Identifier Management

2.15.4.1 Requirement

The organization manages system identifiers for users and devices by:

1. Receiving authorization from a designated organizational official to assign a user or device identifier
2. Selecting an identifier that uniquely identifies an individual or device
3. Assigning the user identifier to the intended party or the device identifier to the intended device
4. Archiving previous user or device identifiers.

2.15.4.2 Supplemental Guidance

Common device identifiers include Media Access Control (MAC) or IP addresses, or device unique token identifiers. Management of user identifiers is not applicable to shared system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of a system account associated with an individual.

2.15.4.3 Requirement Enhancements

None

2.15.4.4 References

NIST SP 800-53r3	IA-4
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R5
NRC RG 5.71	App. B.4.6

2.15.5 Authenticator Management

2.15.5.1 Requirement

The organization manages system authenticators for users and devices by:

1. Verifying, as part of the initial authenticator distribution for a user authenticator, the identity of the individual receiving the authenticator
2. Establishing initial authenticator content for organization-defined authenticators
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators
5. Changing default content of authenticators upon system installation
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate)
7. Changing or refreshing authenticators periodically, as appropriate for authenticator type
8. Protecting authenticator content from unauthorized disclosure and modification
9. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

2.15.5.2 Supplemental Guidance

Device authenticators include, for example, certificates and passwords. User authenticators include tokens, PKI certificates, biometrics, passwords, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many system components are shipped with factory default user authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation.

The system supports user authenticator management requirements by enforcing organization-defined password minimum and maximum lifetime restrictions and password reuse restrictions for organization-defined number of generations. Measures to safeguard user authenticators includes maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.

2.15.5.3 Requirement Enhancements

1. The system, for PKI-based authentication:
   a. Validates certificates by constructing a certification path with status information to an accepted trust anchor
   b. Enforces authorized access to the corresponding private key
   c. Maps the authenticated identity to the user account. Note: Status information for certification paths includes certificate revocation lists or online certificate status protocol responses.
2. The organization requires that the registration process to receive a user authenticator be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
3. The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
4. The organization requires unique authenticators be provided by vendors and manufacturers of system components.

2.15.5.4 References

NIST SP 800-53r3	IA-5
CAG	CC-4
API 1164r2	5, 5.5, Annex A
NERC CIPS	CIP 005-3 B.R5
NRC RG 5.71	App. B.4.7

2.15.6 Account Review

2.15.6.1 Requirement

The organization:

1. Reviews and analyzes system audit records on an organization-defined frequency for indications of inappropriate or unusual activity, and report findings to designated organizational officials
2. Adjusts the level of audit review, analysis, and reporting within the system when a change in risk exists to organizational operations, organizational assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

2.15.6.2 Supplemental Guidance

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual control system-related activities and periodically reviews changes to access authorizations. The organization reviews the activities of users with significant roles and responsibilities for the control system more frequently. The extent of the audit record reviews is based on the impact level of the control system. For example, for low-impact systems, security logs are not intended to be reviewed frequently for every workstation but rather at central points, such as a web proxy or e-mail servers, and when specific circumstances warrant review of other audit records.

2.15.6.3 Requirement Enhancements

1. The system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.
2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
3. The system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system. Note: An example of an automated mechanism for centralized review and analysis is a Security Information Management product.
4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to enhance further the ability to identify inappropriate or unusual activity.

2.15.6.4 References

NIST SP 800-53r3	AC-2, AU-6
CAG	CC-6, CC-9, CC-11
API 1164r2	5, Annex A, Annex B.4
NERC CIPS	CIP 005-3 B.R5
NRC RG 5.71	App. B.1.2, App. B.1.11, App. B.2.6

2.15.7 Access Enforcement

2.15.7.1 Requirement

The control system enforces assigned authorizations for controlling logical access to the system in accordance with applicable policy.

2.15.7.2 Supplemental Guidance

Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrixes, and cryptography) are employed by organizations to control access to the control system. The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.

In addition to enforcing authorized access at the system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased security for the organization. Consideration is given to the implementation of an audited, manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

2.15.7.3 Requirement Enhancements

1. The system enforces dual authorization, based on organizational policies and procedures for organization-defined privileged commands. Note: The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.

2. The system enforces one or more organization-defined nondiscretionary access control policies over organization-defined set of users and resources where the policy rule set for each policy specifies:

   a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day)

   b. Required relationships among the access control information to permit access. Note: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, and Originator Controlled Access Control.

3. The system prevents access to organization-defined security-relevant information except during secure, nonoperable system states. Note: Security relevant information is any information within the system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Secure, nonoperable system states are states in which the system is not performing mission/business-related processing (e.g., the system is offline for maintenance, troubleshooting, bootup, shutdown).

2.15.7.4 References

NIST SP 800-53r3	AC-3
CAG	CC-9, CC-11
API 1164r2	5.10, Annex A
NERC CIPS	CIP 003-3 B.R5
NRC RG 5.71	App. B.1.3

2.15.8 Separation of Duties

2.15.8.1 Requirement

The organization:

1. Establishes division of responsibilities and separates duties of individuals as necessary to eliminate conflicts of interest

2. Implements separation of duties through assigned system access authorizations.

2.15.8.2 Supplemental Guidance

Separation of duties prevents users from having the system access necessary to perform malevolent activity without collusion. Examples of separation of duties include (1) mission functions and distinct system support functions are divided among different individuals and roles; (2) different individuals perform system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security);and (3) security personnel who administer access control functions do not administer audit functions.

In situations where the ICS cannot support the differentiation of roles, the organization employs appropriate compensating controls. The organization carefully considers the appropriateness of single individuals or single groups performing multiple critical roles.

2.15.8.3 Requirement Enhancements

None

2.15.8.4 References

NIST SP 800-53r3	AC-5
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R5.2
NRC RG 5.71	App. B.1.5

2.15.9 Least Privilege

2.15.9.1 Requirement

The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users), as necessary, to accomplish assigned tasks.

2.15.9.2 Supplemental Guidance

The organization employs the concept of least privilege for specific duties and the control system (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

In situations where the ICS cannot support the differentiation of privileges, the organization employs appropriate compensating controls. The organization carefully considers the appropriateness of single individuals or single groups having multiple critical privileges.

2.15.9.3 Requirement Enhancements

1. The organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information. Note: Explicitly authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
2. The organization requires that users of system accounts with access to organization-defined list of security functions or security-relevant information, use nonprivileged accounts when accessing other system functions, and if feasible, audits any use of privileged accounts for such functions.
3. The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the system.

2.15.9.4 References

NIST SP 800-53r3	AC-6
CAG	CC-8, CC-9
API 1164r2	Annex A
NERC CIPS	CIP 003-3 B.R5, R5.2
NRC RG 5.71	App. B.1.6, App. B.5.3

2.15.10 User Identification and Authentication

2.15.10.1 Requirement

The system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

2.15.10.2 Supplemental Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization. Authentication of user identities is accomplished by passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Organizational users include employees and contractors. Access to organizational systems is defined as either local or network. Local access is any access to an organizational system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational system by a user (or process acting on behalf of a user) where such access is obtained across a network connection. Remote access is a type of network access which involves communication through an external, nonorganization-controlled network (e.g., the Internet). Organization-controlled networks include local area networks, wide area networks, and virtual private networks that are totally under the control of the organization. Identification and authentication requirements for system access by other than organizational users are described in other controls.

FIPS 201 specifies a PIV credential for use in the unique identification and authentication of federal employees and contractors. The identification and authentication requirements in this control are satisfied by complying with FIPS 201 as required by Homeland Security Presidential Directive (HSPD) 12. The selection of authentication mechanisms specified in FIPS 201 is constrained by whether access to the organizational system is local or network. FIPS 201 (Section 6.3.2) provides information on appropriate authentication mechanisms for local and network accesses to systems. In addition to identifying and authenticating users at the system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased security for the organization.

2.15.10.3 Requirement Enhancements

1. The system employs multifactor authentication for remote access and for access to privileged accounts.
2. The system employs multifactor authentication for network access and for access to privileged accounts.
3. The system employs multifactor authentication for local and network access.

2.15.10.4 References

NIST SP 800-53r3	IA-2, IA-8
CAG	CC-4, CC-5
API 1164r2	5, Annex A
NERC CIPS	CIP 003-3 B.R5, R5.1, R5.1.1
NRC RG 5.71	App. B.4.2, App. B.4.6

2.15.11 Permitted Actions without Identification or Authentication

2.15.11.1 Requirement

The organization identifies and documents specific user actions, if any, that can be performed on the system without identification or authentication.

2.15.11.2 Supplemental Guidance

The organization may allow limited user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible systems. Organizations should also identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed.

Such bypass may be via a physical switch that is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and authentication have not yet occurred.

2.15.11.3 Requirement Enhancements

The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

2.15.11.4 References

NIST SP 800-53r3	AC-14
NRC RG 5.71	App. B.1.12

2.15.12 Device Identification and Authentication

2.15.12.1 Requirement

The system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.

2.15.12.2 Supplemental Guidance

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The system typically uses either shared known information (e.g., MAC or Transmission Control Protocol/IP [TCP/IP] addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP] or a Radius server with EAP-Transport Layer Security authentication) to identify and authenticate devices on local and wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the system with higher impact levels requiring stronger authentication.

2.15.12.3 Requirement Enhancements

1. The system authenticates devices before establishing remote network connections using bi-directional authentication between devices that are cryptographically based. Note: Remote network connection is any connection with a device communicating through an external, nonorganization-controlled network (e.g., the Internet).
2. The system authenticates devices before establishing network connections using bidirectional authentication between devices that are cryptographically based.

2.15.12.4 References

NIST SP 800-53r3	IA-3
API 1164r2	8.1, Annex B.3.1.4.2
NRC RG 5.71	App. B.4.1, App. B.4.5

2.15.13 Authenticator Feedback

2.15.13.1 Requirement

The authentication mechanisms in the control system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

2.15.13.2 Supplemental Guidance

The control system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the control system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

2.15.13.3 Requirement Enhancements

None

2.15.13.4 References

NIST SP 800-53r3	IA-6
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R3.2
NRC RG 5.71	App. B.4.8

2.15.14 Cryptographic Module Authentication

2.15.14.1 Requirement

The control system employs authentication methods that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

2.15.14.2 Supplemental Guidance

None

2.15.14.3 Requirement Enhancements

Failure of cryptographic module authentication must not create a denial of service or adversely impact the operational performance of the control system.

2.15.14.4 References

NIST SP 800-53r3	IA-7
API 1164r2	8.2.2, Annex A, Annex B.23.1.6
NRC RG 5.71	App. B.4.9

2.15.15 Information Flow Enforcement

2.15.15.1 Requirement

The control system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

2.15.15.2 Supplemental Guidance

Information flow control regulates where information is allowed to travel within a control system and between control systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few general examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within control systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict control system services or provide a packet-filtering capability.

2.15.15.3 Requirement Enhancements

1. The system enforces information flow control using explicit labels on information, source, and destination objects as a basis for flow control decisions. Note: Information flow enforcement mechanisms compare labels on all information (data content and data structure) and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by the information flow policy. Information flow enforcement using explicit labels can be used to control the release of certain types of information.
2. The system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.
3. The system enforces dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations.
4. The system prevents encrypted data from bypassing content-checking mechanisms.
5. The system enforces organization-defined limitations on the embedding of data types within other data types.
6. The system enforces information flow control on metadata.
7. The system enforces organization-defined one-way flows using hardware mechanisms.
8. The system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.
9. The system enforces the use of human review for organization-defined security policy filters when the system is not capable of making an information flow control decision.
10. The system provides the capability for a privileged administrator to enable and disable organization-defined security policy filters.
11. The system provides the capability for a privileged administrator to configure the organization-defined security policy filters to support different security policies.

2.15.15.4 References

NIST SP 800-53r3	AC-4
CAG	CC-4, CC-9, CC-15
API 1164r2	Annex A, Annex B.3.1.3, Annex B.3.1.4
NERC CIPS	CIP 003-3 B.R5

NRC RG 5.71	App. B.1.1, App. B.1.4

2.15.16 Passwords

2.15.16.1 Requirement

The organization develops and enforces policies and procedures for control system users concerning the generation and use of passwords. These policies stipulate rules of complexity, based on the criticality level of the systems to be accessed.

2.15.16.2 Supplemental Guidance

1. Default passwords of applications, operating systems, database management systems, or other programs must be changed immediately after installation.
2. The organization replaces default usernames whenever possible. Passwords need to be allocated, protected, and used based on the criticality level of the systems to be accessed.
3. The organization develops policies that stipulate the complexity (minimum/maximum length, combination of lower/upper case, numerals, special characters, etc.) level of the password for each criticality level. Short or easily guessed passwords are prohibited. Passwords can be a means of system protection when properly generated and used. Although passwords are not advisable in all control system applications, there are some cases where they are of benefit such as for remote access. These passwords are developed to meet defined metrics.
4. Good security practices need to be followed in the generation of passwords. Passwords should not easily be associated with the user or the organization and follow appropriate complexity rules. Initial or default passwords are changed immediately on first login. Following generation, passwords are not sent across any network unless protected by encryption or salted cryptographic hash specifically designed to prevent replay attacks.
5. Passwords need to be transferred to the user via secure media, and the recipient must be verified. The logon ID and password are never combined in the same communication.
6. The authority to keep and change high-level passwords is given to a trusted employee who is available during emergencies.
7. A log for master passwords needs to be maintained separately from the control system, possibly in a notebook in a vault or safe.
8. Passwords need to be changed regularly and expire when the user leaves the organization or after an extended period of inactivity.
9. Users are responsible for their passwords and are instructed not to share them or write them down, and need to be aware of their surroundings when entering passwords. If the operating system supports encryption, stored passwords are encrypted. Passwords are not to be embedded into tools, source code, scripts, aliases, or shortcuts.

2.15.16.3 Requirement Enhancements

ICS deployment will require two-factor authentication or comparable compensating measures to ensure only approved authorized access is allowed. .

2.15.16.4 References

NIST SP 800-53r3	IA-5
CAG	CC-4
API 1164r2	5.5, 8.1, Annex A, Annex B.3.1.4
NERC CIPS	CIP 005-3 B.R4.4

NRC RG 5.71	App. B.4.3, App. B.4.7

2.15.17 System Use Notification

2.15.17.1 Requirement

The system:

1. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states that (a) users are accessing a private or government system; (b) system usage may be monitored, recorded, and subject to audit; (c) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (d) use of the system indicates consent to monitoring and recording
2. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access, the system
3. For publicly accessible systems, (a) displays the system use information, when appropriate, before granting further access; (b) ensures that any references to monitoring, recording, or auditing are consistent with privacy accommodations for such systems that generally prohibit those activities; and (c) includes in the notice given to public users of the system, a description of the authorized uses of the system.

2.15.17.2 Supplemental Guidance

System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the system. System use notification is intended only for system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist.

2.15.17.3 Requirement Enhancement

None

2.15.17.4 References

NIST SP 800-53r3	AC-8
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R3.2
NRC RG 5.71	App. B.1.8

2.15.18 Concurrent Session Control

2.15.18.1 Requirement

The organization limits the number of concurrent sessions for any user on the control system.

2.15.18.2 Supplemental Guidance

The organization may define the maximum number of concurrent sessions for a system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given system account and does not address concurrent sessions by a single user via multiple system accounts.

2.15.18.3 Requirement Enhancements

None

2.15.18.4 References

NIST SP 800-53r3	AC-10
NRC RG 5.71	App. B.4.4

2.15.19 Previous Logon (Access) Notification

2.15.19.1 Requirement

The control system notifies the user, upon successful logon (access), of the date and time of the last logon (access) and the number of unsuccessful logon attempts since the last successful logon.

2.15.19.2 Supplemental Guidance

This control is intended to cover both traditional user logons to ICS systems as well as service-related processes that automatically log on to the ICS.

2.15.19.3 Requirement Enhancements

1. The information system is capable of notifying the user the number of successful logon and access attempts as well as unsuccessful logon and access attempts.
2. The information system is capable of displaying security-related changes to the user's account within an organizational-defined time period.

2.15.19.4 References

NIST SP 800-53r3	AC-9
NRC RG 5.71	App. B.1.9

2.15.20 Unsuccessful Login Attempts

2.15.20.1 Requirement

The system:

1. Enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period
2. Automatically locks the account/node for an organization-defined time period and delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.

2.15.20.2 Supplemental Guidance

Because of the potential for denial of service, automatic lockouts initiated by the system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may choose to employ different algorithms for different system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application level. Permanent automatic lockouts initiated by a control system must be carefully considered before being used because of safety considerations and the potential for denial of service. Operator lockouts for critical and emergency control stations must maintain maximum control. In these cases, compensatory security requirements, such as limited physical access to trusted employees, are used.

2.15.20.3 Requirement Enhancements

The control system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

2.15.20.4 References

NIST SP 800-53r3	AC-7
API 1164r2	5.5
NRC RG 5.71	App. B.1.7

2.15.21 Session Lock

2.15.21.1 Requirement

The system:

1. Prevents further access to the system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user
2. Retains the session lock until the user re-establishes access using appropriate identification and authentication procedures.

2.15.21.2 Supplemental Guidance

A session lock is not a substitute for logging out of the system. Organization-defined time periods of inactivity comply with policy. In some situations, session-lock for ICS operator workstations/nodes is not advisable (e.g., when immediate operator responses are required for emergency situations). In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures).

2.15.21.3 Requirement Enhancements

The system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

2.15.21.4 References

NIST SP 800-53r3	AC-11
API 1164r2	5.4
NRC RG 5.71	App. B.1.10, App. B.4.4

2.15.22 Remote Session Termination

2.15.22.1 Requirement

The system terminates a network connection at the end of a session or after an organization-defined time period of inactivity.

2.15.22.2 Supplemental Guidance

This control applies to both organization-controlled networks and nonorganization-controlled networks. The organization-defined time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses in accordance with an organizational assessment of risk.

2.15.22.3 Requirement Enhancements

Automatic session termination applies to local and remote sessions. The control system terminates a network connection at the end of a session or after a period of inactivity per organization policy and procedures.

2.15.22.4 References

NIST SP 800-53r3	SC-10

API 1164r2	5.4
NRC RG 5.71	App. B.3.11, App. B.4.4

2.15.23 Remote Access Policy and Procedures

2.15.23.1 Requirement

The organization:

1. Documents allowed methods of remote access to the system
2. Establishes usage restrictions and implementation guidance for each allowed remote access method
3. Authorizes remote access to the system prior to connection
4. Enforces requirements for remote connections to the system.

2.15.23.2 Supplemental Guidance

Remote access is any access to an organizational system by a user (or process acting on behalf of a user) communicating through an external, nonorganization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Virtual private network (VPN) when adequately provisioned may be treated as an organization-controlled network. With regard to wireless, radiated signals within organization-controlled facilities typically qualify as outside organizational control. Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Remote access controls are applicable to systems other than public web servers or systems specifically designed for public access.

2.15.23.3 Requirement Enhancements

None

2.15.23.4 References

NIST SP 800-53r3	AC-17
API 1164r2	8.2.4, Annex A
NERC CIPS	CIP 005-3 B.R2
NRC RG 5.71	App. B.3.11

2.15.24 Remote Access

2.15.24.1 Requirement

The organization authorizes, monitors, and manages all methods of remote access to the control system.

2.15.24.2 Supplemental Guidance

The organization documents, monitors, and manages all methods of remote access (e.g., dialup, Internet, physical) to the control system. Appropriate authentication methods are needed to secure adequately remote access.

Remote access is any access to an organizational control system by a user (or a system) communicating through an external, nonorganization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access security requirements are applicable to control systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based on source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).

Remote access to control system component locations (e.g., control center, field locations) is only enabled when necessary, approved, and authenticated. The organization considers multifactor authentication for remote user access to the control system.

2.15.24.3 Requirement Enhancements

1. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.
2. The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. Note: The encryption strength of mechanism is selected based on the FIPS 199 impact level of the information.
3. The system routes all remote accesses through a limited number of managed access control points.
4. The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the system.
5. The system protects wireless access to the system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary.
6. The organization monitors for unauthorized remote connections to the system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered. Note: Organizations proactively search for unauthorized remote connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to those areas within the facility containing the systems. Yet, the scan is conducted outside those areas only as needed to verify that unauthorized wireless access points are not connected to the system.
7. The organization disables, when not intended for use, wireless networking capabilities internally embedded within system components prior to issue.
8. The organization does not allow users to independently configure wireless networking capabilities.
9. The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
10. The organization ensures that remote sessions for accessing an organization-defined list of security functions and security-relevant information employ additional security measures (organization-defined security measures) and are audited.
11. The organization disables peer-to-peer wireless networking capability within the system except for explicitly identified components in support of specific operational requirements.
12. The organization disables Bluetooth wireless networking capability within the system except for explicitly identified components in support of specific operational requirements.

2.15.24.4 References

NIST SP 800-53r3	AC-17
CAG	CC-5, CC-6, CC-8, CC-14
API 1164r2	8.1, 8.2.4, Annex A, Annex B.3.1.4
NERC CIPS	CIP 005-3 B.R4.4
NRC RG 5.71	App. B.1.17, App. B.3.11, App. B.5.3

2.15.25 Access Control for Mobile Devices

2.15.25.1 Requirement

The organization:

1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices
2. Authorizes connection of mobile devices to organizational systems
3. Monitors for unauthorized connections of mobile devices to organizational systems
4. Enforces requirements for the connection of mobile devices to organizational systems
5. Disables system functionality that provides the capability for automatic execution of code on removable media without user direction
6. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures
7. Applies specified measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

2.15.25.2 Supplemental Guidance

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives), portable computing, and communications devices with storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Usage restrictions and implementation guidance related to mobile devices can include configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

In situations where the ICS cannot implement any or all the components of this control, the organization employs other mechanisms or procedures as compensating controls. This may involve physically locking components; specific access logs; and specific monitoring programs for locks, keys, and access logs.

2.15.25.3 Requirement Enhancements

1. The organization restricts the use of writable, removable media in organizational systems.
2. The organization prohibits the use of personally owned, removable media in organizational systems.
3. The organization prohibits the use of removable media in organizational systems when the media have no identifiable owner. Note: An identifiable owner for removable media helps reduce the risk of

employing such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

2.15.25.4 References

NIST SP 800-53r3	AC-19
CAG	CC-6, CC-8
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R2
NRC RG 5.71	App. B.1.19

2.15.26 Wireless Access Restrictions

2.15.26.1 Requirement

The organization:

1. Establishes use restrictions and implementation guidance for wireless technologies
2. Authorizes, monitors, and manages wireless access to the control system.

2.15.26.2 Supplemental Guidance

The organization uses authentication and cryptography or enhanced defense mechanisms to protect wireless access to the control system.

Wireless technologies include, but are not limited to, microwave, satellite, packet radio [UHF/VHF], 802.11x, and Bluetooth.

2.15.26.3 Requirement Enhancements

1. The organization uses authentication and encryption to protect wireless access to the control system. Any latency induced from the use of encryption must not degrade the operational performance of the control system.
2. The organization scans for unauthorized wireless access points at a specified frequency and takes appropriate action if such access points are discovered. Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact control systems. The scan is not limited to only those areas within the facility containing the high-impact control systems.

2.15.26.4 References

NIST SP 800-53r3	AC-17
CAG	CC-4, CC-5, CC-6, CC-8, CC-14
API 1164r2	7.2.2.1, 7.3.8, Annex A, Annex B.1.1.1.1, Annex B.1.1.3, Annex B.3.1.4
NERC CIPS	CIP 005-3 B.R2
NRC RG 5.71	App. B.1.17, App. B.3.11, App. B.5.4

2.15.27 Personally Owned Information

2.15.27.1 Requirement

The organization restricts the use of personally owned information copied to the control system or control system user workstation that is used for official organization business. This includes the processing, storage, or transmission of organization business and critical control system information. The terms and conditions need to address, at a minimum:

1. The types of applications that can be accessed from personally owned IT, either remotely or from within the organization control system
2. The maximum security category of information that can be processed, stored, and transmitted
3. How other users of the personally owned control system will be prevented from accessing organization information
4. The use of VPN and firewall technologies
5. The use of and protection against the vulnerabilities of wireless technologies
6. The maintenance of adequate physical security mechanisms
7. The use of virus and spyware protection software
8. How often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, malware definitions).

2.15.27.2 Supplemental Guidance

The organization establishes strict terms and conditions for the use of personally owned information on control systems and control systems user workstations.

2.15.27.3 Requirement Enhancements

None

2.15.27.4 References

NIST SP 800-53r3	AC-20
CAG	CC-5
API 1164r2	Annex A
NRC RG 5.71	App. B.1.22

2.15.28 External Access Protections

2.15.28.1 Requirement

The organization employs mechanisms in the design and implementation of a control system to restrict public access to the control system from the organization’s enterprise network.

2.15.28.2 Supplemental Guidance

Public access is defined as access from the enterprise system. Care should be taken to ensure data shared with the enterprise system are protected for integrity of the information and applications. Public access to the control system to satisfy business requirements needs to be limited to read only access through the corporate enterprise systems via a demilitarized zone. The organization explicitly allows necessary network protocols in the demilitarized zone; blocks or filters unnecessary protocols, configure firewalls to block inbound connections, limits outbound connections to only those specifically required for operations and eliminates network connections that bypass perimeter protection mechanisms (e.g., firewall, VPN, demilitarized zone).

2.15.28.3 Requirement Enhancements

None

2.15.28.4 References

NIST SP 800-53r3	AC-20, IA-2

CAG	CC-4, CC-5
API 1164r2	7.3, 8, Annex B.3
NERC CIPS	CIP 005-3 B.R1, R2, R3
NRC RG 5.71	App. B.1.18, App. B.1.22, App. B.3.11, App. B.4.6, App. B.5.4

2.15.29 Use of External Information Control Systems

2.15.29.1 Requirement

The organization establishes terms and conditions for authorized individuals to:

1. Access the system from an external system
2. Process, store, and transmit organization-controlled information using an external system.

2.15.29.2 Supplemental Guidance

External systems are systems or components of systems that are outside the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External systems include, but are not limited to, (1) personally owned systems (e.g., computers, cellular telephones, or personal digital assistants), (2) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports), (3) systems owned or controlled by nonfederal governmental organizations, and (4) private or federal systems that are not owned by, operated by, or under the direct supervision and authority of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational system. This control does not apply to the use of external systems to access public interfaces to organizational systems and information. The organization establishes terms and conditions for the use of external systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum (1) the types of applications that can be accessed on the organizational system from the external system and (2) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external system.

2.15.29.3 Requirement Enhancements

1. The organization prohibits authorized individuals from using an external system to access the system or to process, store, or transmit organization-controlled information except in situations where the organization (a) can verify the implementation of required security controls on the external system as specified in the organization’s security policy and security plan or (b) has approved system connection or processing agreements with the organizational entity hosting the external system.
2. The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external systems.

2.15.29.4 References

NIST SP 800-53r3	AC-20
CAG	CC-4, CC-5, CC-13, CC-15, CC-16
API 1164r2	7.3, 8, Annex B.3, Annex B.5
NERC CIPS	CIP 005-3 B.R1, R2, R3
NRC RG 5.71	App. B.1.20, App. B.3.11, App. B.5.4

2.15.30 User-Based Collaboration and Information Sharing

2.15.30.1 Requirement

The organization:

1. Facilitates information sharing by enabling specified authorized users to determine whether access authorization assigned to the end users match allowable access restrictions on information where limited discretion/information access is required
2. Employs automated or manual mechanisms as required to assist authorizing users in making the correct information sharing/collaboration decisions.

2.15.30.2 Supplemental Guidance

This control applies to information that may be restricted (e.g., privileged medical, business, proprietary, personally identifiable information, or special access programs/compartmentalization) based on administrative and/or legal determination. End users may be individuals, groups, or organizations, and the information may be defined by specific content, type, or security categorization.

2.15.30.3 Requirement Enhancements

The information system employs automated mechanisms to enable authorized users to make information sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.

2.15.30.4 References

NIST SP 800-53r3	AC-21
API 1164r2	7.3
NERC CIPS	CIP 008-3 B.R1.3

2.15.31 Publicly Accessible Content

2.15.31.1 Requirement

The organization:

1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information
3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system
4. Reviews the content on the publicly accessible organizational information system for nonpublic information on a routine interval
5. Removes nonpublic information from publicly accessible information systems if discovered.

2.15.31.2 Supplemental Guidance

Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, executive orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information is examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public typically without identification or authentication. The posting of information on nonorganizational information systems is covered by appropriate organizational policy.

2.15.31.3 Requirement Enhancements

None

2.15.31.4 References

NIST SP 800-53r3	AC-22
API 1164r2	6
NRC RG 5.71	App. B.1.23

2.16 Audit and Accountability

Periodic audits and logging of the control system need to be implemented to validate that the security mechanisms present during system validation testing are still installed and operating correctly. These security audits review and examine a system's records and activities to determine the adequacy of system security controls and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of system logs. Logging is necessary for anomaly detection as well as forensic analysis.

2.16.1 Audit and Accountability Policy and Procedures

2.16.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

2.16.1.2 Supplemental Guidance

The organization ensures the audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for a particular control system when required.

2.16.1.3 Requirement Enhancements

None

2.16.1.4 References

NIST SP 800-53r3	AU-1
API 1164r2	1.2, Annex A, Annex B.4, Annex B.5
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.1

2.16.2 Auditable Events

2.16.2.1 Requirement

The organization:

1. Determines, based on a risk assessment in conjunction with mission/business needs, which system-related events require auditing (e.g., an organization-defined list of auditable events and frequency of [or situation requiring] auditing for each identified auditable event)
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
3. Ensures that auditable events are adequate to support after-the-fact investigations of security incidents
4. Adjusts, as necessary, the events to be audited within the system based on current threat information and ongoing assessments of risk.

2.16.2.2 Supplemental Guidance

The purpose of this control is for the organization to identify events that need to be auditable as significant and relevant to the security of the system. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. The checklists and configuration guides at http://web.nvd.nist.gov/view/ncp/repository provide recommended lists of auditable events.

2.16.2.3 Requirement Enhancements

1. The organization reviews and updates the list of organization-defined auditable events on an organization-defined frequency.
2. The organization includes execution of privileged functions in the list of events to be audited by the system.

2.16.2.4 References

NIST SP 800-53r3	AU-2, AU-12
CAG	CC-6, CC-8
API 1164r2	7.2, Annex B.2.1, Annex B.5
NERC CIPS	CIP 007-3 B.R5.1.2
NRC RG 5.71	App. B.2.2, App. B.2.12

2.16.3 Content of Audit Records

2.16.3.1 Requirement

The system produces audit records that contain sufficient information to establish what events occurred, when the events occurred, where the events occurred, the sources of the events, and the outcomes of the events.

2.16.3.2 Supplemental Guidance

Audit record content includes (1) date and time of the event, (2) the component of the system (e.g., software component, hardware component) where the event occurred, (3) type of event, (4) user/subject identity, and (5) the outcome (success or failure) of the event.

2.16.3.3 Requirement Enhancements

1. The system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
2. The system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

2.16.3.4 References

NIST SP 800-53r3	AU-3, AU-12
CAG	CC-6
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R5
NRC RG 5.71	App. B.2.3, App. B.2.12

2.16.4 Audit Storage Capacity

2.16.4.1 Requirement

The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

2.16.4.2 Supplemental Guidance

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

2.16.4.3 Requirement Enhancements

None

2.16.4.4 References

NIST SP 800-53r3	AU-4
CAG	CC-6
NRC RG 5.71	App. B.2.4

2.16.5 Response to Audit Processing Failures

2.16.5.1 Requirement

The system:

1. Alerts designated organizational officials in the event of an audit processing failure
2. Takes the following additional actions: an organization-defined set of actions to be taken (e.g., shutdown system, overwrite oldest audit records, and stop generating audit records).

2.16.5.2 Supplemental Guidance

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

2.16.5.3 Requirement Enhancements

1. The system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity.
2. The system provides a real-time alert when the following audit failure events occur: an organization-defined audit failure event requiring real-time alerts.
3. The system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and either rejects or delays network traffic above those thresholds.

2.16.5.4 References

NIST SP 800-53r3	AU-5

CAG	CC-6
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.5

2.16.6 Audit Monitoring, Analysis, and Reporting

2.16.6.1 Requirement

The organization:

1. Reviews and analyzes system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to designated organizational officials
2. Adjusts the level of audit review, analysis, and reporting within the system when a change in risk exists to organizational operations, organizational assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

2.16.6.2 Supplemental Guidance

Organizations increase the level of audit monitoring and analysis activity within the control system whenever an indication of increased risk exists to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. Audit records need to be monitored regularly for inappropriate activities in accordance with organizational procedures. Audit reports need to be provided to those responsible for cybersecurity.

2.16.6.3 Requirement Enhancements

1. The system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.
2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
3. The system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system. Note: An example of an automated mechanism for centralized review and analysis is a Security Information Management product.
4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to enhance further the ability to identify inappropriate or unusual activity.

2.16.6.4 References

NIST SP 800-53r3	AU-6
CAG	CC-6
API 1164r2	Annex A, Annex B.3.1.2, Annex B.5.1.1.3
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.6

2.16.7 Audit Reduction and Report Generation

2.16.7.1 Requirement

The system provides an audit reduction and report generation capability.

2.16.7.2 Supplemental Guidance

An audit reduction, review, and reporting capability provides support for near real-time audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records.

In general, audit record processing is not performed on the control system.

2.16.7.3 Requirement Enhancements

1. The control system provides the capability to automatically process audit records for events of interest based on selectable event criteria.
2. Audit record processing must not degrade the operational performance of the control system.

2.16.7.4 References

NIST SP 800-53r3	AU-7, AU-12
CAG	CC-6
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R5.1.2
NRC RG 5.71	App. B.2.7, App. B.2.12

2.16.8 Time Stamps

2.16.8.1 Requirement

The system uses internal system clocks to generate time stamps for audit records.

2.16.8.2 Supplemental Guidance

Time stamps generated by the system include both date and time.

2.16.8.3 Requirement Enhancements

The system synchronizes internal system clocks on an organization-defined frequency.

2.16.8.4 References

NIST SP 800-53r3	AU-8
CAG	CC-6
NERC CIPS	CIP 007-3 B.R6, R6.3
NRC RG 5.71	App. B.2.8

2.16.9 Protection of Audit Information

2.16.9.1 Requirement

The control system protects audit information and audit tools from unauthorized access, modification, and deletion.

2.16.9.2 Supplemental Guidance

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit control system activity. The logs are important for error correction, security breach recovery, investigations, and related efforts.

2.16.9.3 Requirement Enhancements

The system produces audit records on hardware-enforced, write-once media.

2.16.9.4 References

NIST SP 800-53r3	AU-9
CAG	CC-6
API 1164r2	Annex A

NERC CIPS	CIP 007-3 D1.4
NRC RG 5.71	App. B.2.9

2.16.10 Audit Record Retention

2.16.10.1 Requirement

The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

2.16.10.2 Supplemental Guidance

The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes retention and availability of audit records relative to subpoena and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated.

2.16.10.3 Requirement Enhancements

None

2.16.10.4 References

NIST SP 800-53r3	AU-11
API 1164r2	Annex A
NERC CIPS	CIP 007-3 D1.4
NRC RG 5.71	App. B.2.11

2.16.11 Conduct and Frequency of Audits

2.16.11.1 Requirement

The organization conducts audits at planned intervals to determine whether the security objectives, measures, processes, and procedures:

1. Conform to the requirements and relevant legislation or regulations
2. Conform to the identified information security requirements
3. Are effectively implemented and maintained
4. Perform as expected
5. Identify inappropriate activities.

2.16.11.2 Supplemental Guidance

Audits can be either in the form of internal self-assessment or independent, third-party audits. Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for internal purposes. An internal audit needs to be conducted to ensure that documentation is current with any changes to the system. Independent audits review and examine records and activities to assess the adequacy of control system security measures, ensure compliance with established policies and operational procedures, and recommend necessary changes in security requirements, policies, or procedures. For independent audits, the auditors need to be accompanied by an appropriate knowledgeable control system staff person to answer any questions about the particular system under review.

2.16.11.3 Requirement Enhancements

None

2.16.11.4 References

NIST SP 800-53r3	AU-1, CA-7
CAG	CC-17
API 1164r2	Annex A
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.1

2.16.12 Auditor Qualification

2.16.12.1 Requirement

The organization's audit program specifies auditor qualifications in accordance with the organization's documented training program.

2.16.12.2 Supplemental Guidance

The selection of auditors and conduct of audits ensure the objectivity and impartiality of the audit process. Security auditors need to:

1. Understand the control system to be audited and be personally familiar with the systems and operating practices
2. Understand the risk involved with the audit and the consequences associated with unintentional stimulus or denial of service to the control system
3. Fully understand the corporate cyber and control system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and process.

2.16.12.3 Requirement Enhancements

The organization assigns auditor and system administration functions to separate personnel.

2.16.12.4 References

NIST SP 800-53r3	CA-2
CAG	CC-17
API 1164r2	Annex A
NRC RG 5.71	C.3.3.2.8

2.16.13 Audit Tools

2.16.13.1 Requirement

The organization under the audit program specifies strict rules and careful use of audit tools when auditing control system functions.

2.16.13.2 Supplemental Guidance

As a general practice, system audits determine compliance of the control system to the organization's security plan. For new control systems, system auditing utilities need to be incorporated into the design. Appropriate security audit practices for legacy systems require appropriate precautions be taken before assessing the system. For system audits to determine inappropriate activity, information custodians ensure that system monitoring tools are installed to log system activity and security events. Auditing and log management tools need to be used cautiously in maintaining and proving the integrity of the control system from installation through the system life cycle. Access to control systems audit tools need to be protected to prevent any possible misuse or compromise.

2.16.13.3 Requirement Enhancements

If automated cybersecurity scanning tools are used on business networks, extra care needs to be taken to ensure that they do not scan the control system network by mistake. Many installed devices do not have much processing power or sophisticated error-handing routines, and scans can overload the device and effectively create a denial-of-service interruption that could lead to equipment damage, production loss, or health, safety, and environmental incidents.

2.16.13.4 References

NIST SP 800-53r3	AU-7
API 1164r2	Annex B.4.1.1
NRC RG 5.71	App. B.2.7, App. C.3.4

2.16.14 Security Policy Compliance

2.16.14.1 Requirement

The organization demonstrates compliance to the organization’s security policy through audits in accordance with the organization’s audit program.

2.16.14.2 Supplemental Guidance

Periodic audits of the control system are implemented to demonstrate compliance to the organization’s security policy. These audits:

1. Assess whether the defined cybersecurity policies and procedures, including those to identify security incidents, are being implemented and followed
2. Document and ensure compliance to organization policies and procedures
3. Identify security concerns, validate the system is free from security compromises, and provide information on the nature and extent of compromises should they occur
4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes
5. Verify that security mechanisms and management practices present during system validation are still in place and functioning
6. Ensure reliability and availability of the system to support safe operation
7. Continuously improve performance.

2.16.14.3 Requirement Enhancements

None

2.16.14.4 References

NIST SP 800-53r3	CA-1
API 1164r2	Annex A, Annex B.4.1
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	C.3.3.3, C.3.3.2.2, App. C.2.1, App. C.5.1, App. C.7

2.16.15 Audit Generation

2.16.15.1 Requirement

The system:

1. Provides audit record generation capability for the auditable events
2. Provides audit record generation capability at the organization-defined system components
3. Allows authorized users to select which auditable events are to be audited by specific components of the system
4. Generates audit records for the selected list of auditable events.

2.16.15.2 Supplemental Guidance

Audit records can be generated from various components within the system. This control defines the specific system components providing auditing capability. In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

2.16.15.3 Requirement Enhancements

The system provides the capability to compile audit records from multiple components within the system into a systemwide (logical or physical) audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail. Note: This control does not require that audit records from every component that provides auditing capability within the system be included in the systemwide audit trail. The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance. In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls.

2.16.15.4 References

NIST SP 800-53r3	AU-12
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	App. B.2.12, App. C.3.4

2.16.16 Monitoring for Information Disclosure

2.16.16.1 Requirement

The organization monitors open source information for evidence of unauthorized release or disclosure of organizational information.

2.16.16.2 Supplemental Guidance

Unauthorized sensitive protected information (proprietary, security, and configuration) can be discovered in the public domain by self searching public information sources for these types of information releases. This allows the owner to attempt to contain or remove identified sensitive information from such public sources.

2.16.16.3 Requirement Enhancements

None

2.16.16.4 References

NIST SP 800-53r3	AU-13

NERC CIPS	CIP 002-3 through CIP 009-3, D

2.16.17 Session Audit

2.16.17.1 Requirement

Where legally required, the system provides the capability to:

1. Capture and record and log all content related to a user session
2. Remotely view and hear all content related to an established user session in real time.

2.16.17.2 Supplemental Guidance

Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, executive orders, directives, policies, or regulations. Very specific critical infrastructure applications in multiple industrial sectors require control room or cockpit monitoring as a part of operational regulation.

2.16.17.3 Requirement Enhancements

None

2.16.17.4 References

NIST SP 800-53r3	AU-14
API 1164r2	Annex A
NERC CIPS	CIP 002-3 through CIP 009-3, D

2.17 Monitoring and Reviewing Control System Security Policy

Monitoring and reviewing the performance of an organization’s cyber and control system security policy provides the organization the ability to evaluate the performance of its security program. Internal checking methods, such as compliance audits and incident investigations, allow the company to determine the effectiveness of the security program and whether it is operating according to expectations. Finally, through a continuous improvement process, the organization’s senior leaders regularly review compliance information on the security program, developed through the audit and corrective action process, and any deviations from the goals, targets, and objectives set in the planning process. If deviations or nonconformance exists, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

2.17.1 Monitoring and Reviewing Control System Security Management Policy and Procedures

2.17.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, monitoring and reviewing control system security management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the monitoring and reviewing control system security management policy and associated audit and accountability controls.

2.17.1.2 Supplemental Guidance

The organization ensures the monitoring and reviewing of control system security management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The monitoring and reviewing of control system security management policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for a particular control system when required.

2.17.1.3 Requirement Enhancements

None

2.17.1.4 References

NIST SP 800-53r3	PM-1
CAG	CC-17
API 1164r2	1.2
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	App. C.3.4

2.17.2 Continuous Improvement

2.17.2.1 Requirement

The organization's security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into control system security policies and procedures.

2.17.2.2 Supplemental Guidance

None

2.17.2.3 Requirement Enhancements

None

2.17.2.4 References

NIST SP 800-53r3	CA-2, CA-7
CAG	CC-17
API 1164r2	1.2
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	C.4.1

2.17.3 Monitoring of Security Policy

2.17.3.1 Requirement

The organization includes a process for monitoring and reviewing the performance of its cybersecurity policy.

2.17.3.2 Supplemental Guidance

Regular review of the control system security policy needs to be done to validate its effectiveness in implementing the organization's security program and objectives. Effectiveness is measured by the results of cybersecurity audits, incidents, suggestions, and feedback from the organizations corrective action program.

2.17.3.3 Requirement Enhancements

None

2.17.3.4 References

NIST SP 800-53r3	CA-2, CA-7
CAG	CC-2, CC-3, CC-4
API 1164r2	Annex B.4.1.2
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	C.3.3.3.2, C.4.1, C.4.1.1, C.4.1.2, C.4.1.3

2.17.4 Best Practices

2.17.4.1 Requirement

The organization incorporates industry best practices into the organization's security program for control systems.

2.17.4.2 Supplemental Guidance

Best practices include, but are not be limited to:

1. Industry events that identify failed and successful cybersecurity breaches
2. Actions to be taken to resolve a breach of cybersecurity that are defined in light of the
    a. Business priorities
    b. Processes employed to collect metrics (e.g., audits, incidents) that help verify that the cybersecurity activities (manual or automated) are performing as expected
    c. Process that will trigger a review of the level of residual risk and acceptable risk taking when changes exist to the organization, technology, business objectives, and processes
    d. External events including identified threats and changes in social climate
    e. Operational data analyzed, recorded, and reported to assess the effectiveness or performance of the cybersecurity management system.

2.17.4.3 Requirement Enhancements

None

2.17.4.4 References

NIST SP 800-53r3	CA-7
CAG	CC-17
API 1164r2	1.2
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. C.3.5

2.17.5 Security Accreditation

2.17.5.1 Requirement

The organization authorizes (i.e., accredits) the control system for processing before operations and periodically updates the authorization based on organization-defined frequency or when a significant change occurs to the system. A senior organizational official signs and approves the security accreditation.

2.17.5.2 Supplemental Guidance

The organization assesses the security mechanisms employed within the control systems before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications and need to be reviewed annually.

2.17.5.3 Requirement Enhancements

None

2.17.5.4 References

NIST SP 800-53r3	CA-6
API 1164r2	3.6, Annex A
NRC RG 5.71	C.3.3

2.17.6 Security Certification

2.17.6.1 Requirement

The organization assesses the security mechanisms in the control system to determine the extent the security measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

2.17.6.2 Supplemental Guidance

Assessments are performed and documented by qualified assessors as authorized by the organization. External audits are outside the scope of this requirement. Ensure that the assessments do not interfere with control system functions. Care must be taken to ensure that the assessments do not interfere with control system functions. The assessor fully understands the corporate cyber and control system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process. A control system may need to be taken offline, to the extent feasible, before the assessments can be conducted. If a control system must be taken offline for assessments, assessments are scheduled to occur during planned control system outages whenever possible.

2.17.6.3 Requirement Enhancements

1. The organization employs an independent certification agent or certification team to assess the security mechanisms in the control system.

2. An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational control system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the control system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside the organization.

3. Contracted certification services are considered independent if the control system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security mechanisms in the control system.

4. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the control system and the ultimate risk to organizational operations and organizational assets and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

4. In special situations, for example when the organization that owns the control system is small or the organizational structure requires that the assessment of the security mechanisms be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results.
5. The authorizing official should consult with representatives of the appropriate regulatory bodies, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

2.17.6.4 References

NIST SP 800-53r3	CA-4
API 1164r2	3.7

2.18 Risk Management and Assessment

Risk management planning is a key aspect of ensuring that the processes and technical means of securing control systems have fully addressed the risks and vulnerabilities in the system.

An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of control system and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the control system’s compliance status. A documented plan is developed on how the organization will strive to stay in compliance within acceptable risk.

A comprehensive organization risk assessment process is implemented and periodically executed. Assets are categorized into security levels based on the level of security necessary for each asset to be sufficiently protected. Risk is assessed across the organization by determining the likelihood of potential threats and cost if the threat is realized. Control system vulnerabilities need to be recognized and documented.

2.18.1 Risk Assessment Policy and Procedures

2.18.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

2.18.1.2 Supplemental Guidance

The organization ensures the risk assessment policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The risk assessment policy also takes into account the organization’s risk tolerance level. The risk assessment policy can be included as part of the general security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular control system, when required.

2.18.1.3 Requirement Enhancements

None

2.18.1.4 References

NIST SP 800-53r3	RA-1
API 1164r2	3.3, Annex B.2
NERC CIPS	CIP 002-3 B.R1, R1.2
NRC RG 5.71	C.3.3

2.18.2 Risk Management Plan

2.18.2.1 Requirement

The organization develops a risk management plan. A senior organization official reviews and approves the risk management plan.

2.18.2.2 Supplemental Guidance

None

2.18.2.3 Requirement Enhancements

None

2.18.2.4 References

NIST SP 800-53r3	CA-1, RA-1, PM-9
CAG	CC-9
API 1164r2	3.3, Annex B.2
NERC CIPS	CIP 002-3 B.R1, R1.2
NRC RG 5.71	C.3.3, C.3.3.3, C.3.3.3.2, App. C.13

2.18.3 Certification, Accreditation, and Security Assessment Policies and Procedures

2.18.3.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. Formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
2. Formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

2.18.3.2 Supplemental Guidance

The organization ensures the security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The certification, accreditation, and security assessment policies can be included as part of the general information security policy for the organization. Certification, accreditation, and security assessment procedures can be developed for the security program in general and for a particular control system when required. The organization defines what constitutes a significant change to the control system to achieve consistent security reaccreditations.

2.18.3.3 Requirement Enhancements

None

2.18.3.4 References

NIST SP 800-53r3	CA-1, PM-9
API 1164r2	3.3, Annex B.2
NRC RG 5.71	C.3.3, C.3.3.3, C.3.3.3.2, App. C.13

2.18.4 Security Assessments

2.18.4.1 Requirement

The organization:

1. Assesses the security controls in the system on an organization-defined frequency, at least annually, to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system
2. Produces a security assessment report that documents the results of the assessment.

2.18.4.2 Supplemental Guidance

The organization assesses the security controls in a system as part of (1) security authorization or reauthorization, (2) meeting the requirement for annual assessments, (3) continuous monitoring, and (4) testing/evaluation of the system as part of the system development life-cycle process. The requirement for (at least) annual security control assessments should not be interpreted by organizations as adding assessment requirements to those requirements already in place in the security authorization process. To satisfy the annual assessment requirement, organizations can draw on the security control assessment results from any of the following sources, including but not limited to, (1) security assessments conducted as part of a system authorization or reauthorization process, (2) continuous monitoring, or (3) testing and evaluation of the system as part of the ongoing system development life-cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the system and in accordance with policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls for the system is based on (1) the security categorization of the system, (2) the specific security controls selected and employed by the organization, and (3) the level of assurance that the organization must have in determining the effectiveness of the security controls. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the system for assessment. Those security controls that are volatile or critical to protecting the system are assessed at least annually. All other controls are assessed at least once during the system’s 3-year authorization cycle. The organization can use the current year’s assessment results from any of the above sources to meet the annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness.

2.18.4.3 Requirement Enhancements

1. The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the system.
2. The organization includes as part of security control assessments, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises.

2.18.4.4 References

NIST SP 800-53r3	CA-2
CAG	CC-17

API 1164r2	Annex B.4.1.2
NERC CIPS	CIP 003-3 B.R4, R4.3, CIP 005-3 B.R4
NRC RG 5.71	C.3.3, C.3.3.3, C.3.3.3.2, App. C.13

2.18.5 Control System Connections

2.18.5.1 Requirement

The organization:

1. Authorizes all connections from the system to other systems outside the authorization boundary through the use of system connection agreements
2. Documents the system connections and associated security requirements for each connection
3. Monitors the system connections on an ongoing basis verifying enforcement of documented security requirements.

2.18.5.2 Supplemental Guidance

Because security categorizations apply to individual systems, the organization carefully considers the risks that may be introduced when systems are connected to other systems with different security requirements and security controls, both internal to the organization and external to the organization. Each interconnection between systems must be addressed individually, documenting the interface characteristics. The level of formality for this documentation varies depending on the relationship between the systems. The relationship ranges from systems with the same owner for which there is no need of an agreement but simply a description of the interface characteristics, to systems within different organizations necessitating a formal interconnection security agreement and a Memorandum of Understanding/Agreement. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the systems. Risk considerations also include systems sharing the same networks.

2.18.5.3 Requirement Enhancements

None

2.18.5.4 References

NIST SP 800-53r3	CA-3
CAG	CC-5
API 1164r2	7.1, 7.3.1, 7.3.2, 7.3.3, 7.3.4, 8.2
NERC CIPS	CIP 005-3 B.R1, R2, R3

2.18.6 Plan of Action and Milestones

2.18.6.1 Requirement

The organization develops and updates a plan of action and milestones for the control system that documents the organization’s planned, implemented, and evaluated remedial actions to correct weaknesses or deficiencies noted during the assessment of the security measures and to reduce or eliminate known vulnerabilities in the system. The organization reviews the action plan at least annually.

2.18.6.2 Supplemental Guidance

The plan of action and milestone updates are based on the findings from security control assessments, security impact analyses, and continual monitoring activities.

2.18.6.3 Requirement Enhancements

None

2.18.6.4 References

NIST SP 800-53r3	CA-5
API 1164r2	Annex B.3.1.1, Annex B.5.1.1.1
NERC CIPS	CIP 002-3 through CIP 009-3, C and D

2.18.7 Continuous Monitoring

2.18.7.1 Requirement

The organization monitors the security mechanisms in the control system on an ongoing basis. Those security mechanisms that are volatile or critical to protecting the control system are assessed at least annually. All other security mechanisms are assessed at least once during the control system's 3-year accreditation cycle.

2.18.7.2 Supplemental Guidance

A continuous monitoring program allows an organization to maintain the security authorization of a system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management for systems. An effective continuous monitoring program includes: (1) configuration management and control of system components, (2) security impact analyses of changes to the system or its environment of operation, (3) ongoing assessment of security controls, and (4) status reporting.

This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the system. An effective continuous monitoring program results in ongoing updates to the system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security authorization package. A rigorous and well-executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the system.

2.18.7.3 Requirement Enhancements

The organization employs an independent assessor or assessment team to monitor the security controls in the system on an ongoing basis.

2.18.7.4 References

NIST SP 800-53r3	PM-4, PM-8, PM-9, PM-11, CA-7
CAG	CC-17
API 1164r2	7.2, Annex A, Annex B.3.1.4, Annex B.4.1
NERC CIPS	CIP 007-3 B.R6
NRC RG 5.71	C.4, C.4.1, App. C.3.4, App. C.5.8

2.18.8 Security Categorization

2.18.8.1 Requirement

The organization:

1. Categorizes information and systems in accordance with applicable laws, management orders, directives, policies, regulations, standards, and guidance

2. Documents the security categorization results (including supporting rationale) in the system security plan for the information system

3. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

2.18.8.2 Supplemental Guidance

A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be compromised through a loss of availability, integrity, or confidentiality. The organization conducts security categorization as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, control system owners, and information owners. As part of a defense-in-depth protection strategy, the organization may consider partitioning higher-impact control systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk.

This control includes, but is not limited to, the categorization of control system design information, network diagrams, process programs, and vulnerability assessments. Categorization is based on the need, priority, and level of protection required commensurate with sensitivity and impact of the loss of availability, integrity, or confidentiality. The organization periodically inventories and reviews the control system and information categorizations with established configuration management plans including where the information is processed, stored, and transmitted. The organization considers safety issues in categorizing the control system. The organization also considers potential impacts to other organizations (e.g., business partners, stakeholders), including interdependencies, and potential local, regional, and national impacts in categorizing the control system.

2.18.8.3 Requirement Enhancements

None

2.18.8.4 References

NIST SP 800-53r3	RA-2
CAG	CC-9
API 1164r2	6, Annex B.2.1
NERC CIPS	CIP 007-3 A, B, C, D

2.18.9 Risk Assessment

2.18.9.1 Requirement

The organization develops, disseminates, and reviews/updates:

1. A formal documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance

2. Formal documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

2.18.9.2 Supplemental Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable laws, executive orders, directives, policies regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment also considers potential impacts to other organizations (e.g., business partners, stakeholders), and potential local, regional, and national level impacts of the control system including interdependencies and safety issues.

2.18.9.3 Requirement Enhancements

None

2.18.9.4 References

NIST SP 800-53r3	RA-3
CAG	CC-5, CC-10, CC-15, CC-16, CC-17
API 1164r2	7.2, Annex A, Annex B.3.1.4, Annex B.4.1
NERC CIPS	CIP 003-3 B.R4, R4.3, CIP 005-3 B.R4
NRC RG 5.71	C.3.3, App. C.13

2.18.10 Risk Assessment Update

2.18.10.1 Requirement

The organization updates the risk assessment plan annually or, whenever significant changes occur to the control system, the facilities where the system resides, or other conditions that may affect the security or accreditation status of the system.

2.18.10.2 Supplemental Guidance

The organization develops and documents specific criteria for what are considered significant changes to the control system.

2.18.10.3 Requirement Enhancements

None

2.18.10.4 References

NIST SP 800-53r3	RA-3
CAG	CC-10, CC-17
API 1164r2	3.3, 3.6, Annex A
NERC CIPS	CIP 007-3 B.R8
NRC RG 5.71	C.3.3, App. C.13

2.18.11 Vulnerability Assessment and Awareness

2.18.11.1 Requirement

The organization:

1. Scans for vulnerabilities in the system on an organization-defined frequency and randomly in accordance with organization-defined process and when new vulnerabilities potentially affecting the system are identified and reported
2. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations; (b) formatting and making transparent checklists and test procedures; and (c) measuring vulnerability impact
3. Analyzes vulnerability scan reports and remediates legitimate vulnerabilities within a defined timeframe based on an assessment of risk

4. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other systems.

2.18.11.2 Supplemental Guidance

Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for web-based vulnerabilities, source code reviews, and static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms. Operational approval and care must be used when and if vulnerability scanning and penetration testing are used, to ensure ICS functions are not adversely impacted by the scanning process. Production ICS need to be taken off-line or replicated on test beds to the extent feasible. It is possible to scan ICS systems if they are off-line, but caution and approval of such scans are essential. Network scanning tools have been known to cause detrimental operational issues if not configured and tested before being used. It is not recommended to scan operational ICS systems unless absolutely required. If the risks for scanning on operational equipment are deemed too great, the organization should employ compensating controls.

2.18.11.3 Requirement Enhancements

1. The organization employs vulnerability scanning tools that include the capability to readily update the list of system vulnerabilities scanned.
2. The organization updates the list of system vulnerabilities scanned on an organization-defined frequency or when new vulnerabilities are identified and reported.
3. The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., system components scanned and vulnerabilities checked).
4. The organization attempts to discern what information about the system is discoverable by adversaries.
5. The organization performs security testing to determine the level of difficulty in circumventing the security controls of the system.
6. The organization includes privileged access authorization to organization-defined system components for selected vulnerability scanning activities to facilitate more thorough scanning.
7. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.
8. The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational systems and notify designated organizational officials.

2.18.11.4 References

NIST SP 800-53r3	RA-5
CAG	CC-4, CC-5, CC-7, CC-10, CC-17
API 1164r2	3.3, 3.6, Annex A
NERC CIPS	CIP 007-3 B.R8
NRC RG 5.71	C.4, C.4.1.3, App. C.13.1

2.18.12 Identify, Classify, Prioritize, and Analyze Potential Security Risks

2.18.12.1 Requirement

The organization identifies, classifies, prioritizes, and analyzes potential security threats, vulnerabilities, and consequences to their control systems assets using accepted methodologies.

2.18.12.2 Supplemental Guidance

The organization begins by identifying the potential risks for its system. This is not a detailed analysis but a general identification of places and systems that might be at risk. These are then classified as to potential for harm and the organizations tolerance for risk. The risks are prioritized by which are of the most concern to the organization.

Each of the risks is then analyzed using an accepted methodology. A written plan documents the types of security incidents and the response to each type. This plan includes step-by-step actions to be taken by the various organizations. Risk reduction measures are implemented, and the results are monitored to ensure effectiveness of the risk management plan.

The reasons for selecting or rejecting certain security mitigation measures and the risks they address need to be documented. The security measures and countermeasures contained in the risk mitigation plan are designed to lower the risk to an acceptable level and minimize the adverse effect of a threat-exploiting vulnerability in the control system network.

2.18.12.3 Requirement Enhancements

None

2.18.12.4 References

NIST SP 800-53r3	RA-5
CAG	CC-4, CC-5, CC-7, CC-10, CC-17
API 1164r2	Annex B.3.1
NERC CIPS	CIP 007-3 B.R8
NRC RG 5.71	C.4, C.4.1.3, App. C.13.1

2.19 Security Program Management

2.19.1 Information Security Program Plan

2.19.1.1 Requirement

The organization:

1. Develops and disseminates an organization-wide security program plan that:
   a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements
   b. Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended
   c. Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance

   d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation

2. Reviews the organization-wide security program plan on an organization-defined frequency, at least annually

3. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

2.19.1.2 Supplemental Guidance

The security program plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual systems and the organization-wide security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's security program plan unless the controls are included in a separate security plan for a system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational systems). The organization-wide security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a separate document or in multiple documents in situations where different organizational entities are assigned responsibility. These different entities are accountable for the implementation, assessment, and approval of the common controls that are not implemented as part of a system. In those cases, the documents describing common controls are included as attachments to the security program plan. If multiple common control documents are contained in the security program plan, the organization specifies in each document, the organizational official or officials responsible for the implementation, assessment, and approval of the common controls included in the respective documents. For example, the organization may require that the Facilities Management Office develop, implement, assess, and approve common physical and environmental protection controls or that the Human Resources Office develop, implement, assess, and approve common personnel security controls when such controls are not associated with a system.

2.19.1.3 Requirement Enhancements

None

2.19.1.4 References

NIST SP 800-53r3	PM-1
API 1164r2	1.2, 3
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. C.5.3

2.19.2 Senior Information Security Officer

2.19.2.1 Requirement

The organization appoints a senior security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.

2.19.2.2 Supplemental Guidance

The security officer described in this control is an official of the organization or an official of an appropriate subordinate organization. Organizations also may refer to this organizational official as the Senior Security Officer or Chief Security Officer.

2.19.2.3 Requirement Enhancements

None

2.19.2.4 References

NIST SP 800-53r3	PM-2
API 1164r2	1.2, Annex B.5
NERC CIPS	CIP 002-3 B.R4
NRC RG 5.71	C.3.1.2

2.19.3 Information Security Resources

2.19.3.1 Requirement

The organization:

1. Ensures that all capital planning and investment requests include the resources needed to implement the security program and documents all exceptions to this requirement
2. Employs a business case to record the resources required
3. Ensures that security resources are available for expenditure as planned and approved.

2.19.3.2 Supplemental Guidance

Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the security-related aspects of the capital planning and investment control process.

2.19.3.3 Requirement Enhancements

None

2.19.3.4 References

NIST SP 800-53r3	PM-3
API 1164r2	3.6
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.4 Plan of Action and Milestones Process

2.19.4.1 Requirement

The organization (1) implements a process for ensuring that plans of action and milestones for the security program and the associated organizational systems are maintained and (2) documents the remedial security actions (from identification of needed action through assessment of implementation) to mitigate risk to organizational operations and assets, individuals, other organizations, and the nation.

2.19.4.2 Supplemental Guidance

The plan of action and milestones is a key document in the security program. The plan of action and milestones updates is based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

2.19.4.3 Requirement Enhancements

None

2.19.4.4 References

NIST SP 800-53r3	PM-4
API 1164r2	Annex B.3.1.1, Annex B.5.1.1.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.5 Information System Inventory

2.19.5.1 Requirement

The organization develops and maintains an inventory of its systems and critical components.

2.19.5.2 Supplemental Guidance

This control addresses the inventory requirements in Federal Information Security Management Act (FISMA). Federal organizations or organizations using information systems on behalf of a federal agency must comply with FISMA requirements. Additionally, a central tenet of the US Comprehensive National Cybersecurity Initiative states that "offense must inform defense." Or, knowledge of actual attacks that have already compromised systems is the essential foundation on how to begin to construct effective defenses. But the basic tenant in cybersecurity is that you have to know what elements you have and how they work and how they are connected before you can begin the process of protecting them.

2.19.5.3 Requirement Enhancements

None

2.19.5.4 References

NIST SP 800-53r3	CA-3, CM-3 CM-6, IA-3,PM-5
CAG	CC-1
API 1164r2	3.6, Annex B. 1.1, Annex B.2.1
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. C.11.9

2.19.6 Information Security Measures of Performance

2.19.6.1 Requirement

The organization develops, monitors, and reports on the results of security measures of performance.

2.19.6.2 Supplemental Guidance

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the security program and the security controls employed in support of the program.

2.19.6.3 Requirement Enhancements

None

2.19.6.4 References

NIST SP 800-53r3	PM-6
CAG	CC-1, CC-2, CC-3
API 1164r2	7.2.2, 8.2.4, Annex A, Annex B.1, Annex B.2.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.7 Enterprise Architecture

2.19.7.1 Requirement

The organization develops an enterprise architecture with consideration for security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation.

2.19.7.2 Supplemental Guidance

The integration of security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting standards and guidelines. The Federal Enterprise Architecture Segment Architecture Methodology provides guidance on integrating security requirements and security controls into enterprise architectures.

2.19.7.3 Requirement Enhancements

None

2.19.7.4 References

NIST SP 800-53r3	PM-7
CAG	CC-16
API 1164r2	7, Annex B.1.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.8 Critical Infrastructure Plan

2.19.8.1 Requirement

The organization addresses security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

2.19.8.2 Supplemental Guidance

The critical infrastructure and key resources protection plan is consistent with applicable laws, directives, policies, regulations, standards, and guidance.

2.19.8.3 Requirement Enhancements

None

2.19.8.4 References

NIST SP 800-53r3	PM-8
API 1164r2	4
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.9 Risk Management Strategy

2.19.9.1 Requirement

The organization:

1. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the nation associated with the operation and use of systems
2. Implements that strategy consistently across the organization.

2.19.9.2 Supplemental Guidance

An organization-wide risk management strategy should include an unambiguous expression of the risk tolerance of the organization, guidance on acceptable risk assessment methodologies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy.

2.19.9.3 Requirement Enhancements

None

2.19.9.4 References

NIST SP 800-53r3	PM-9
API 1164r2	3.3
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.10 Security Authorization Process

2.19.10.1 Requirement

The organization:

1. Manages (i.e., documents, tracks, and reports) the security state of organizational systems through security authorization processes
2. Fully integrates the security authorization processes into an organization-wide risk management strategy.

2.19.10.2 Supplemental Guidance

The security authorization process for systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines.

2.19.10.3 Requirement Enhancements

None

2.19.10.4 References

NIST SP 800-53r3	PM-10
API 1164r2	7.3, Annex B. 2.1, Annex B.5.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.11 Mission/Business Process Definition

2.19.11.1 Requirement

The organization:

1. Defines mission/business processes with consideration for security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation
2. Determines protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

2.19.11.2 Supplemental Guidance

Protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Inherent in defining an organization’s protection needs is an understanding of the level of adverse impact that could result if a compromise occurs and, therefore, a categorization of information in accordance with FIPS 199. Modeling and simulation techniques can help in discerning the security ramification in mission/business process definitions.

2.19.11.3 Requirement Enhancements

None

2.19.11.4 References

NIST SP 800-53r3	PM-11
API 1164r2	Annex A, Annex B.1.1
NERC CIPS	CIP 002-3 through CIP 009-3

3. CONCLUSIONS

This document presents a wide sampling of best practice, guidelines, and security controls for control systems used in many industries. Because this document is not limited to a specific industry sector, it should, therefore, be viewed as a master listing of reference information to be used when reviewing and developing standards for control systems. The recommended controls are designed specifically to provide standards bodies of industry sectors the basic security framework needed to develop sound security standards within each individual industry sector.

The recommendations presented in this document are designed to assist in creating the appropriate security program for control system networks with awareness to the threats and vulnerabilities of the enterprise. However, each industry has its own definitions and deployment intricacies, and therefore, all recommendation may not be appropriate. In particular, definitions and institutional operations drive the language and structure of many diverse standards and guidelines, yet the convergence and similarities of industrial cybersecurity is undeniable. Various guidelines and standards cannot be compared using control family titles only, as several standards and guidelines address similar security concerns in different areas, and typically within the context of related control families. Both the CAG and RG5.71 tend to do this, in that on first look, it appears security controls may not have been addressed. In fact, they have been extensively addressed, within several control families (examples would be “roles and responsibilities,” “document retention times” and “access control.” Each of these families are widely addressed within other controls, as roles and responsibilities, document retention times and access controls change with the subject matter (i.e., visitor control, configuration management, incident control).

These recommendations should be reviewed periodically to stay abreast of changing control system technologies, standards, guidelines, and cybersecurity threats to the industry. These recommendations address control system problems of a general nature. Implementing all these controls cannot guarantee absolute safety and security against cyber threats, as the dynamic nature of threats define defense as always lagging the offensive nature of malware. However, judicious adoption of the control system elements and defenses to harden existing ICSs must be made in the attempt to protect CIKR. The recommendations presented in this document can and should be customized by standards bodies representing each particular industry and business. Local, state, and federal laws and regulations should be reviewed as having precedence with respect to each particular industry and control system deployment.

4. GLOSSARY: DEFINITIONS OF TERMS

The terms and definitions referenced in this glossary are specific to their use in this document. No attempt has been made to correlate the definitions of the terms in this glossary with similar terms in other documents or standards.

Term	Definition
Access Control	The control of entry or use, to all or part, of any physical, functional, or logical component of a control system.
Accountability	An obligation or willingness to accept responsibility. A property or record that ensures that the actions of an entity may be traced uniquely to that entity.
Accreditation	The official management decision given by a senior organization official to authorize operation of a control system and explicitly to accept the risk to organization operations (including mission, functions, image, or reputation), organization assets, or individuals based on the implementation of an agreed-upon set of security measures.
Accreditation Boundary	All components of a control system to be accredited by an authorizing official and exclude separately accredited systems, to which the control system is connected. Synonymous with the term security perimeter defined in Committee on National Security Systems (CNSS) Instruction 4009 and DCID 6/3.
Activities	The performance of job functions or duties (e.g., conducting system backup operations, monitoring network traffic). An observed physical or logical event (e.g., the output from surveillance equipment or an entry in a log file).
Adequacy	Sufficient for a specific requirement or level of security.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information of a control system.
Agency	Of or belonging to the organization (e.g., senior agency information security officer).
Agreement	A contract or arrangement, either written or verbal, and sometimes enforced by law.
Approval	To give formal or official sanction.
Asset	An entity that may have value to the organization. Assets may be tangible or intangible. Assets may be people, a facility, materials, equipment, information, business reputation, an activity, or operation.
Attack	Attempt to gain unauthorized access to a system’s services, resources, or information, or the attempt to compromise a control system’s integrity, availability, or confidentiality.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a control system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Term	Definition
Authorization	The right or a permission that is granted to a system entity to access a control system resource.
Authorizing Official	Official with the authority to formally assume responsibility for operating a control system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability	The property of a system or a system resource being accessible and usable on demand by an authorized system entity, according to performance specifications for the system.
Backup	A copy of information to facilitate recovery of operations or data restoration, if necessary. Redundant control system equipment that is available to allow continued control system operations in the event that the primary equipment fails.
Bandwidth	The rate at which a data path (e.g., a channel) carries data, measured in bits per second.
Bluetooth	A short-range wireless standard developed to create cableless connections between devices.
Boundary Protection	Methods to protect and/or isolate the ICS from IT Business systems and outside internet capable systems.
Business Network	An organization's data communications network used for general purpose business activities, typically connecting a wide variety of noncritical assets and users.
Can	The word "can," equivalent to "is able to," is used to indicate possibility and capability, whether material or physical.
Certificate	See "public key certificate."
Certification	A comprehensive assessment of the management, operational and technical security mechanisms in a control system, made in support of security accreditation, to determine the extent the security measures are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.
Chief Information Officer	An organization official responsible for: providing advice and other assistance to the head of the organization and other senior management personnel of the organization to ensure that control system technology is acquired and control system resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the organization; developing, maintaining, and facilitating the implementation of a sound and integrated control system technology architecture for the organization; and promoting the effective and efficient design and operation of all major control system resources management processes for the organization, including improvements to work processes of the organization.
Client	A device or program requesting a service.
Compromise	The unauthorized disclosure, modification, substitution, or use of data or equipment.

Term	Definition
Confidential	Spoken, written, or electronic information that must be kept secret or in the confidence of a trusted employee; secret; private, entrusted with another's confidence or secret affairs, kept hidden or separate from the knowledge of others. Information that if released could cause harm to the operator and that is only supplied on a need-to-know basis.
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Contingency	A plan for how an organization will resume partially or completely interrupted critical function(s) within a predetermined time after a disaster or disruption.
Control System	A set of hardware and software acting in concert that manages the behavior of other devices.
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).
Cost	Value impact to the organization or person that can be measured.
Countermeasure	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a control system. Synonymous with security measures and safeguards.
Covert Channel Analysis	A method to covertly analyze and identify aspects of system communication that are potential avenues for covert storage, timing channels, and unauthorized information.
Cryptographic Boundary	A logical container where all the relevant security components of a control system that employ cryptography reside. It includes the processing hardware, data, and memory as well as other critical components.
Cryptographic Key (key)	A parameter used in conjunction with a cryptographic algorithm that defines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.
Cryptographic Module	The set of hardware, software, and/or firmware that implements an approved security function(s) (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
Cyber	Of, relating to, or involving computers or computer networks.
Cyber Attack	Exploitation of the software vulnerabilities of IT-based control components.

Term	Definition
Cybersecurity	The protection of digital systems and their support systems from threats of: Cyberspace attack by adversaries who wish to disable or manipulate them. Physical attack by adversaries who wish to disable or manipulate them. Access by adversaries who want to obtain, corrupt, damage, or destroy sensitive information. This is an aspect of information security. Electronic data can be obtained by theft of computer storage media or by hacking into the computer system. A cyberspace attack may be mounted to obtain sensitive information to plan a future physical or cyberspace attack.
Cybersecurity Incident	Any malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.
Data	A common term used to indicate the basic elements that can be processed or produced by a computer.
Demilitarized Zone	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
Denial-of-Service	The prevention of authorized access to a system resource or the delaying of system operations and functions. (See "interruption.")
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented, provides the services of origin authentication, data integrity, and signer nonrepudiation.
Distributed Control Systems	A distributed control system is a type of plant automation system similar to a SCADA system, except that a distributed control system is usually employed in factories and is located within a more confined area. It uses a high-speed communications medium, which is usually a separate wire (network) from the plant LAN. A significant amount of a closed loop control is present in the system.
Domain Name	An abstraction of IP addresses using more easily remembered names.
Electronic Security Perimeter	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Element	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be composed of one or more components.
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state [RFC 2828].
Entity	The facility or critical asset owner, operator, etc.
Environment	The ambient natural and artificial conditions that surround a piece of operating equipment.

Term	Definition
Facility	A plant, building, structure, or complex contiguously located on the same site, defined by a single geographical perimeter (usually determined by a fence or other barrier that surrounds and limits uncontrolled access), and used by the operator or its contractors for the performance of work under the jurisdiction of the operator. The term "facility" includes the land (soil), surface water, and groundwater contained within its geographical perimeter.
File Transfer Protocol	FTP is an Internet standard for transferring files over the Internet. FTP programs and utilities are used to upload and download web pages, graphics, and other files from your hard drive to a remote server which allows FTP access.
Firewall	A set of programs residing on a gateway server that protect the resources of an internal network. Basically, a firewall working closely with a router program examines each network packet to determine whether to forward it to its destination. A firewall is often installed in a specially designated computer that is separate from the rest of the network so no incoming request can get directly at private network resources. Several firewall screening methods are available; a simple one is to screen requests to make sure they come from an acceptable (previously identified) domain name and IP address on known ports. For mobile users, firewalls may allow remote access to the private network using secure logon procedures and authentication mechanisms.
Firmware	Programs or instructions that are permanently stored in hardware memory devices (usually read-only memories) that control hardware at a primitive level.
Gateway	A gateway is a network point that acts as an entrance to another network. [W–Gateway]
Hardware	Physical equipment directly involved in performing industrial process measuring and controlling functions.
Heterogeneity	Increasing the diversity of information technologies within the information system reduces the impact of exploitation from a specific technology.
Honeypots	Devices and/or techniques designed to actively seek out, monitor, and log malicious code and exploits in the internet in a secure configuration by posing as unprotected cyber clients.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a control system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the requirements for its generation, collection, processing, dissemination, and disposal.
Information Security	The protection of information and control systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide availability, integrity, and confidentiality.
Information Security Policy	Aggregate of directives, regulations, rules, practices, and procedures that prescribe how an organization manages, protects, and distributes information.

Term	Definition
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the organization. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity	Quality of a control system reflecting the logical correctness and reliability of the operation of the system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
Interface	A logical entry or exit point of a cryptographic boundary that provides access to cryptographic modules for logical information flow.
Internal	Information that is accessible to all Employees and Contractors within the electronic perimeter, while providing services to the organization.
Interruption	A degradation or disruption of the communication from a device using message flooding, generation of invalid messages, or physical attacks on the communication system. Most commonly known as denial of service or distributed denial of service if multiple attackers are involved.
Intrusion	Unauthorized act of bypassing the security boundaries of a system.
Intrusion Detection (IDet)	IDet is a type of security management system for computers and networks. An IDet system gathers and analyzes information from various areas within a device or a network to identify possible security breaches, including intrusions (attacks from outside the organization) and misuse (attacks from within the organization).
IPSec	Short for “IP Security,” a set of protocols developed by the Internet Engineering Task Force to support the secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs). IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.
ISA	International Society of Automation – Industrial Automation Controls System standards group, associated with ANSI and IEC.
Key	See cryptographic key.
Key Establishment	The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

Term	Definition
Label	In data processing, a set of symbols used to identify or describe an item, record, message, or file. Occasionally, it may be the same as the address in storage.
Least Privilege	The concept of "Least Privilege" is to grant users only those permissions they need to operate and function. This reduces and eliminates the introduction of rouge or malware into cyber systems.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the availability, integrity, or confidentiality of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host, spyware, and some forms of adware (extortionware) are also examples of malicious code.
Malware	Malicious software developed to cause harm or undesirable effects to a computer or device.
Master	A device that initiates communications requests to gather data or perform control functions.
May	The word "may," equivalent to "is permitted," is used to indicate a course of action permissible.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, firmware, or physical devices) employed within or at the boundary of a control system.
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within a control system. The physical interconnection between devices attached to a network. Typical media are twisted pair, baseband coax, broadband coax, and fiber optics.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Message	An arbitrary amount of information whose beginning and end are defined or implied.
Mobile Code	Software programs or parts of programs obtained from remote control systems, transmitted across a network, and executed on a local control system without explicit installation or execution by the recipient. Typically used in configuration or alert pop-ups in gui interfaces.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Mobile Devices	Portable cartridge/disk-based, removable storage media (floppy disks, CDs, tape, USB flash drives, external hard drives, and other flash memory cards (SD)/drives that contain nonvolatile memory) or portable computing and communications device with information storage capability (notebook computers, personal digital assistants, cellular telephones, cameras). Used for component control system configuration.
Modification	The alteration of data or information; in the adverse situation, the alteration results in a condition other than intended by the originator.

Term	Definition
Monitor	To measure a quantity continuously or at regular intervals so that corrections to a process or condition may be made without delay if the quantity varies outside prescribed limits. Software or hardware that observes, supervises, or verifies the operations of a system.
Monitoring	The act of observing, carrying out surveillance on, and/or recording the presence of individuals for the purpose of maintaining and improving procedural standards and security. The act of detecting the presence of unauthorized personnel, sounds, or visual signals, and the measurement thereof with appropriate measuring instruments.
Must	The use of the word "must" is deprecated and shall not be used when stating mandatory requirements. The word "must" is used to describe unavoidable situations only.
Network Disconnect	The cyber system terminates a network connection at the end of a session or after a period of inactivity.
Nonrepudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information and receiving a message.
Operator	The person who initiates and monitors the operation of a computer or process.
Organization	An administrative and functional structure that pursues collective goals, that manages its own performance, and that has a boundary separating it from its environment (as a business, association, or society); also the personnel of such a structure.
Packet	A collection of data created for transmittal across a network. The data include the data needing transmission along with control data needed to direct the data properly to its destination.
Parity	A simple error detection technique that uses an extra parity bit for blocks of data.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Patch	An update for software created to fix bugs and errors but has become synonymous with fixing security vulnerabilities.
Penetration Testing	A test methodology in which assessors, using all available documentation (system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Periodically	An amount of time not to exceed 1 year.
Physical Security	Measures intended to improve protection by means such as fencing, locks, vehicle barriers, area lighting, surveillance systems, guards, dogs, intrusion detection systems, alarms, access controls, vehicle control, and housekeeping.
Physical Security Perimeter	A type of gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel. The physical border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled.

Term	Definition
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Port	A logical entry or exit point on a computer for connecting communications or peripheral devices.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (1) a limited adverse effect (FIPS 199 low), (2) a serious adverse effect (FIPS 199 moderate), or (3) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Predictable Failure Prevention	Mean time between failure rates are defendable and based on considerations that are installation specific, not the industry average. This provides the asset owner with a list of substitute information system components when needed and a mechanism to exchange active and standby roles of the components.
Private Key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.
Process Control	Descriptive of systems in which computers or intelligent electronic devices are used for automatic regulation of operations or processes. Typical are operations wherein the control is applied continuously and adjustments to regulate the operation are directed by the computer or device to keep the value of a controlled variable constant. Contrasted with numerical control.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Protocol	A set of rules used by end point devices in a telecommunication connection to facilitate data exchange.
Proxy Server	A server placed between users and the Internet to act as a filter for malicious or unwanted traffic. Proxy servers are stateful, and most focus on a single application (HTTP, FTP, etc.) and, therefore, can detect more malicious activity than a firewall or router.
Public	Information that can be shared with the general public.
Public Key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered Collaborative Signal Processing.)
Public Key Certificate	A set of data that uniquely identifies an entity contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.
Public Key Infrastructure	A framework that is established to issue, maintain, and revoke public key certificates.
Recommended	The word "recommended" is used to indicate flexibility of choice with a strong preference for the referenced control.
Record	A group of related facts or fields of information treated as a unit, thus a listing of information, usually in printed or printable form. To put data into a storage device.

Term	Definition
Records	The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the control system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
Register	High speed storage within a Central Processing Unit (CPU) where data or the data's address in RAM resides when being processed. Consider adding definition for a Programmable Logic Controller register
Remote Access	Access by users (or control systems) communicating external to a control system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to a control system security perimeter.
Replay	Recording message traffic and "playing it back" to a device later in order to make it do what you want.
Residual Risk	The remaining risks after the security controls have been applied.
Restricted	Information with limited or confined distribution, which is not accessible to the general public or other company employees.
Risk	A measure combining the severity and likelihood of harm from an event. Alternatively, the likelihood of an adverse outcome: Risk = L × P × C, L is the likelihood of attack and depends on the motivation, capabilities, and intent of adversaries. P is the probability of success and depends on vulnerabilities present. C is the consequence(s). Risk is also the potential for damage to or loss of an asset.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of a control system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints because of laws, directives, policies, or regulations.
Role	A set of transactions that a user or set of users can perform within the context of an organization.

Term	Definition
Role-based Access Control	Access control based on user roles (a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Router	A network layer device that sends traffic on the quickest route to reach its destination.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a control system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
SCADA System	Supervisory Control and Data Acquisition systems are a combination of computer hardware and software used to send commands and acquire data for the purpose of monitoring and controlling.
Secret Key	A cryptographic parameter held private by one or more entities to limit the ability to communicate or access that group or entity.
Security	Protection against threats and attacks.
Security Category	The characterization of information or a control system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or control system would have on organizational operations, organizational assets, or individuals.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Label	Explicit or implicit marking of a data structure or output media associated with a control system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Performance	Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, postcompromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.
Security Perimeter	See Accreditation Boundary.
Security Plan	A document that describes an operator's plan to address security issues and related events, such as security assessments and mitigation options, and includes security levels and response measures to security threats.

Term	Definition
Security Policies	Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.
Security Practices	Security practices provide a means of capturing experiences and activities that help ensure system protection and reduce potential manufacturing and control systems compromise. Subject areas include physical security, procedures, organization, design, and programming. Security practices include the actual steps to be taken to ensure system protection.
Security Procedures	Security procedures define exactly how security practices and policies are implemented and executed. They are implemented through personnel training and actions using currently available and installed technology (such as disconnecting modems). Procedures and contained criteria also include more technology-dependent system requirements that need careful analysis, design, planning, and coordinated installation and implementation.
Security Program	A security program brings together all aspects of managing security, ranging from the definition and communication of guidelines through implementation of best industry practices and ongoing operation and auditing.
Security Requirements	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a control system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, control system owners, and system security officers.
Server	A device or computer system that is dedicated to providing specific facilities to other devices attached to the network.
Server Farm	A cluster of networked servers generally housed in the same location used to perform computationally intense functions by distributing the workload.
Session	Layer 5 of OSI. (ISA definition of OSI: Abbreviation for open system interconnection [a connection between one communication system and another using a standard protocol]. OSI reference model, Layer 5—Session: provides user-to-user connections.)
Shall	Equivalent to "is required to" and used to indicate mandatory requirements strictly to be followed to conform to the standard and from which no deviation is permitted.
Should	Equivalent to "is recommended that" and used to indicate several possibilities recommended as particularly suitable, without mentioning or excluding other, that a certain course of action is preferred but not required, that (in the negative form) a certain course of action is deprecated but not prohibited.
Six-wall border	This refers to a physical, completely enclosed border such as a room, cage, safe or metal cabinet. Raised floors and drop ceilings may not constitute part of a border because they could create potentially uncontrolled access points.

Term	Definition
Software	A set of programs, procedures, rules, and possibly associated documentation concerned with the operation of a computer system compilers, library routines, manuals, circuit diagrams.
Spam	Unsolicited and often unwanted e-mail.
Specifications	An assessment object that includes document-related artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with a control system.
Spyware	Software that is secretly or surreptitiously installed into a control system to gather information on individuals or organizations without their knowledge.
Standard	A reference established by authority, custom, or general consent as a model or example. For the purposes of the U.S. Chemicals Sector Cyber Security Strategy, a standard is considered a voluntary practice or guideline that is established by consensus of the industry.
Supervisory Control	A term used to imply that a controller output or computer program output is used as an input to other controllers, e.g., generation of setpoints in cascaded control systems. Used to distinguish from direct digital control.
Supervisory Control and Data Acquisition (SCADA)	A computer control system used in real time to monitor and control one or more remote facilities. The system collects data and/or sends control instructions, either automatically or by operators at other locations. SCADA is used to control facilities in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.
Supply Chain Protection	A supply chain is a system of organizations, people activities, information, and resources that provides products and/or services to consumers. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those informational systems.
Switch	A network device that interconnects devices and creates separate paths for communication.
System	An assembly of procedures, processes, methods, routines, or techniques united by some form of regulated interaction to form an organized whole. An assemblage of equipment, machines, or control devices, interconnected mechanically, hydraulically, pneumatically or electrically, and intended to act together to perform a predetermined function. A combination of generation, transmission, and distribution components.
System Security Plan	Formal document that provides an overview of the security requirements for the control system and describes the security mechanisms in place or planned for meeting those requirements.
System Software	The special software within the cryptographic boundary (e.g., operating system, compilers, or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.
Technical Measures	The security mechanisms (i.e., safeguards or countermeasures) for a control system that are primarily implemented and executed by the control system through mechanisms contained in the hardware, software, or firmware components of the system.

Term	Definition
Thin Nodes	Information system that employs processing components that have minimal functionality and data storage.
Third Party	Refers to vendors, support personnel, other companies.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), assets, or individuals through a control system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat source to successfully exploit control system vulnerabilities.
Threat Source	The intent and method targeted at the intentional exploitation of vulnerabilities or a situation and method that may accidentally trigger a specific vulnerability. Synonymous with term threat agent.
Trustworthiness	Defined in degrees of correctness for intended functionality and the degree of resilience to attach by explicitly identified levels of adversary capability. This is defined on different levels on a basis of component-by-component, subsystem-by-subsystem, function-by-function or a combination.
Unauthorized Disclosure	An event involving the exposure of information to entities not authorized access to the information.
User	Individual or (system) process authorized to access a control system.
Utility	A generic term that, when qualified, identifies the business entity including all its operating and business functions; e.g., electric utility, gas utility, water utility, wastewater utility, pipeline utility. Any general-purpose computer program included in an operating system to perform common functions. Any of the systems in a process plant, manufacturing facility not directly involved in production; may include any or all the following – steam, water, refrigeration, heating, compressed air, electric power, instrumentation, waste treatment, and effluent systems.
Virtual Private Network	A network that is constructed by using public wires to connect nodes. For example, a number of systems enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
Vulnerability Analysis	The identification of the ways in which assailants may attack a facility to cause harm. It can include qualitative risk analysis.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in a control system.

5. DOCUMENTS REFERENCED

The following documents and tools were reviewed or referenced in the preparation of this catalog. Some of these documents are still in draft stage or do not apply directly to control systems. Other references are not standards, but very informative guidelines or implementation guidance documents containing timely and useful information for improving the security of ICSs. An attempt has been made to organize these references with respect to the DHS critical Infrastructure sectors. Some of the references listed below may be proprietary, designed for licensed in-house usage, and may be obtained via purchase or specific individual request. All the documents listed below are listed for user awareness. The contents of proprietary/licensed documents are not used in this document unless expressed written permission of the originator/publisher was received. Several documents such as the multiple NIST Publications, DHS publications, NERC documents, and various open source documents are freely available; and some of the content was included in the creation of this document.

General:

American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.01-2007), Security Technologies for Manufacturing and Control Systems, 2007. http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9665

American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.02-2004), Integrating Electronic Security into the Manufacturing and Control Systems Environment, April 12, 2004. http://www.isa.org/Template.cfm?Section=Find_Standards&Template=/Customsource/ISA/Standards/TaggedStandardsCommittee.cfm&id=4296

Department of Homeland Security, National Cyber Security Division, Control System Security Program, Cyber Security Evaluation Tool, Release 3.0. http://www.us-cert.gov/control_systems/pdf/CSET_fact_sheet.pdf

Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules,” issued May 25, 2001, updated December 03, 2002. FIPS-140-3 is a DRAFT Security Requirements for Cryptographic Modules and is still in draft form. FIPS 140-2 also contains the following four annexes:

A – January 4, 2011, Draft “Approved Security Functions for FIPS Pub 140-2”

B – June 14, 2007, Draft “Approved Protection Profiles for FIPS PUB 140-2”

C – November 24, 2010, Draft “Approved Random Number Generators for FIPS PUB 140-2”

D – January 4, 2011, Draft “Approved Key Establishment Techniques for FIPS PUB 140-2.”

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Federal Information Processing Standards Publication 180-3, “Secure Hash Standards,” issued October 2008. http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

Federal Information Processing Standards Publication 198-1, “The Keyed-Hash Message Authentication Code (HMAS),” issued July 2008. http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

International Electrotechnical Commission 62351-1, “Data and Communication Security,” Committee Draft Version 1, April 2005.

International Electrotechnical Commission 62443-2-1, "Industrial Communication Networks – Network and System Security":

Part 1-1: "Terminology, concepts and models," July 2009

Part 2-1: "Establishing an industrial automation and control system security program," November 2010

Part 3-1: "Security technologies for industrial automation and control systems," July 2009

Part 3-3: "

http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/43215

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=62443&Pa=2&Se=1&Am=&Fr=&TR=&Ed=1"

International Organization for Standardization 17799, "Code of Practice for Information Security Management," June 10, 2005. (Note: This document has been superseded by ISO/IEC 27002:2005, Stage 90.92, April 2008.)

International Organization for Standardization 27001, "Information Security Management Systems Requirements," October 14, 2005.

International Society of Automation Society Standards Committee, ANSI/ISA-99.00.01-2007, "Manufacturing and Control Systems Security Part 1: Concepts, Models and Terminology," October 29, 2007.

International Society of Automation Standards Committee, ANSI/ISA-99.02.01-2009, "Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program," January 13, 2009.

National Institute of Standards and Technology Special Publication 800-48, "Wireless Network Security 802.1, Bluetooth and Handheld Devices," Revision 1, September 2008. http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," Revision 3 Final, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Institute of Standards and Technology Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," Final Public Draft, September 2008. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

National Institute of Standards and Technology Special Publication 800-127, "Guide to Securing WiMAX Wireless Communications," September 2010. http://csrc.nist.gov/publications/nistpubs/800-127/sp800-127.pdf

"Twenty Critical Controls for Effective Cyber Defense: Consensus Audit," Version 2.3, November 13, 2009. http://www.sans.org/critical-security-controls/print.php http://www.sans.org/whatworks/20-critical-controls-poster-122010.pdf

WIB, "Process Control Domain-Security Requirements for Vendors: Plant Security," second issue, M2784-X-10, Version 2.0, Evaluation International (EI), WIB and EXERA, October 2010. http://www.wib.nl/

Chemical:

Chemical Information Technology Council (ChemITC), Guidance for Cyber Security in Chemistry, Version 4.0, November 2009.

Department of Homeland Security – Office of Infrastructure Protection – Infrastructure Security Compliance Division – "Risk-Based Performance Standards Guidance (RBPS)– Chemical Facility Anti-Terrorism Standards," Version 2.4 May 2009. http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

Electric Power:

Institute of Electrical and Electronics Engineers 1402, "Guide for Electric Power Substation Physical and Electronic Security," January 30, 2000.

National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Volume 1, Smart Grid Cyber Security Strategy, Architeture, and High-Level Requirements," August 2010. http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Volume 2, Privacy and the Smart Grid," August 2010. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Volume 3, Smart Grid Cyber Security: Supportive Analyses and References," August 2010. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-3 through CIP 009-3), Approved by Board of Trustees: December 16, 2009. http://www.nerc.com/page.php?cid=2%7C20

North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-4 through CIP 009-4), approved draft (Phase II), which involves the more complex FERC directives. These drafts have not yet been submitted to the NERC Board of Trustees for approval at the time of writing.

North American Electric Reliability Council, Security Guidelines for the Electricity Sector, Version 1.0, June 14, 2002.

Gas:

American Gas Association, "Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan (AGA 12, Part 1)," March 14, 2006.

American Gas Association, "Cryptographic Protection of SCADA Communications Part 2: Retrofit link encryption for asynchronous serial communications (AGA 12, Part 2)," March 31, 2006.

Nuclear:

Department of Energy DOE O 205.1A "Department of Energy Cyber Security Management," December 4, 2006. http://cio.energy.gov/policy-guidance/doe_policies.htm

Department of Energy DOE M 205.1-4, "National Security System Manual," March 8, 2007. http://cio.energy.gov/policy-guidance/doe_policies.html

Department of Energy DOE M 205.1-5, "Cyber Security Process Requirements Manual."

Department of Energy DOE M 205.1-6, "Media Sanitization Manual," December 23, 2008.

Department of Energy DOE M 205.1-7, "Security Controls for Unclassified Information Systems Manual," January 5, 2009.

Department of Energy DOE M 205.1-8, “Cyber Security Incident Management Manual,” January 8, 2009.

Nuclear Energy Institute “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09, Revision 6, April 2010.

U.S. Nuclear Regulatory Commission – Regulatory Guide 5.71 “Cyber Security Programs for Nuclear Facilities,” January 2010. http://nrc-stp.ornl.gov/slo/regguide571.pdf

Oil and Petroleum:

American Petroleum Institute, “API 1164: Pipeline SCADA Security, Second Edition,” June 2009.

American Petroleum Institute, “Security Guidelines for the Petroleum Industry,” April 2005.

Transportation:

American Public Transit Association “Securing Control and Communications Systems in Transit Environments – Part 1: Elements, Organization and Risk Assessment/Management,” APTA RP-CCS-1-RT-001-10, July 2010.

Department of Transportation – Federal Transit Administration - 49 CFR, Part 659, Rail Fixed Guideway Systems; State Safety Oversight, April 2005 – This document authorizes 26 individual states authorization to implement and manage 43 separate rail transit agencies. http://transit-safety.fta.dot.gov/Publications/order/singledoc.asp?docid=603

Appendix A

Cross Reference of Standards

This cross reference mapping loosely correlates the requirements and guidance contained in the referenced source documents against the recommendations in the Catalog of Control Systems Security. This correlation depicts a general relationship between multiple documents in multiple industrial sectors. The cross reference cannot imply an exact matching between specific requirement details and multiple controls currently existing, but strives to implicitly address and associate specific controls across several standards and guidance documents.

The source documents in the cross reference are constantly evolving to address new and expanded understanding of security topics. Previous source documents have been deleted from this document as they are no longer relevant, or have been superseded by newer documents. This crosswalk attempts to use the most recent update of the source documents available at the time of publication, but availability, publishing and timing may result in older versions of source documents being referenced and used. Furthermore, it is not possible to determine the priority and baseline risk for each control family in every industrial facility and control system deployment.

Two reference sources were removed from the cross reference at this time. They are: (1) ChemITC—"Guidance for Addressing Cybersecurity in the Chemical Sector, Version 3.0; Chemical Sector Cyber Security Program May 2006"; This document has been superseded by "Guidance for Addressing Cyber Security in the Chemical Industry, Version 4, November 2009," and has not yet been reviewed; and (2) "NERC Security Guidelines—Security Guidelines for the Electricity Sector, Version 1.0 May 3, 2005," has been superseded by the NERC Critical Infrastructure Protection (CIP) reliability standards.

Two new additional reference sources were added at this time. They are (1) "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)," Version 2.3 November 13, 2009, and (2) U.S. Nuclear Regulatory Commission—Regulatory Guide 5.71—"Cyber Security Programs for Nuclear Facilities," January 2010. These two sources were added, as they are the latest cybersecurity standards released and provide a very good basis in industrial cybersecurity. The CAG, for instance, is broken down into four categories within each of the 20 critical controls. The first category is label "QW," which denotes a "quick win," action that will immediately improve the security posture, especially if addressed by the user. The second category is "Improved Visibility and Attribution," meant to increase monitoring, visibility and attribution, so organizations can better monitor network and computer systems. The third category is "Hardened Configuration and Improved Information Security Hygiene," and focuses on protecting against poor security practices by system administrators and end users. The final category is "Advanced" and identifies actions and items that further improve security beyond the other three categories. The CAG also lists functional/effectiveness testing to see how and if security functions are working. The NRC RG 5.71 takes elements from NIST SP 800-53 r3 and NIST SP 800-82 and focuses on how to use these elements in the operation of nuclear reactors. Most ICSs share similar layout, function and security. Three appendixes are in NRC 5.71. Appendix A is a generic Cyber Security Plan template for utilities to use. Appendix B contains Technical Security Controls, while Appendix C consists of Operational and Management Security Controls. The unique method on which roles, configuration, what to test, how to test, and periodic retesting provides an element lacking in current cybersecurity standards and guidelines.

The cross reference is accurate at the time of the most recent update. The reader is encouraged to confirm the currency, accuracy, and applicability of the source documents and obtain current copies of all pertinent source documents as necessary. The versions of the documents used in the cross reference are listed below:

AGA 12-1	Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan, Draft 5, April 14, 2005.
AGA 12-2	Cryptographic Protection of SCADA Communications Part 2: Retrofit Link Encryption for Asynchronous Serial Communications, March 31, 2006.
FIPS 140-2	Security Requirements for Cryptographic Modules, issued May 25, 2001, updated December 3, 2002.
API 1164	Pipeline SCADA Security, Second Edition, June 2009.
API Security Guidelines	Security Guidelines for the Petroleum Industry, April 2005.
CAG	Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines, Version 2.3 November 13, 2009.
ChemITC	Guidance for Cyber Security in Chemistry, Version 4, November 2009.
ISO 17799	Information Technology—Security Techniques—Code of Practice for Information Security Management, Second Edition, 2005-06-15, superseded by ISO 27002.
ISO 27001	Information Technology—Security Techniques—Information Security Management Systems—Requirements, First Edition, October 15, 2005.
IEC 62351	Data and Communications Security—Introduction, Committee Draft Version 1, April 2005.
IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security, January 30, 2000.
ISA 99-1	Manufacturing and Control Systems Security, Part 1: Models and Terminology, Draft 1, Edit, February 8, 2005.
ISA99-2	Manufacturing and Control System Security, Part 2: Establishing a Manufacturing and Control System Security Program, Draft 1, Edit 1, April 15, 2005.
NERC CIP	Cyber Security, 002-3 to 009-3: Approved by Board of Trustees: December 16, 2009.
NIST SP 800-53R3	NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009.
RG 5.71	U.S. Nuclear Regulatory Commission – Regulatory Guide 5.71 – "Cyber Security Programs for Nuclear Facilities", January 2010.

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.1.1	Security Policy and Procedures	X	—	X	X	X	X	X	X	—	—	X	X	X	X	X
2.2.1	Management Policy and Procedures	—	—	—	X	X	—	X	X	—	—	X	X	X	X	X
2.2.2	Management Accountability	X	—	—	X	X	—	X	X	—	—	X	X	—	X	X
2.2.3	Baseline Practices	—	—	—	X	X	—	X	X	—	—	X	X	X	X	X
2.2.4	Coordination of Threat Mitigation	—	—	—	X	X	—	X	—	—	—	—	X	—	X	X
2.2.5	Security Policies for Third Parties	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.2.6	Termination of Third-Party Access	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.1	Personnel Security Policy and Procedures	—	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.3.2	Position Categorization	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.3.3	Personnel Screening	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.3.4	Personnel Termination	X	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.5	Personnel Transfer	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.6	Access Agreements	—	—	X	X	—	—	X	—	—	—	—	X	X	—	X
2.3.7	Third-Party Personnel Security	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.3.8	Personnel Accountability	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.3.9	Personnel Roles	—	—	—	X	X	—	X	—	—	X	—	X	X	X	X
2.4.1	Physical and Environmental Security Policy and Procedures	X	—	X	X	X	—	X	—	—	X	—	X	X	X	X
2.4.2	Physical Access Authorizations	—	—	X	X	—	—	X	—	—	X	—	X	X	X	X
2.4.3	Physical Access Control	—	—	—	X	X	—	X	—	—	X	—	X	X	X	X
2.4.4	Monitoring Physical Access	—	—	—	X	X	—	X	—	X	X	—	X	X	X	X
2.4.5	Visitor Control	—	—	—	X	X	—	X	—	—	X	—	—	X	X	X
2.4.6	Visitor Records		—	—	X	X	—	X	—	—	—	—	—	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.4.7	Physical Access Log Retention	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.4.8	Emergency Shutoff	—	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.4.9	Emergency Power	—	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.4.10	Emergency Lighting	—	—	—	X	X	—	X	—	—	—	—	X	X	—	X
2.4.11	Fire Protection		—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.4.12	Temperature and Humidity Controls	—	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.4.13	Water Damage Protection	—	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.4.14	Delivery and Removal	—	—	—	—	—	—	X	—	—	—	—	X	—	—	X
2.4.15	Alternate Work Site	—	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.4.16	Portable Media	X	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.4.17	Personnel and Asset Tracking	—	—	—	—	—	—	X	—	—	—	—	X	X	—	—
2.4.18	Location of Control System Assets	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.4.19	Information Leakage	—	—	—	X	X	—	X	X	—	—	—	—	X	—	X
2.4.20	Power Equipment and Power Cabling	—	—	—	X	—	—	—	—	—	—	X	—	X	—	X
2.4.21	Physical Device Access Control	X	—	X	X	X	—	—	—	—	—	X	—	X		X
2.5.1	System and Services Acquisition Policy and Procedures	—	—	—	X	X	X	X	X	—	—	—	—	X	—	X
2.5.2	Allocation of Resources	X	—	—	X	—	—	X	X	—	—	—	—	X	—	X
2.5.3	Life-Cycle Support	—	—	—	—		X	—	—	—	—	—	—	X	—	X
2.5.4	Acquisitions	—	—	X	—	—	X	X	—	—	—	—	—	X	—	X
2.5.5	Control System Documentation	X	—	X	X	—	—	X	X	—	—	—	—	X	X	X
2.5.6	Software License Usage Restrictions	—	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.5.7	User-Installed Software	X	—	—	X	X	X	X	—	—	—	—	—	X	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.5.8	Security Engineering Principles	X	—	—	X	X	X	X	X	—	—	—	—	X	—	X
2.5.9	Outsourced Control System Services	—	—	—	X	X	—	X	—	—	—	—	—	X	—	X
2.5.10	Developer Configuration Management	X	—	X	X	X	X	—	—	—	—	—	—	X	—	X
2.5.11	Developer Security Testing	—	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.5.12	Supply Chain Protection	X	—	X	—	X	—	X	—	—	—	—	—	X	—	X
2.5.13	Trustworthiness	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.5.14	Critical Information System Components	X	—	X	X	—	—	X	—	—	—	X	X	X		X
2.6.1	Configuration Management Policy and Procedures	X	—	X	X	—	X	X	—	—	—	X	X	X	X	X
2.6.2	Baseline Configuration	X	—	X	X	—	X	—	—	—	—	—	—	X	X	X
2.6.3	Configuration Change Control	X	—	X	X	—	X	X	—	—	—	X	X	X	X	X
2.6.4	Monitoring Configuration Changes	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.6.5	Access Restrictions for Configuration Change	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.6.6	Configuration Settings	—	—	—	—	X	X	X	—	—	—	—	X	X	X	X
2.6.7	Configuration for Least Functionality	—	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.6.8	Configuration Assets	—	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.6.9	Addition, Removal, and Disposal of Equipment	—	—	—	—	—	X	X	—	—	—	—	X	X	X	—

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.6.10	Factory Default Authentication Management	—	—	X	X	—	X	X	—	—	—	—	X	X	X	X
2.6.11	Configuration Management Plan	—	—	—	X	—	—	—	—	—	—	—	—	X	X	X
2.7.1	Strategic Planning Policy and Procedures	—	—	—	—	X	—	X	X	—	X	—	X	X	X	X
2.7.2	Control System Security Plan	X	—	—	X	X	—	X	X	—	X	—	X	X	X	X
2.7.3	Interruption Identification and Classification	—	—	—	—	X	X	X	X	—	—	—	X	X	X	X
2.7.4	Roles and Responsibilities	X	—	—	X	X	X	X	X	—	X	—	X	X	X	X
2.7.5	Planning Process Training	X	—	—	X	X	X	X	X	—	—	X	X	X	X	X
2.7.6	Testing	X	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.7.7	Investigation and Analysis	—	—	—	X	X	—	X	X	—	—	—	X	X		X
2.7.8	Corrective Action	—	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.7.9	Risk Mitigation	—	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.7.10	System Security Plan Update	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.7.11	Rules of Behavior	—	—	X	X	X	—	X	—	—	—	—	X	X	X	X
2.7.12	Security-Related Activity Planning	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.8.1	System and Communication Protection Policy and Procedures	X	—	X	X	X	—	X	—	—	—	—	X	X	X	X
2.8.2	Management Port Partitioning	X	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.8.3	Security Function Isolation	—	—	X	X	—	X	X	—	—	—	—	—	X	X	X
2.8.4	Information in Shared Resources	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.8.5	Denial-of-Service Protection	—	X	—	X	X	—	—	—	X	—	—	X	X	—	X
2.8.6	Resource Priority	X	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.8.7	Boundary Protection	—	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.8.8	Communication Integrity	X	—	—	X	X	—	X	—	—	—	—	—	X	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.8.9	Communication Confidentiality	X	—	X	X	X	X	X	—	—	—	—	X	X	—	X
2.8.10	Trusted Path	X	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.8.11	Cryptographic Key Establishment and Management	X	—	X	—	—	—	X	—	—	—	—	—	X	—	X
2.8.12	Use of Validated Cryptography	X	—	X	—	—	X	X	—	—	—	—	—	X	—	X
2.8.13	Collaborative Computing Devices	—	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.8.14	Transmission of Security	X	—	—		—	—	X	—	—	—	—	—	X	—	X
2.8.15	Public Key Infrastructure Certificates	X	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.8.16	Mobile Code	—	—	—	—	—	X	X	—	—	—	—	—	X	—	X
2.8.17	Voice-Over Internet Protocol	—	—	—	X	—	—	—	—	—	—	—	—	—	—	X
2.8.18	System Connections	X	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.8.19	Security Roles	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.8.20	Session Authenticity	X	—	—	X	—	—	X	X	X	—	X	—	X	—	X
2.8.21	Architecture and Provisioning for Name/Address Resolution Service	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.22	Secure Name/Address Resolution Service (Authoritative Source)	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.24	Fail in Known State	—	—	—	—	—	X	—	—	—	—	—	—	X	—	X
2.8.25	Thin Nodes	—	—	—		—	—	—	—	—	—	—	—	X	—	X
2.8.26	Honeypots	—	—	—	—	—	X	—	—	—	—	—	—	—	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.8.27	Operating System-Independent Applications	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.8.28	Confidentiality of Information at Rest	—	—	—	X	—	X	—	—	—	—	—	—	X	—	X
2.8.29	Heterogeneity	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.8.30	Virtualization Techniques	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X
2.8.31	Covert Channel Analysis	—	—	—	—	—	X	—	—	—	—	—	—	—	—	X
2.8.32	Information System Partitioning	—	—	—	X	—	—	X	—	—	—	—	X	X		X
2.8.33	Transmission Preparation Integrity	—	—	—	—	X	—	X	—	—	—	—	X	X		X
2.8.34	Non-Modifiable Executable Programs	—	—	—	X	—	—	X	—	—	—	—	X	—	—	X
2.9.1	Information and Document Management Policy and Procedures	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.9.2	Information and Document Retention	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.9.3	Information Handling	X	—	—	X	—	—	X	X	—	—	—	X	X	X	X
2.9.4	Information Classification	X	—	X	X	X	X	X	—	—	—	—	X	X	X	X
2.9.5	Information Exchange	X	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.9.6	Information and Document Classification	X	—	X	X	—	X	X	—	—	—	—	X	X	X	X
2.9.7	Information and Document Retrieval	X	—	—	X	—	—	X	X	—	—	—	X	X	—	X
2.9.8	Information and Document Destruction	X	—	—	X	—	—	X	X	—	—	—	X	X	—	—
2.9.9	Information and Document Management Review	X	—	—	X	—	—	X	—	—	—	—	X	X	X	—

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.9.10	Media Marking	—	—	—	X	—	X	—	—	—	—	—	—	X	—	X
2.9.11	Security Attributes	—	—	—	—	—	—	—	—	—	—	—	—	X	—	X
2.10.1	System Maintenance Policy and Procedures	X	—	X	X	—	—	X	X	—	X	—	X	X	X	X
2.10.2	Legacy System Upgrades	X	—	X	X	—	X	—	—	—	—	—	X	X		X
2.10.3	System Monitoring and Evaluation	X	—	X	X	X	X	X	—	—	—	X	X	X	X	X
2.10.4	Backup and Recovery	X	—	X	X	X	X	X	—	—	—	X	X	X	X	X
2.10.5	Unplanned System Maintenance	X	—	—	X	—	—	X	—	—	—	X	X	X		—
2.10.6	Periodic System Maintenance	X	—	—	—	—	—	X	—	—	—	—	X	X	—	X
2.10.7	Maintenance Tools	X	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.10.8	Maintenance Personnel	—	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.10.9	Non-Local (Remote) Maintenance	—	—	X	X	—	—	X	—	—	—	X		X	—	X
2.10.10	Timely Maintenance	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.11.1	Security Awareness and Training Policy and Procedures	—	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.11.2	Security Awareness	X	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.11.3	Security Training	—	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.11.4	Security Training Records	—	—	X	X	—	—	—	X	—	—	—	X	X	X	X
2.11.5	Contact with Security Groups and Associations	X	—	X	X	X	—	X	—	—	—	—	—	X	X	X
2.11.6	Security Responsibility Testing	—	—	—	X	X	—	—	X	—	—	—	X	X	—	—
2.12.1	Incident Response Policy and Procedures	X	—	—	X	X	X	X	X	—	X	—	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.12.2	Continuity of Operations Plan	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.12.3	Continuity of Operations Roles and Responsibilities	—	—	X	X	X	—	X	X	—	—	—	X	X	X	X
2.12.4	Incident Response Training	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.12.5	Continuity of Operations Plan Testing	—	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.12.6	Continuity of Operations Plan Update	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.12.7	Incident Handling	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.12.8	Incident Monitoring	—	—	—	X	X	X	X	X	—	—	—	—	X	X	X
2.12.9	Incident Reporting	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.12.10	Incident Response Assistance	—	—	—	—	X	—	X	—	—	—	—	—	X		X
2.12.11	Incident Response	—	—	—	X	—	—	X	X	—	—	—	X	X	X	X
2.12.12	Corrective Action	X	—	—	X	X	—	X	X	—	—	—	X	X	X	X
2.12.13	Alternate Storage Sites	—	—	—	X	—	—	X	—	—	—	—	X	X	X	X
2.12.14	Alternate Command/Control Methods	—	—	—	X	X	—	X	—	—	X	—	X	X	—	X
2.12.15	Alternate Control Center	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.12.16	Control System Backup	—	—	—	X	X	X	—	—	—	—	—	X	X	X	X
2.12.17	Control System Recovery and Reconstitution	—	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.12.18	Fail-Safe Response	—	—	—	X	—	—	—	—	—	—	—	—	—	—	—
2.13.1	Media Protection Policy and Procedures	X	—	—	X	—	—	—	X	—	—	—	—	X	X	X
2.13.2	Media Access	—	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.13.3	Media Classification	—	—	—	X	X	X	X	X	—	—	—	—	X	X	X
2.13.4	Media	—	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.13.5	Media Storage	—	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.13.6	Media Transport	—	—	—	—	—	—	X	X	—	—	—	—	X	—	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.13.7	Media Sanitization and Disposal	X	—	—	X	—	—	X	X	—	—	—	—	X	X	X
2.14.1	System and Information Integrity Policy and Procedures	—	—	—	—	X	—	—	X	—	—	—	—	X	X	X
2.14.2	Flaw Remediation	—	—	—	X	X	—	X	X	—	—	—	—	X	X	X
2.14.3	Malicious Code Protection	X	—	—	X	X	X	X	—	—	—	—	—	X	X	X
2.14.4	System Monitoring Tools and Techniques	X	—	—	X	—	X	X	—	—	—	—	—	X	X	X
2.14.5	Security Alerts and Advisories and Directives	X	—	—	X	X	—	X	—	—	—	—	—	X	X	X
2.14.6	Security Functionality Verification	—	X	X	X	—	—	X	—	—	—	—	—	X	—	X
2.14.7	Software and Information Integrity	—	X	X	X	—	X	X	—	—	—	—	—	X	—	X
2.14.8	Spam Protection	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.14.9	Information Input Restrictions	—	—	—	X	X	—	X	—	—	—	—	—	X	X	X
2.14.10	Information Input	—	—	—	X	—	X	X	—	—	—	—	—	X	—	X
2.14.11	Error Handling	—	X	—	X	—	—	X	—	—	—	—	—	X	—	X
2.14.12	Information Output Handling and Retention	—	—	—	X	X	—	X	X	—	—	—	—	X	X	X
2.14.13	Predictable Failure Prevention	—	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.15.1	Access Control Policy and Procedures	X	—	X	X	X	X	X	X	—	X	—	X	X	X	X
2.15.2	Identification and Authentication Policy and Procedures	X	X	X	—	X	—	X	X	—	X	—	X	X	X	X
2.15.3	Account Management	X	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.15.4	Identifier Management	X	—	X	X	X	—	X	—	—	—	—	X	X	X	X
2.15.5	Authenticator Management	—	—	X	X	—	X	X	—	—	—	—	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.15.6	Account Review	X	—	X	X	—	X	X	X	—	—	—	X	X	X	X
2.15.7	Access Enforcement	X	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.15.8	Separation of Duties	X	—	X	X	—	—	X	—	—	—	—	X	X	X	X
2.15.9	Least Privilege	X	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.15.10	User Identification and Authentication	X	—	—	X	X	X	X	—	—	—	—	X	X	X	X
2.15.11	Permitted Actions without Identification or Authentication	—	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.15.12	Device Identification and Authentication	—	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.15.13	Authenticator Feedback	—	—	X	X	—	—	X	—	—	—	—	—	X	X	X
2.15.14	Cryptographic Module Authentication	X	—	X	X	—	—	X	—	—	—	—	—	X	—	X
2.15.15	Information Flow Enforcement	—	—	X	X	—	X	X	—	—	—	—	—	X	X	X
2.15.16	Passwords	X	—	X	X	—	X	X	—	—	—	—	X	X	X	X
2.15.17	System Use Notification	—	—	—	X	—	—	X	—	—	—	—	—	X	X	X
2.15.18	Concurrent Session Control	X	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.15.19	Previous Logon (Access) Notification	—	—	—	—	—	—	X	—	—	—	—	—	X	—	X
2.15.20	Unsuccessful Login Attempts	—	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.15.21	Session Lock	—	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.15.22	Remote Session Termination	X	—	—	X	—	—	X	—	—	—	—	—	X	—	X
2.15.23	Remote Access Policy and Procedures	X	—	—	X	X	—	X	—	—	—	—	X	X	X	X
2.15.24	Remote Access	X	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.15.25	Access Control for Mobile Devices	—	—	—	X	X	X	X	—	—	—	—	X	X	—	X
2.15.26	Wireless Access Restrictions	X	—	—	X	—	X	X	—	—	—	—	—	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.15.27	Personally Owned Information	—	—	—	X	—	X	—	—	—	—	—	—	X	—	X
2.15.28	External Access Protections	—	—	—	X	X	X	X	—	—	—	—	—	X	X	X
2.15.29	Use of External Information Control Systems	X	X	—	X	X	X	—	—	—	—	—	X	X	X	X
2.15.30	User-Based Collaboration and Information Sharing	X	X	—	X	—	—	—	—	—	—	—	X	—	X	X
2.15.31	Publicly Accessible Content	X	X	—	X	—	—	—	—	—	—	—	X	X	X	X
2.16.1	Audit and Accountability Policy and Procedures	X	—	X	X	X	—	X	X	—	X	—	X	X	X	X
2.16.2	Auditable Events	X	—	X	X	X	X	X	—	—	—	—	—	X	X	X
2.16.3	Content of Audit Records	X	—	X	X	—	X	X	—	—	—	—	—	X	X	X
2.16.4	Audit Storage Capacity	—	—	—	—	—	X	X	—	—	—	—	—	X	—	X
2.16.5	Response to Audit Processing Failures	—	—	—		—	X	X	—	—	—	—	—	X	X	X
2.16.6	Audit Monitoring, Analysis, and Reporting	X	—	X	X	X	X	X	X	—	—	—	—	X	X	X
2.16.7	Audit Reduction and Report Generation	X	—	X	X	—	X	X	X	—	—	—	—	X	X	X
2.16.8	Time Stamps	—	—	—	—	—	X	X	—	—	—	—	—	X	X	X
2.16.9	Protection of Audit Information	X	—	—	X	—	X	X	X	—	—	—	—	X	X	X
2.16.10	Audit Record Retention	X	—	—	X	—	—	X	X	—	—	—	—	X	X	X
2.16.11	Conduct and Frequency of Audits	X	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.16.12	Auditor Qualification	—	—	—	X	—	X	—	—	—	—	—	X	X	—	X
2.16.13	Audit Tools	X	—	—	X	—	—	X	—	—	—	—	X	X	—	X
2.16.14	Security Policy Compliance	—	—	—	X	—	—	X	X	—	—	—	—	X	X	X
2.16.15	Audit Generation	—	—	—	—	—	—	—	—	—	—	—	—	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.16.16	Monitoring for Information Disclosure	—	—	—	—	—	—	—	—	—	—	—	—	—	X	X
2.16.17	Session Audit	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.17.1	Monitoring and Reviewing Control System Security Management Policy and Procedures	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.17.2	Continuous Improvement	—	—	—	X	—	X	X	X	—	—	X	X	X	X	X
2.17.3	Monitoring of Security Policy	—	—	—	X	—	X	—	X	—	—	—	X	X	X	X
2.17.4	Best Practices	—	—	—	X	X	X	—	X	—	—	—	X	X	X	X
2.17.5	Security Accreditation	X	—	—	X	—	—	—	—	—	—	—	—	X	—	X
2.17.6	Security Certification	X	—	—	X	X	—	—	X	—	—	—	—	—	—	X
2.18.1	Risk Assessment Policy and Procedures	X	—	—	X	X	—	X	X	—	X	X	X	X	X	X
2.18.2	Risk Management Plan	X	—	—	X	X	X	X	X	—	X	—	X	X	X	X
2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	X	—	—	X	X	—	X	—	—	X	—	X	X	—	X
2.18.4	Security Assessments	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.18.5	Control System Connections	—	—	—	X	X	X	X	—	—	—	—	—	—	X	X
2.18.6	Plan of Action and Milestones	—	—	—	X	X	—	—	X	—	—	—	X	—	X	X
2.18.7	Continuous Monitoring	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X
2.18.8	Security Categorization	—	—	—	X	—	X	X	—	—	—	—	X	—	X	X
2.18.9	Risk Assessment	—	—	—	X	X	X	X	X	—	X	X	X	X	X	X
2.18.10	Risk Assessment Update	—	—	—	X	X	X	X	X	—	—	—	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164, 2nd Edition	API Security Guidelines 3rd Edition	20 Critical Controls	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NRC Reg Guide 5.71	NERC CIP-rev -3	NIST SP800-53 Rev. 3
2.18.11	Vulnerability Assessment and Awareness	—	—	—	X	—	X	X	—	—	—	—	X	X	X	X
2.18.12	Identify, Classify, Prioritize, and Analyze Potential Security Risks	—	—	—	X	—	X	—	—	—	—	—	—	X	X	X
2.19.1	Information Security Program Plan	—	—	—	X	—	—	—	—	—	—	—	—	X	X	X
2.19.2	Senior Information Security Officer	—	—	—	X	—	—	—	—	—	—	—	—	X	X	X
2.19.3	Information Security Resources	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.4	Plan of Action and Milestones Process	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.5	Information System Inventory	—	—	—	X	—	X	—	—	—	—	—	—	X	X	X
2.19.6	Information Security Measures of Performance	—	—	—	X	—	X	—	—	—	—	—	—	—	X	X
2.19.7	Enterprise Architecture	—	—	—	X	—	X	—	—	—	—	—	—	—	X	X
2.19.8	Critical Infrastructure Plan	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.9	Risk Management Strategy	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.10	Security Authorization Process	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X
2.19.11	Mission/Business Process Definition	—	—	—	X	—	—	—	—	—	—	—	—	—	X	X

Appendix M

MANTECA AWWA REFERENCES

Sec. 4.6 Access Control and Intrusion Detection

4.6.1 *Identify utility assets requiring access control.* Through the risk assessment or other means, the utility shall identify assets or facilities that require controlled access based on criticality to maintain normal operations (identified critical assets).

4.6.2 *Establish and maintain physical control of access to identified critical assets.* The utility shall establish and maintain a means of physically controlling access to identified critical assets. Examples of physical access controls include the following and can be used individually or in combination:

- Substantial buildings with intrusion prevention devices on windows and access points
- Fences
- Barriers
- Locked gates, hatches, and doors
- Monitored intrusion alarms
- Tamper-resistant devices at key distribution or collection points

4.6.3 *Implement annual inspections of identified critical assets.* The utility shall implement and maintain annual inspections to assure that security features are adequate and functioning, and to identify if any corrective work is necessary to maintain access control or other security features.

4.6.4 *Establish and maintain a means of detecting and assessing intrusion.* The utility shall establish and maintain a means of detecting and assessing intrusion into identified critical assets by unauthorized persons in a manner that is timely and enables the utility to respond effectively. Monitoring for physical intrusion can include physical and procedural improvements. Examples of physical improvements include installing detection devices such as motion detectors and intrusion alarms, or improved assessment tools such as well-lighted facility perimeters, or monitoring with closed-circuit TV (CCTV). Procedural improvements include the use of neighborhood watches, regular employee rounds, or arrangements with the local police or fire department to help identify and report unusual activity.

4.6.5 *Establish and maintain procedures to control personnel access to identified critical assets.* The utility shall establish and maintain procedural controls to limit access to identified critical assets to authorized persons only. Examples of procedural access controls include the following and can be used individually or in combination:

- Inventory and control keys
- Develop procedure that limits access rights to employees to maximum extent possible
- Develop hierarchical key and/or access card system to limit access to extent possible
- Change access codes regularly
- Require security passes for access
- Establish a security presence at access points
- Require visitors to have scheduled appointments, and/or have a protocol to address unscheduled visitors
- Require employees and other authorized persons to display identification at all times when on-site, if appropriate
- Require visitors to sign in and display identification at all times when on-site
- Implement chemical delivery and testing procedures including chain-of-custody control or tamper-evident packaging requirements
- Limit delivery hours
- Check deliveries to ascertain the nature of the material

4.6.6 *Establish and maintain a means of restricting authorization for access.* The utility shall establish and maintain a means of restricting unescorted access to identified critical assets.

4.6.6.1 Background checks. Where legally permissible and appropriate, the utility shall institute a system of background checks on employees, contractors, temporary workers, or any other person authorized to access identified assets without an escort. The level or complexity of background checks used should be commensurate with the level of access and the privileges granted to the person. Other benefits of background checks, depending on the level employed, may include verifying identity, establishing citizenship, determining previous criminal activity, and determining work eligibility.

4.6.6.2 Other means of identity verification. When background checks are not permitted or appropriate, the utility shall establish a defined alternative method of verifying identity and granting access rights and privileges to a person seeking authorization.

4.6.7 *Establish a protocol for employees or others who have been terminated, have resigned, or have had a relevant change of status.* The utility shall establish and maintain a protocol to recover keys, revise passwords, and take other appropriate actions immediately on termination, resignation or re-assignment of an employee or the relevant change of status of other personnel who have access to high-risk assets. Other personnel may include vendors, consultants, contractors, public officials, or others who had been granted appropriate access and are no longer performing a relevant function.

4.6.8 *Testing.* The utility shall test physical and procedural access controls routinely to ensure performance. The tests shall be conducted annually, or more frequently if required by law or regulation.

Sec. 4.11 Emergency Response and Recovery Plans and Business Continuity Plan

4.11.1 *Incorporate security into emergency response and recovery plans, business continuity plans, and operations.*

4.11.1.1 Update plans. The utility shall revise its emergency response and recovery plans and business continuity plans as necessary to incorporate security considerations into the plans. Additional guidance is provided in ANSI/AWWA G440 and *Business Continuity Planning for Water Utilities** (Water RF 2008).

4.11.1.2 Emergency response. The utility shall comply with the National Incident Management System (NIMS) guidelines, and use Incident Command System (ICS) protocol for emergency response.

4.11.2 *Test emergency response and recovery plans and business continuity plans regularly.* The utility shall establish and maintain a schedule for testing its emergency response and recovery plans and business continuity plans. Testing may include training, tabletop exercises or drills, or real-time simulated responses.

4.11.3 *Update emergency response and recovery plans and business continuity plans as necessary.*

4.11.3.1 Review and update. The utility shall perform a timely review and update its emergency response and recovery plans and business continuity plans as necessary to correct identified deficiencies after exercises or actual implementation (lessons learned) in accordance with ANSI/AWWA G440.

4.11.3.2 Routine reviews. The utility shall perform a timely review and update of its emergency response and recovery plans and business continuity plans routinely and as necessary to reflect relevant changes in potential threats, physical infrastructure, utility operations, critical interdependencies, or response protocols in partner organizations. In no event shall the interval exceed five years, but the review and update can be more frequent if required by law or regulation.

4.11.3.3 The utility should consider participating in a mutual aid and assistance agreement. The utility should consider participating in a mutual aid and assistance agreement with local, regional, and state utilities, as appropriate, to expedite response and recovery of service. This may include, but not be limited to, joining the state Water and Wastewater Agency Response Network (WARN), if applicable.

4.11.4 *Contact list.* The utility shall establish, maintain current, and distribute a list of contacts to include key employees and key contacts for critical customers and support organizations. This list shall include names, phone numbers, and other information necessary to establish contact with those persons or designated alternates during an emergency.

4.11.5 *Response to contamination threat.* The emergency plan shall have a procedure for responding to potential contamination events or threats, which includes reporting out, field verification, credibility assessments, site sampling, lab qualification, lab analysis, and public notification.

4.11.6 *Protection of public health.* The utility must be prepared to consider contamination evidence carefully and make public health decisions with incomplete data and analysis.

Appendix N

AWWA CYBERSECURITY RISK AND RESPONSIBILITY

REPORT
American Water Works Association
Dedicated to the World's Most Important Resource®

CYBERSECURITY RISK & RESPONSIBILITY IN THE WATER SECTOR

Prepared by Judith H. Germano

Contents

ACKNOWLEDGEMENTS

Judith H. Germano is a Professor and Distinguished Fellow at the NYU Center for Cybersecurity, teaching incident response, cybercrime and emerging threats in NYU's Masters in Cybersecurity Risk and Strategy executive education degree program, and is an Adjunct Professor of Law at NYU School of Law. Judith is the founder of GermanoLaw LLC, advising organizations and corporate boards on cybersecurity, data privacy, fraud and regulatory compliance issues. Judith is the former Chief of Economic Crimes at the U.S. Attorney's Office for the District of New Jersey; a federal prosecutor for 11 years, Judith has handled matters of cybercrime, identity theft, securities and other financial fraud, political corruption and national security.

AWWA would like to thank multiple reviewers including Mike Hooker, Robert Walters, Patrick Norton, John Lucas, and Jaimie Foreman.

Project Funding

This project was funded by the American Water Works Association (AWWA), utilizing Water Industry Technical Action Fund (WITAF), as WITAF Project #030 and managed by Kevin M. Morley.

Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

EXECUTIVE SUMMARY

Cybersecurity is a top priority for the water and wastewater sector. Entities, and the senior individuals who run them, must devote considerable attention and resources to cybersecurity preparedness and response, from both a technical and governance perspective. **Cyber risk is the top threat** facing business and critical infrastructure in the United States. Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data. Managing cybersecurity is a complex challenge that requires an interdisciplinary, risk-based approach, involving an organization's business leaders, as well as their technical and legal advisors.

A robust and tested cybersecurity program is critical to protect public health and safety, prevent service disruptions, and safeguard customer and employee personal and financial information. Inadequate cybersecurity measures and flawed responses to cybersecurity incidents carry tremendous risk. In addition to serious threats to people, property, operations and data, cybersecurity incidents also can result in potential civil and regulatory liability, and reputational harm. ***Attacks will happen; do not be caught unprepared.***

Despite sector challenges, it is critically important to bolster cybersecurity protocols and defenses. Getting cybersecurity "right" is not an easy issue. Threats are persistent and mutable. The diverse nature of the water and wastewater sector, with organizations of varying size and ownership, the sector's splintered regulatory regime, and a lack of cybersecurity governance protocols, present significant cybersecurity challenges.

Moreover, entities within the sector often face insufficient financial, human and technological resources. Many organizations have limited budgets, aging computer systems, and personnel who may lack the knowledge and experience for building robust cybersecurity defenses and responding effectively to cyber attacks.

Despite these challenges, organizations – on their own and with outside technical and legal experts as needed -- must develop a plan and give sufficiently rigorous attention to cybersecurity. An optimistic reliance on sovereign immunity defenses or insurance policies, or an unconfirmed expectation that someone else within the organization is "handling" cybersecurity issues, are not sufficient to protect an organization or its leaders from the repercussions of a cybersecurity attack and the related reputational harm.

There are scalable and effective measures that water sector members – individually and collectively – can take to improve the cybersecurity of their organizations, and of the sector as a whole. Given the very real threat and significant consequences of a cyber attack, it is critical that organizations prioritize cybersecurity and take reasonable steps to prevent, detect and respond to cyber incidents.

CYBER RISK: A TOP THREAT, CYBERSECURITY: A TOP PRIORITY

Significant Risk

Cyber risk is the top threat facing business and critical infrastructure in the United States, according to the Director of National Intelligence, the Federal Bureau of Investigation and the Department of Homeland Security.[1] A survey of more than 20,000 utility employees revealed that cyber threats are what they fear could have the biggest impact on operations, with a lack of resources and conflicting priorities as the greatest challenges.[2] Water and Wastewater Sector (referred to collectively here as "water sector") entities have suffered a range of attacks, including from ransomware attacks, tampering with Industrial Control Systems, manipulating valve and flow operations and chemical treatment formulations, and other efforts to disrupt and potentially destroy operations. In March and April 2018, the U.S. Department of Homeland Security and Federal Bureau of Investigation warned that the Russian government is specifically targeting the water sector and other critical infrastructure sectors as part of a multi-stage intrusion campaign.[3] Attacks for financial, political and terroristic gain are a serious concern.

The effects of a cybersecurity attack on critical water sector operations could cause devastating harm to public health and safety, threaten national security and result in costly recovery and remediation efforts to address system issues as well as data loss. Attacks causing contamination, operational malfunction, and service outages could result in illness and casualties, compromise emergency response by firefighters and healthcare workers, and negatively impact transportation systems and food supply. Water sector entities also are responsible for protecting sensitive personal information, including employee records and customer billing data. This personal information is an attractive target for cybercriminals and the stolen data business continues to grow. Indeed, the U.S. had 16.7 million identity fraud victims in 2017, with $16.8 billion stolen from U.S. consumers through identity fraud.[4]

Examples of confirmed water sector attacks include, among others:

- City of Atlanta ransomware attack. The City of Atlanta was crippled by a ransomware attack in March 2018, which disrupted city utilities, courts and other operations.[5] For roughly a week, employees with the Atlanta Department of Watershed Management were unable to turn on their work computers or gain wireless internet access, and two weeks after the attack Atlanta completely took down its water department website "for server maintenance and updates until further notice."[6] It has taken Atlanta months, and estimated costs of up

[1] https://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx.

[2] BRIDGE Energy Group, 2018 BRIDGE Index™ Utility Industry Grid Operations Survey, Jan. 9, 2018, https://www.bridgeenergygroup.com/news/press/bridge-energy-groups-2018-utility-industry-survey-grid-operations/.

[3] U.S. Department of Homeland Security (DHS), US-CERT, Alert (TA18-074A), *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, March 15, 2018, revised, March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A; U.S. DHS, US-CERT, Alert (TA18-106A), *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*, April 16, 2018, revised, April 20, 2018, https://www.us-cert.gov/ncas/alerts/TA18-106A.

[4] Javelin Strategy and Research, 2018 Identity Fraud Study, February 6, 2018, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

[5] https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

[6] "https://www.reuters.com/article/us-usa-cyber-atlanta-water/atlanta-takes-down-water-department-website-two-weeks-after-cyber-attack-idUSKCN1HC2WB.

to $5 million in recovery efforts, to address the attack.[7] (While the Atlanta attack focused primarily on public-facing operations, the Colorado Department of Transportation was hit with a sequence of ransomware attacks on its back-office systems, costing approximately $1 to $1.5 million to address.[8])

- Ransomware attack on a water utility effected through spear-phishing. An employee clicked on a malicious email link that caused malware to download. Cybercriminals gained access through an Internet-facing commercial network and locked the utility out of its own systems, demanding the equivalent of $25,000 in Bitcoin to recover access.[9] Replacing the infected computers and software cost $10 million, and full remediation costs (including paying the ransomware in this instance) were approximately $2.4 million, $500,000 of which was not covered by insurance.[10] This attack underscores the importance of resiliency and redundancy of systems, malware detection and prevention, and employee training, as well as the importance of having cyber-insurance in place.

- Attack on Industrial Control System (ICS) of a water and sewage authority. Cybercriminals exploited a vulnerability in a remote wireless Internet connection for operations for approximately two months, and also exploited a hard-coded factory password.[11] This attack underscored the importance of staying current with vendor patches and firmware updates, and regularly (if not continuously) scanning networks for intruders. It also highlights a common developer flaw of hard-coded passwords, which should be avoided if possible; if the password is for the initial default account, that account should be deleted after the set-up.[12]

- In one water utility attack, cybercriminals exploited antiquated computer systems to gain access to valve and flow operations and were able to manipulate the water flow and amount of chemicals used to treat the water. Cybercriminals also accessed customer data via the company's online payment system, through which the attackers gained administrator credentials and maneuvered laterally through the network.[13]

- In the well-publicized Bowman Dam hack, Iranian activists exploited a vulnerability to identify an unprotected computer that controlled sluice gates and other functions of the dam. The hactivists detected the vulnerability through "Google Dorking," a process of performing advance Google searches to detect vulnerabilities. At the time of the attack, the gate was manually disconnected for maintenance, which helped avoid more serious harm. Remediation costs for the dam exceeded $30,000, and the hackers were charged in a

[7] https://www.ajc.com/news/local/atlanta-network-almost-recovered-from-cyber-attack-cost-still-unkown/k6srGim85Q8dKwUFPbcDhN/.

[8] https://statescoop.com/colorado-has-spent-more-than-1-million-bailing-out-from-ransomware-attack.

[9] https://thehackernews.com/2016/04/power-ransomware-attack.html.

[10] https://www.freep.com/story/news/local/michigan/2016/11/09/bwl-paid-ransom-cyberattack/93576218/.

[11] *See, e.g.,* https://www.csoonline.com/article/3038302/application-development/hard-coded-passwords-remain-a-key-security-flaw.html.

[12] *See* Id.

[13] *See* Verizon's Data Breach Digest (2016) p. 39-42.

criminal indictment.[14] The relatively simple way the hackers discovered the significant vulnerability underscores the importance of regular security assessments and penetration testing of systems, networks and applications.

In a March 2018 technical alert, DHS and FBI warned of "a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS)." The alert warns the water sector also is a target of this Russian government attack effort.

Based on the DHS alert, the threat actors for this campaign employed a variety of tactics, techniques and procedures, including: spear-phishing emails (from a compromised, legitimate account); watering-hole domains; credential gathering; open-source and network reconnaissance; host-based exploitation; and targeting industrial control system (ICS) infrastructure. *Spear Phishing* are attacks targeting specific individuals, in this case by sending emails personalized to the recipient that are (or appear to be) from a legitimate account and usually entice the recipient to click on a link that injects malware onto their systems. Spear phishing emails currently are the most prevalent method for delivering advanced persistent threat (APT) attacks -- 84% of organizations have said a spear-phishing attack successfully penetrated their organization in 2015, with an average impact of $1.6 million per attack.[15] Those numbers have continued to increase.[16] *Watering Hole Domain Attacks* are where attackers discern websites a target group regularly uses (such as for trade organizations and information websites), and infect one or more of those websites with malware, usually aimed at collecting information and credentials of the user. *Credential Gathering* is a highly valuable attack because it enables attackers to use those credentials to gain access to the target systems and navigate within the system for recognizance and, potentially, to wreak havoc.

According to the DHS and FBI, the Russian attackers leveraged compromised credentials to access victims' networks ***where multi-factor authentication was not used***. *Multi-factor authentication* is an important step for adding another layer of security by requiring more than one piece of evidence (such as a security key sent to a second device) to gain access to an account and, as the National Standards of Industry and Technology (NIST) advocates, should be used whenever possible.[17]

In addition to the March 2018 warning, in April 16, 2018, the DHS warned of a Russian government campaign to exploit infrastructure devices critical to utility operations in the water and other sectors.

[14] DOJ press release, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

[15] FireEye, *Spear-Phishing Attacks: Why They Are Successful and How to Stop Them*, https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf.

[16] *See, e.g.,* "Why 2017's Phishing Attacks Teach Us All to Beware," InfoSecurity Magazine, September 20, 2017, https://www.infosecurity-magazine.com/opinions/why-2017-phishing-attacks-teach/.

[17] https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.

DHS noted that the infrastructure network devices are often public facing and operating without sufficient security, thereby making them easy targets.[18] Factors increasing the vulnerability include:

- Insufficient antivirus, integrity-maintenance and other security tools, particularly for network devices used by small businesses and operating on residential-class routers;
- Manufacturers build and distribute the devices with exploitable services to make them easier to install, operate and maintain;
- Failure to change vendor default settings, enhance security and regularly patch systems and software;
- Failure to remove or update antiquated or outdated equipment that is no longer being supported by the manufacturer or vendor; and
- Overlooking network devices when assessing risk or recovering from a cyber intrusion.[19]

Foreseeability Mandates Due Diligence and Reasonable Efforts

Cybersecurity risks – whether in the form of technical mistakes, cyber-crime, espionage, "hacktivism", terrorism or warfare -- continue to increase. One study reported that *every sixty seconds* cyber-crime costs more than $1.1 million and impacts more than 1,800 people.[20] Phishing attacks (22.9 per minute) and ransomware (victimizing 1.5 companies per minute) top the vulnerabilities list.[21] After the December 2015 attacks that shut down Ukraine's power grid, the U.S. government warned American power companies, water suppliers and transportation networks that the same methods of attack could be used against them.[22]

Technical and procedural security measures can help protect against many cyber threats. For example, phishing attacks can be reduced by teaching employees not to click on questionable links, and to have better filters that block or flag external, or suspicious, emails. The harm from ransomware attacks can be minimized with adequate system redundancies, tested backups and diligent updates and patches to block certain vulnerabilities. *Also, given that perhaps close to 90 percent of attacks are caused by human error or behavior,*[23] *it is essential to increase cybersecurity awareness, education, training and best practices within an organization*.

[18] U.S. Department of Homeland Security (DHS), US-CERT, Alert (TA18-074A), *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, March 15, 2018, revised, March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A;

[19] Id. See also AWWA Utility Advisory, April 19, 2018 (summarizing the technical alert). http://social.bluehornet.com/hostedemail/email.htm?CID=38807374598&ch=B16C42F0EC4155D2BC94F867B6B1EC9D&h=6aeaa7c9c5c035bd55305248f17efb17&ei=Tso1WTu1N&schema=echo4.

[20] RiskIQ Evil Internet Minute 2.0 (2018) report, *available at* https://www.riskiq.com/infographic/evil-internet-minute-2018/ (also discussed at, e.g., https://www.pcmag.com/news/363217/more-than-1-1m-lost-to-cybercrime-every-minute).

[21] Id.

[22] David Sanger, "Utilities Cautioned About Potential for a Cyberattack After Ukraine's," New York Times, Feb. 29, 2016, *available at* https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html.

[23] Ross Kelly, "Almost 90% of Cyber Attacks are Caused by Human Error or Behavior, Chief Executive, March 3, 2017, *available* at https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/.

While the *legal* determination of whether a particular incident was "foreseeable" might be disputed on a case-by-case basis[24], it is well established that public and private entities that fail to anticipate and prepare for a diverse set of cyber threats face a very real threat of civil and regulatory liability when incidents do happen. Courts and regulators – as well as the public, impacting reputational harm – are increasingly demanding that entities employ due diligence and reasonable measures to prevent, detect and respond to cyber risk. Cyber attacks have filled news headlines, there have been numerous warnings for critical infrastructure generally and the water sector in particular, and it is necessary to expect that your organization will be targeted. (It is now over-used but no less true: for cyberattacks, "it is not a question of *if* but *when*," and the answer may be the hackers already are in your systems and you do not know it.)

There are numerous examples of organizations facing multi-million dollar penalties for failing to employ reasonable measures to prevent, detect and respond to cyber threats. In one class action lawsuit, against an employer following a phishing scheme that compromised sensitive W-2 data of employees and their families, a federal district court in California stated: *[I]t is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently. Castillo v. Seagate Tech., LLC,* No. 16 Civ. 1958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016). The employer subsequently paid $5.75 million to settle that lawsuit.[25] In a similar case, a New York federal court recently quoted *Castillo* and added: *Employers have a duty to take reasonable precautions to protect the PII that they require from employees. Sackin, et al. v. TransPerfect Global Inc.*, Case No. 1:17-cv-1469-LGS (S.D.N.Y.).[26] Also, in *FTC v. Wyndham Worldwide Corp.*, the U.S. Court of Appeals for the Third Circuit found that unreasonable data security would constitute "unfair and deceptive practices" under Article 5 of the FTC Act, 15 U.S.C., §45(a), and recognized that the Federal Trade Commission had authority to bring a civil regulatory action. 799 F.3d 236 (3d Cir. 2015). The Third Circuit found that Wyndham had "fair notice" of its potential liability for failing to employ "reasonable" data security measures. *Id.*

Thus, even if you are not certain exactly when or how your organization will suffer a cyber attack, it is critical to accept the reality that some type of cyber risk is at least foreseeable, perhaps inevitable. The reality and prevalence of cyber risk mandates that organizations and their leaders not only take meaningful action to prevent and detect harms, but also have a tested plan for responding swiftly and effectively when cyber incidents do occur. Failing to address cybersecurity risk in a proactive way can have devastating results.

Failing to take reasonable measures and employ best practices to prevent, detect, and swiftly respond to cyber-attacks means that organizations and the people who run them will face greater damage – including technical, operational, financial and reputational harm – when the cyber-attacks do occur.

[24] For a legal discussion regarding the sometimes-elusive concept of "foreseeability" in civil tort (including negligence) actions, *see, e.g.*, David Owen, *Figuring Foreseeability*, 44 Wake Forest L. Rev. 1277 (2009), *available at* https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1937&context=law_facpub.

[25] *Castillo,* Order Granting Mot. For Final Approval of Class Action Settlement, etc., Docket No. 85 (March 14, 2018), *available at* https://secure.dahladmin.com/SEAGAT/content/documents/OrderGrantingFinalApprovalofSettlement.pdf.

[26] *Available at* https://www.leagle.com/decision/infdco20171005i57.

Beyond Technical Risk: Reputational, Regulatory and Civil Liability Costs

In addition to technical damage and outages from a breach, an entity that fails to adequately protect its systems, operations, and customer data also faces the risk of reputational harm, as well as regulatory enforcement, criminal penalties and civil liability costs. Proposed legislation has even been introduced to impose *criminal* penalties for failing to timely disclose data breaches. The Data Security and Breach Notification Act, proposed in November 2017, sought to impose jail time for executives who actively conceal data breaches.[27] (That law was proposed on the heels of the Uber data breach disclosure, which involved the theft of data on 57 million customers; Uber paid the hackers $100,000 to destroy the stolen data, classified it as a "bug bounty payment,"[28] and failed to report the breach to regulators or the public for more than a year.)

Corporate executives and government officials have been called to testify before congress, been criticized in the media, and have lost their jobs as a result of how they prepared, or failed to prepare, for and respond to cybersecurity incidents.[29] The reputational damage to entities and individuals, and the cost of recovering from a poorly handled cyber incident response are significant and long lasting.

A robust approach to cybersecurity will help prevent cyber incidents, enable a far better response to incidents that do happen, and provide a far better explanation of preparedness and response when confronted by customers, constituents, investors, boards, regulators, civil litigants, legislators, and the media.

Examples of corporate executives and government officials who have lost their jobs as a result of cybersecurity breaches include, among others, the:

- General Counsel at Yahoo, after a state-sponsored hack and delayed disclosures;
- Director General of the Swedish Transport Agency and also the Minister of the Interior who lost his place in the Swedish Cabinet, after unauthorized access to the vehicle registration and drivers license database by third-party contractor IBM;
- CEO and CFO of Austrian aerospace company FACC, after a business email compromise (though this was not confirmed as the sole cause of termination);
- CEO of Sony Pictures, after a nation-state hack exposed corporate emails;
- CSO and also the Legal Director of Security and Enforcement of Uber, after paying $100,000 to hackers and failing to disclose a major data breach for more than a year;

[27] *See* Larson, Sandra, "Senators Introduce Data Breach Disclosure Bill," CNN Tech, Dec. 1, 2017, *available at* https://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html.

[28] Bug bounty programs, a way to crowdsource vulnerability testing, offer recognition and compensation to security researchers who report vulnerabilities and exploits to the organization so the problems can be fixed before becoming known to the general public. Many public and private sector organizations use bug bounty programs, including the U.S. Department of Defense, Pentagon, Google, Microsoft, Facebook, United Airlines and others. An increasing number of state governments also are considering adopting bug bounty programs. Bergal, Jenni, "White-Hat Hackers to the Rescue, Government Technology, May 14, 2018, *available at* http://www.govtech.com/security/White-Hat-Hackers-to-the-Rescue.html.

[29] https://www.csoonline.com/article/3158825/it-jobs/how-to-get-fired-in-2017-have-a-security-breach.html.

- CEO, CSO and also the CIO of Equifax, after a major breach impacting more than 143 million Americans;

- CEO and certain board members of Target, after a major retail breach that occurred when Target's third-party heating and air conditioning vendor was compromised.[30]

Also, the Federal Trade Commission (FTC) has brought more than 60 cases against companies for failing to have "reasonable" or "industry standard" cybersecurity practices, defenses and responses.[31] The Securities and Exchange Commission, Department of Health and Human Services, banking regulators, and many states have also imposed fines and brought lawsuits against entities that failed to protect consumer data. In addition, private civil litigants and states attorneys general have obtained millions of dollars in settlements and penalties related to cybersecurity breaches.[32]

Government Actors: Sovereign Immunity May Not Protect You

Although principles of sovereign immunity may prevent, or at least hinder, civil actions against government actors, many government entities have nonetheless paid millions in settlements related to cybersecurity breaches. Sovereign immunity, a legal concept that protects federal and state governments from liability in many situations, also has exceptions as determined by statute. **Moreover, defending these lawsuits, and addressing the numerous other harms and costs that result from mishandled cybersecurity incidents (impacts on systems, data, operations, reputations and perhaps even personal safety) can be far more costly, distracting and damaging than taking a proactive approach to cybersecurity.**

If property damage, injury or death occur due to negligence or a wrongful act, claims may be allowed pursuant to the Federal Tort Claims Act (FTCA),[33] and comparable state laws that specifically waive immunity under those circumstances.[34]

Also, the Administrative Procedure Act (APA) governs internal procedures of administrative agencies, including how they interact with the public, and provides that final agency decisions are subject to judicial review.[35] The APA includes the federal Privacy Act (FPA), which governs how U.S. federal government agencies collect, maintain, use and disseminate personally identifiable information about individuals. The FPA includes a waiver of immunity where there is a (1) willful, intentional and improper disclosure of personal information that results in (2) actual harm.[36] As with the FTCA, many states also

[30] https://www.csoonline.com/article/2859485/data-breach/the-buck-stops-here-8-security-breaches-that-got-someone-fired.html#slide1.

[31] https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (page 4-5).

[32] https://www.f5.com/labs/articles/cisotociso/breach-costs-are-rising-with-the-prevalence-of-lawsuits.

[33] Title 28, United States Code, Sections 1346(b), 2671-2680.

[34] https://www.mwl-law.com/wp-content/uploads/2013/03/MUNICIPAL-COUNTY-LOCAL-GOVERNMENTAL-LIABILITY-CHART-00212510.pdf.

[35] Title 5, United States Code, Sections 551-559.

[36] Title 5, United States Code, Section 552a.

have comparable statutes to the APA and FPA.[37] (As discussed below, plaintiffs suing the Office of Personnel Management (OPM) for that massive data breach relied upon the APA and FPA.)

Examples where government entities have paid millions in settlements related to cybersecurity breaches impacting personal information include:

- Mille Lacs County in Minnesota paid $1 million to settle a class-action lawsuit after an employee allegedly accessed driver's license records of 379 residents without authorization.[38] The county fired the employee and, as required, notified the impacted individuals. In the lawsuit, plaintiffs alleged that the county had insufficient policies and "failed to put into place systems and/or procedures to ensure … class members' private data would be protected and would not be subject to misuse."
- Three years earlier, Rock County, Minnesota, paid $2 million for a breach where a county employee improperly searched the same database.[39]
- Maricopa County Community College in Arizona paid $26 million to settle a lawsuit and pay fees and costs to address a breach where hackers compromised multiple databases and stole personal information of two million employees, students and prospective students.
- Skagit County, Washington, paid $215,000 in fines imposed by the U.S. Department of Health and Human Services (HHS) for inadvertently uploading protected health information of more than 1500 people to a county public server. As part of the settlement, the county was required to draft written protocols, implement new policies and train all employees, as well as follow new reporting requirements. HHS said this case was a call to all local governments "to adopt a meaningful compliance program to ensure the privacy and security of Patients' information."

Where an entity hosts its own services and software it more likely would be held responsible for a compromise than if it contracts the hosting to a reputable third party or using cloud-based services. The breach of Superion's *Click2Gov* system potentially exposed tens of thousands of customers of local government, including many utility customers, in a number of states including California, Florida, Texas, Arizona and Wisconsin.[40] The *Click2Gov* system is used by hundreds of local governments for payment processing as well as other services, such as permit applications. Hackers apparently placed a digital card skimmer on top of Click2Gov code, compromising networks in certain towns and cities that locally hosted the software; notably, Superion's data centers and cloud-based services were not compromised. This creates questions of liability based on the governments' failure to implement proper security upgrades and monitoring, and whether Superion should have played a more proactive role.

Some lawsuits have been dismissed where a court finds plaintiffs have not shown the necessary level of harm from a breach or, where applicable, plaintiffs have failed to overcome sovereign immunity defenses. A federal district court judge in September 2017 dismissed the civil lawsuits brought, based on laws including the APA and FPA, against the Office of Personnel Management (OPM) for the

[37] See, e.g., http://www.uniformlaws.org/ActSummary.aspx?title=State%20Administrative%20Procedure%20Act,%20Revised%20Model.
[38] http://www.governing.com/gov-institute/voices/col-cybersecurity-data-breach-government-liability.html.
[39] Id.
[40] http://www.govtech.com/security/Thousands-Exposed-in-Municipal-Website-Breaches.html

breaches, disclosed in 2015 and attributed to a Chinese intelligence operation, which exposed highly sensitive security clearance information of more than 20 million people.[41] The court stated that there was insufficient evidence the individuals were actually harmed by the breach that exposed, among other information, details regarding finances, romantic relationships, substance abuse and some current, former and prospective government employees' fingerprints.

OPM officials had failed to encrypt highly sensitive data, did not fix known flaws in its systems and disregarded warnings from the OPM Inspector General that certain systems failed to meet cybersecurity standards. The court, however, also noted the plaintiffs had failed to establish that OPM was not protected by sovereign immunity.[42] Plaintiffs have appealed that decision, meaning litigation costs continue to increase, as the law regarding liability for cyber breaches continues to develop.

CHALLENGES TO MANAGING CYBER RISK

For many utilities and other public infrastructure entities, the resources and capabilities for preventing, detecting and mitigating cyber risk fall short, particularly given the significance of the threat and potential harm. Challenges to managing cyber risk in the water sector are organizational, physical and technological. The water sector presents diverse challenges due to its varying drinking water and wastewater infrastructure, and the fact it is comprised of entities of vastly different sizes, capabilities, resources and types of ownership. Multiple governing authorities, on a federal and state level, oversee water and wastewater concerns regarding public health, environmental protection and security, among others.[43] Fractured organizational structure, often embedded within a multifaceted municipality, shared infrastructure with different levels of risk, and a prevalence of legacy -- sometimes antiquated -- systems increase the challenges of managing cyber risk. Some of these challenges are not unique to the water sector; according to the Brookings Institute, the vast majority of public agencies lack a clear cybersecurity plan.[44]

Large organizations often say it is hard to defend against cyber attacks due to their size and multi-faceted systems, underscored by the concern that one point of compromise across a global network with thousands of employees could cause harm. Smaller organizations often claim inadequate financial and personnel resources, and lack of the time and knowledge, needed to address cybersecurity issues. In either case, where to start and how best to prioritize cybersecurity defenses are challenging. Regardless of the size of the entity, executives, managers and boards are haunted by (or at least should be asking) key questions, including:

[41] *In re: U.S. Office of Personnel Management Data Security Breach Litig.*, Misc. Action No. 15-1394, MDL Docket No. 2664, Mem. Op. dated Sept. 19, 2017, *avail. at* https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2015mc1394-117.

[42] https://www.mwl-law.com/wp-content/uploads/2013/03/MUNICIPAL-COUNTY-LOCAL-GOVERNMENTAL-LIABILITY-CHART-00212510.pdf.

[43] DHS and EPA Water and Wastewater Systems Sector-Specific Plan, 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

[44] https://www.brookings.edu/blog/techtank/2015/02/03/the-vast-majority-of-the-government-lacks-clear-cybersecurity-plans/.

- Have we identified and adequately secured our critical data and systems?
- Are we doing enough to anticipate threats and prevent, detect and quickly respond to cyber attacks?
- Have we done a recent risk assessment and developed a plan to address known risks?
- Are we ensuring patches are up to date and employing encryption and access limitations?
- Are we addressing vulnerabilities caused by legacy, or outdated systems, and working with vendors to develop a priority-based plan, timeline and budget for adopting cybersecurity upgrades (and, if necessary, overhauls) to improve cybersecurity?
- Will we have a good explanation to give our clients, constituents, customers, regulators and shareholders when attacks do happen?

Water sector utility owners and operators tend to be advanced in emergency response and resilience planning based on their preparations for natural disasters; similar redundancy and recovery methods and structures to ensure continuity of operations and protect public health and the environment also must be applied in the cybersecurity context.[45] Although replacing legacy systems and networks can be extremely costly, it is essential to work with vendors and cybersecurity experts to implement updates and, if necessary, overhauls of outdated systems. Invoke the help of internal or external advisors to prioritize risk and develop a realistic approach and plan for enhancing cybersecurity. At a minimum, comply with basic standards including restricted physical and technical access, firewalls, logging and encryption.

When it comes to cybersecurity, how much is enough? How much is needed to spend on cybersecurity defenses and personnel? How much time, effort and resources should be focused on cybersecurity governance? How much is sensible to insure against cyber risk and to adequately protect systems, data and assets? How much regulation is helpful to increase smart cybersecurity, without unduly diverting resources to check-the-box compliance efforts, or quelling innovation and new technologies? These are not easy questions to answer, so that leads to another question: Is there a way to make this all easier, or at least less overwhelming for organizations of varying sizes?

[45] *See* DHS and EPA Water and Wastewater Systems Sector-Specific Plan, 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

STANDARDS, GUIDANCE, REGULATION AND INSURANCE

Standards, guidance, regulation and insurance are available to help water sector entities address cybersecurity issues and develop comprehensive cybersecurity policies, programs and procedures.

Standards, Guidance and Regulation

Standards, toolkits and regulatory mandates help guide water sector entities regarding cybersecurity defenses and requirements addressing technological, physical and personal considerations. A discussion of the water sector's regulatory authorities and critical infrastructure partners is provided in the DHS and U.S. Environmental Protection Agency (USEPA) Water and Wastewater Systems Sector-Specific Plan (SSP), including a list of authorities in Appendix 2 and list of Critical Infrastructure Partners in Appendix 3 of the SSP.[46]

For more specific guidance in building and enhancing a cybersecurity program and plan, resources developed by the National Institute of Standards and Technology and the American Water Works Association (AWWA) are particularly helpful.

NIST Framework & Publications

A key and especially helpful cybersecurity resource is the National Institute of Standards and Technology (NIST) framework. This is a voluntary set of standards, guidelines and best practices to manage cybersecurity related risk.[47] As NIST states, the "Cybersecurity Framework's prioritized, flexible and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."[48] On April 16, 2018, NIST published a newer Version 1.1 of the Framework, which is fully compatible with Version 1; it includes additional guidance on identity management and supply chain cybersecurity.[49] NIST also provides additional guidance, including through special publications (SPs) and webinars, including SP800, on computer security, SP1800 on cybersecurity practice guides, and SP500 on computer systems technology.

AWWA Guidance & Use-Case Tool

The AWWA provides *Process Control System Security Guidance for the Water Sector* and a supporting Use-Case Tool that also is very helpful for establishing and improving cybersecurity systems specific to operations technology (OT) but can also inform enterprise security practices. The Water Sector Coordinating Council, the USEPA and NIST have recognized the AWWA Guidance and Use-Tool as the foundation of a voluntary, sector-specific approach to implementing the NIST Cybersecurity

[46] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf. Also, the Water Sector ISAC published a "Roadmap to a Secure and Resilient Water and Wastewater Sector," May 2017, which address cyber risk management, https://www.waterisac.org/sites/default/files/public/2017_CIPAC_Water_Sector_Roadmap_FINAL_051217.pdf.

[47] https://www.nist.gov/cyberframework.

[48] Id.

[49] Id.

Framework.[50] The *Process Control System Security Guidance for the Water Sector* identifies 12 cybersecurity "practice categories," and recommends specific, critical practices under each category that direct map water-specific application to the NIST Cybersecurity Framework.

In an effort to provide water utilities with actionable tasks, the Use-Case Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user selects from a series of pre-defined use cases that represents the type of functions their process control system may perform. The Use-Case Tool places emphasis on actionable recommendations with the highest priority assigned to those that will have the most impact in the short term. It should be noted, that the tool does not assess the extent to which a utility has implemented any of the recommended controls.

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA), while specific to "covered entities" and "business associates" providing medical services or handling personal health information, provides a HIPAA Security Rule that can provide helpful cybersecurity guidance event to non-HIPAA regulated entities.[51] Regardless of whether your organization must comply with HIPAA, the HIPAA Security Rule "provides a clear, jargon-free framework for developing information security policies and programs" and can help municipalities and other water sector owners and operators build a solid foundation for cybersecurity programs.[52] In particular, as Jeffrey Morgan notes in a *CIO.com* article,[53] the final six pages of the HIPAA Security Rule, includes a helpful matrix on required actions for administrative, physical and technical cybersecurity safeguards.

State and Federal Regulation

Certain states have enacted regulations or provided guidance to address and prioritize cybersecurity in the water sector. For example, on July 21, 2017, New Jersey enacted the Water Quality Accountability Act (WQAA, effective as of October 19, 2017), which established new requirements designed to improve the safety, reliability and administrative oversight of the water infrastructure.[54] The Act applies to public water systems with more than 500 service connections -- approximately 300 water systems in New Jersey.[55] The New Jersey WQAA requires covered water system operators to inspect, maintain, repair and update their infrastructure consisting with AWWA standards, and requires water system operators with internet connected control systems to create cybersecurity programs and join the NJ

[50] https://www.awwa.org/cybersecurity.

[51] HIPAA Security Rule, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

[52] Morgan, Jeffrey, CIO.com, *County and Municipal Cybersecurity, Part 2*, April 3, 2017, https://www.cio.com/article/3186510/government-use-of-it/county-and-municipal-cybersecurity-part-2.html.

[53] See HIPAA Security Rule, cited above; *see also*, Morgan, Jeffrey, CIO.com, *HIPAA as an Umbrella for County/Municipal Cybersecurity,* https://www.cio.com/article/3188667/governance/hipaa-as-an-umbrella-for-countymunicipal-cybersecurity.html.

[54] New Jersey Statutes Annotated, 58:31-1, *et seq.*, available at http://www.njleg.state.nj.us/2016/Bills/PL17/133_.PDF.

[55] http://www.nj.gov/dep/watersupply/g_reg-wqaa.html.

Cybersecurity and Communications Integration Cell, designed to foster better collaboration and improved cybersecurity defenses.[56]

New York Public Health Law requires water suppliers to develop and submit emergency plans that, among other things, include "a vulnerability analysis assessment, including an analysis of vulnerability to terrorist attack and cyber attack, which shall be made after consultation with local and state law enforcement agencies."[57]

Connecticut's Public Utilities Regulatory Authority (PURA) set forth a Public Utilities Cybersecurity Action Plan with Compliance Standards and Oversight Procedures, dated April 6, 2016.[58] The Connecticut Plan seeks to increase partnership among utilities, increase monitoring and develop an enhanced "culture of security" to address cyber risk. The Connecticut Plan references the AWWA Guidance and Use-Tool and the NIST Framework, among other guidance for improving cybersecurity.[59]

At the federal level, the recent America's Water Infrastructure Act of 2018,[60] requires community water systems serving a population of more than 3,300 persons to conduct a risk and resilience assessment of their systems (42 U.S.C. 300i-2). This includes assessing the security of any electronic, computer, or other automated systems that the community water system uses. The Act also requires covered community water systems to certify to the USEPA, starting in March 2020 and re-certifying every five years, that they have completed the required assessments.

Cyber Insurance

Cyber insurance is an important consideration for both private-sector and government entities and also provide guidance regarding an organization's cyber risk profile. Determining the proper type and amount of cyber insurance requires a rigorous assessment of risk, and evaluation of specific coverage and policies. It is important to understand what data and systems are covered, to what extent, and for what incidents and responses. Coverage often varies among insurers, and from policy to policy. The scope of cyber insurance is an emerging area based on currently limited data analytics. Therefore, it is important not only to ask whether an entity has "cyber insurance" but to work with a knowledgeable advisor regarding specifically what is and may not be covered under the entity's policies.

The issue of cyber insurance can be difficult for most entities, and is often more complex for state operations, due to the sprawling nature and diverse systems that exist for many states.[61] According to the 2017 State CIO Survey, 38 percent of state CIOs reported having some type of cyber insurance, up

[56] Id.

[57] New York Consolidated Laws, Public Health, Article 11: Water Supply Emergency Plans, Section 1125, https://www.nysenate.gov/legislation/laws/PBH/1125.

[58] http://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf; *see also* Connecticut Office of Legislative Research report November 2, 2016, https://www.cga.ct.gov/2016/rpt/pdf/2016-R-0274.pdf.

[59] http://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf.

[60] Congress passed the bipartisan Act in October 2018 and, at the time of publication, it was pending signature by the President. https://www.congress.gov/bill/115th-congress/senate-bill/3021/text?q=%7B%22search%22%3A%5B%22s+3021%22%5D%7D&r=1

[61] Bergal, Jenni, "Worried About Hackers, States Turn to Cyber Insurance," Insurance Journal, Nov. 13, 2017, *available at* https://www.insurancejournal.com/news/national/2017/11/13/470991.htm.

from 20 percent in 2015.[62] Thus, for a government utility, it may be advisable to have a utility-specific cyber policy, in addition to whatever policy may apply more broadly to the government, or at least to ensure that existing policies address the utility's potential cyber risks.

PRIORITIZING CYBERSECURITY SOLUTIONS

Key to a good cybersecurity plan is understanding the threat and establishing cybersecurity governance protocols for addressing and managing the risk across the enterprise. To do this effectively requires executive support. Senior leadership – including the Board, Chief Executive Officer, Governor's Office, Municipal Executive – needs to be invested in ensuring cybersecurity is taken seriously in the organization. Also, because the issues and solutions are multi-faceted, an interdisciplinary team is required, examining the concerns from a technological, cost, efficiency, personnel and legal perspective.

Start by asking some basic questions:

- **WHAT** do we need to protect and **WHY**?
    - This requires understanding and then assessing risks within the organization in terms of technology, physical security and personnel. Senior leadership and technical experts within the organization need to confer, with the help of outside advisors if necessary. Do not overlook the fact that almost 90% of cyber attacks are caused by human error or behavior and those risks must be managed by limited access to systems and data to those critical for business functions.[63] Also, third-party vendors, partners and service providers who may have access to your systems and data also provide vulnerabilities that must be considered and managed.[64]
- **WHO** is the lead for cybersecurity within the organization?
    - The cybersecurity team should be interdisciplinary and the lead for the organization should have a direct line to senior management; as has been said many times, cybersecurity – particularly in terms of critical infrastructure – is not just a "tech" issue but also a critical component of enterprise risk management.
- **HOW** are we going to allocate resources, evaluate options and prioritize solutions?
    - Based on the risk assessment, develop a cybersecurity plan and protocols. NIST and the AWWA Guidance and Use-Tool are particularly helpful for prioritizing areas, analyzing gaps and developing a plan, including for cost-effective solutions such as two-factor authentication, restricted access, regular patches and updates, and education that fosters a culture of security and awareness throughout the enterprise.

[62] https://www.nascio.org/Portals/0/Publications/Documents/2017/NASCIO_2017_State_CIO_Survey.pdf?ver=2017-10-25-174540-510.

[63] https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/.

[64] Germano, Judith, *Third Party Cyber Risk and Corporate Responsibility*, https://www.lawandsecurity.org/wp-content/uploads/2017/02/Germano.NYU_.ThirdPartyRiskWhitepaper.Feb2017.pdf.

- Many, particularly smaller and mid-sized organizations or those with a less sophisticated cybersecurity posture and experience may find outsourcing – of governance and technical advisors as well as for cloud-based services and functions – can provide greater expertise and security than the organization may have or be able to provide internally.
- It also is critical to recognize that this is an organic and evolving process that requires regular assessments and continual updates to technology and processes to optimize cyber defenses.

In partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC, the WaterISAC has developed a list of 10 basic cybersecurity recommendations that water and wastewater utilities can use to reduce exploitable weaknesses and defend against avoidable data breaches and cyber attacks:[65]

1. Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks;
2. Implement Network Segmentation and Apply Firewalls;
3. Use Secure Remote Access Methods;
4. Establish Role-Based Access Controls and Implement System Logging;
5. Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls;
6. Maintain Awareness of Vulnerabilities and Implement Necessary Patches and Updates;
7. Develop and Enforce Policies on Mobile Devices;
8. Implement an Employee Cybersecurity Training Program;
9. Involve Executives in Cybersecurity; and
10. Implement Measures for Detecting Compromises and Develop a Cybersecurity Incident Response Plan.

Partnerships, within the organization, within the sector, and among public and private entities are critically important for successful cybersecurity and cyber risk management.[66] Sharing threat information, solutions, best practices and other resources can provide greater security that benefits the

[65] WaterISAC, Security Information Center, *10 Basic Cybersecurity Measures, Best Practices to Reduce Exploitable Weaknesses and Attacks*, June 2015, https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf.

[66] Germano, Judith, *Cybersecurity Partnerships, A New Era of Public-Private Collaboration, NYU School of Law,* http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.

sector as a whole. When it comes to cybersecurity in the water and wastewater sector, far more is to be gained by collaboration and communication than competition.

The cybersecurity landscape is changing rapidly as threats and technology continues to evolve. Given the severity of risk and potential harm, cybersecurity is a top threat that must be made a top priority for the water and wastewater sector. It is critically important to take a proactive and comprehensive approach to cybersecurity, involving active participation of the senior leaders of the organization, to ensure adequate technological and governance procedures are in place as part of an enterprise-wide cybersecurity program and strategy.

Appendix O

MANATEE SMP PLC REPLACEMENT BOM

carollo
Engineers...Working Wonders With Water®

Lake Manatee WTP

Budgetary Costs (Bill of Materials)

Project:	SCADA MASTER PLAN	PIC:	Sethi
Client:	Manatee County, FL	PM:	Anderson
Location:	Manatee County, FL	Date:	3/12/2020
		By:	Hanlon
Carollo Job #	10528C.00, task 8	Reviewed:	

Control Panel	PLC Model	Equipment Pricing	Labor	Total Cost	Project
63rd St. PLC Panel	SLC	$ 15,147.87	$ 14,879.25	$ 30,027.12	SE WRF
63rd St. Radio Panel	SLC	$ 2,331.55	$ 17,897.25	$ 20,228.80	SE WRF
Rye Road PLC Panel	SLC	$ 15,541.90	$ 14,879.25	$ 30,421.15	SE WRF
Rye Road Radio Panel	SLC	$ 2,331.55	$ 8,190.75	$ 10,522.30	SE WRF
Spencer Parish PLC Panel	SLC	$ 15,147.87	$ 8,843.25	$ 23,991.12	SE WRF
Spencer Parish Radio Panel	SLC	$ 2,331.55	$ 9,561.50	$ 11,893.05	SE WRF
MARS_NE	SLC	$ 8,166.47	$ 8,843.25	$ 17,009.72	N WRF
SP-1	SLC	$ 12,716.21	$ 11,861.25	$ 24,577.46	N WRF
SP-2	SLC	$ 8,166.47	$ 8,125.00	$ 16,291.47	N WRF
SP-3	SLC	$ 13,308.34	$ 20,269.50	$ 33,577.84	N WRF
SP4_N	SLC	$ 17,863.62	$ 27,175.50	$ 45,039.12	N WRF
NE_Everfilt	SLC	$ 14,775.25	$ 25,079.75	$ 39,855.00	N WRF
Lake Filter North	SLC	$ 14,775.25	$ 25,079.75	$ 39,855.00	N WRF
ADF12PLC	SLC	$ 14,775.25	$ 27,452.00	$ 42,227.25	N WRF
Micro Clarifier Pump West	SLC	$ 8,079.66	$ 9,779.00	$ 17,858.66	N WRF
Sludge Pump #1	SLC	$ 8,079.66	$ 9,779.00	$ 17,858.66	N WRF
Sludge Pump #2	SLC	$ 8,079.66	$ 9,779.00	$ 17,858.66	N WRF
Headworks MCC SP2-A	SLC	$ 19,371.54	$ 23,011.00	$ 42,382.54	SE WRF
Headworks MCC SP2-B, rack 1	SLC	$ 15,242.89	$ 10,925.50	$ 26,168.39	SE WRF
Headworks MCC SP2-B, rack 2	SLC	$ 17,373.25	$ 21,416.00	$ 38,789.25	SE WRF
Headworks Spiragrit	Micrologix	$ 8,286.62	$ 9,060.75	$ 17,347.37	SE WRF
Belt Press office	SLC	$ 11,228.86	$ 18,194.00	$ 29,422.86	SE WRF
Biosolids building -RTO	SLC	$ 18,212.07	$ 24,157.50	$ 42,369.57	SE WRF
Biosolids building -R10-10 (PLC10)	SLC	$ 11,701.91	$ 12,362.00	$ 24,063.91	SE WRF
Biosolids buidling - Burner Mgmt.	SLC	$ 9,187.26	$ 6,543.50	$ 15,730.76	SE WRF
Blower building - SP-3	SLC	$ 12,635.03	$ 20,922.00	$ 33,557.03	SE WRF
Main MCC SP1-A	SLC	$ 16,012.43	$ 21,422.75	$ 37,435.18	SE WRF
Main MCC SP1-B Rack 1	SLC	$ 11,846.97	$ 13,449.50	$ 25,296.47	SE WRF
Main MCC SP1-B Rack 2	SLC	$ 10,608.59	$ 17,686.50	$ 28,295.09	SE WRF
Nova Filters (SP5)	SLC	$ 6,872.88	$ 12,072.00	$ 18,944.88	SE WRF
Main MCC (HS - SP6)	Compact Logix	$ 9,271.70	$ 11,643.75	$ 20,915.45	SE WRF
GBT Panel	SLC	$ 14,963.48	$ 17,897.25	$ 32,860.73	SE WRF
GBT2 Panel	Compact Logix	$ 11,397.73	$ 21,633.50	$ 33,031.23	SE WRF
RTD HSP1	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
RTD HSP2	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
RTD HSP3	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
RTD HSP4	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
RTD Jockey P1	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
RTD Jockey P2	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
Polymer Mixing Pnl.	Micrologix	$ 15,673.60	$ 9,779.00	$ 25,452.60	SE WRF
Generator Controller	GE 90-30	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF
Landfill flame station	Versamax	$ 9,316.20	$ 9,779.00	$ 19,095.20	SE WRF

Lake Manatee WTP

Operations Rm SW RU	SLC	$ 13,465.30	$ 9,779.00	$ 23,244.30	SW WRF
Low Service PS (LSPS)	SLC	$ 19,031.52	$ 33,073.25	$ 52,104.77	SW WRF
Chem Bldg. SP-2	SLC	$ 17,415.35	$ 21,647.00	$ 39,062.35	SW WRF
DAF Bldg. SP-3	SLC	$ 12,990.09	$ 17,251.50	$ 30,241.59	SW WRF
Headworks Bldg. SP-4	SLC	$ 20,161.65	$ 33,218.25	$ 53,379.90	SW WRF
Digester Bldg. SP-5	SLC	$ 17,038.64	$ 23,511.75	$ 40,550.39	SW WRF
Dewatering Bldg. SP-6	SLC	$ 12,798.48	$ 9,561.50	$ 22,359.98	SW WRF
Electric South Bldg.		$ 20,161.65	$ 10,497.25	$ 30,658.90	SW WRF
Blower building SP-8	SLC	$ 16,077.38	$ 22,503.50	$ 38,580.88	SW WRF
Sludge Pump Bldg.	SLC	$ 14,145.11	$ 20,269.50	$ 34,414.61	SW WRF
ASR Well SP-10	Micrologix	$ 15,336.95	$ 4,678.75	$ 20,015.70	SW WRF
North Lake Level SP-11	Micrologix	$ 9,316.20	$ 8,342.50	$ 17,658.70	SW WRF
North Lake Reject PS SP-12	Micrologix	$ 9,316.20	$ 4,454.50	$ 13,770.70	SW WRF
Plant Reuse PS SP-13	Micrologix	$ 9,316.20	$ 9,779.00	$ 19,095.20	SW WRF
ABW	SLC	$ 15,073.90	$ 11,360.50	$ 26,434.40	SW WRF
North Lake PS SP-14	SLC	$ 12,924.05	$ 15,380.00	$ 28,304.05	SW WRF
Nova Filters (SP-15)	SLC	$ 14,478.52	$ 17,396.50	$ 31,875.02	SW WRF
HS SP-16	SLC	$ 12,487.81	$ 15,380.00	$ 27,867.81	SW WRF
HS (HSPS)	Compact Logix	$ 12,487.81	$ 9,779.00	$ 22,266.81	SW WRF
HS (LSPS)	Compact Logix	$ 12,487.81	$ 8,701.63	$ 21,189.43	SW WRF
HSPS 1 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
HSPS 2 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
HSPS 3 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
HSPS 4 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
HSPS 5 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
LSPS 1 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
LSPS 2 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
LSPS 3 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
LSPS 4 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
LSPS 5 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
LSPS 6 VFD	Micrologix	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
South Elec. Bldg. SP-18	SLC	$ 9,316.20	$ 2,339.38	$ 11,655.58	SW WRF
Turbo Blower Bldg. Blower 1	Compact Logix		$ 2,339.38	$ 2,339.38	SW WRF
Turbo Blower Bldg. Blower 2	Compact Logix		$ 2,339.38	$ 2,339.38	SW WRF
Turbo Blower Bldg. (SP-19)	Compact Logix		$ 3,416.75	$ 3,416.75	SW WRF
Dewatering Bldg. Polymer Pumps 5 & 6	SLC	$ 9,316.20	$ 10,714.75	$ 20,030.95	SW WRF
Dewatering Bldg. Polymer Mixing System	SLC	$ 9,316.20	$ 10,714.75	$ 20,030.95	SW WRF
Headworks - Grit Classifer	Micrologix	$ 9,316.20	$ 9,278.25	$ 18,594.45	SW WRF
Total	Total	$ 887,140.29	$981,323.38	$1,883,611.54	

Facility	
SE WRF	$ 771,908.45
N WRF	$ 312,008.84
SW WRF	$ 799,694.25

Labor Calculations

	Hardware Upgrade																Rates			
Control Panel	DI	DI Labor	DO	DO Labor	AI	AI Labor	AO	AO LAbor	Total I/O	PLC Program Migration	HMI Migration	Design Engineering	CAD	Subtotal Cost	25% Contingency	Total Cost	Field Tech	Programmer	Design Engineer	CADD
63rd St. PLC Panel	48	$ 435.00	16	$ 145.00	12	$ 652.50	0	$ -	76	$ 4,750.00	$ 4,750.00	$ 2,223.00	$ 1,539.00	$ 14,494.50	$ 384.75	$ 14,879.25	145	250	195	135
63rd St. Radio Panel	64	$ 580.00	16	$ 145.00	12	$ 652.50	0	$ -	92	$ 5,750.00	$ 5,750.00	$ 2,691.00	$ 1,863.00	$ 17,431.50	$ 465.75	$ 17,897.25				
Rye Road PLC Panel	48	$ 435.00	16	$ 145.00	12	$ 652.50	0	$ -	76	$ 4,750.00	$ 4,750.00	$ 2,223.00	$ 1,539.00	$ 14,494.50	$ 384.75	$ 14,879.25				
Rye Road Radio Panel	16	$ 145.00	16	$ 145.00	12	$ 652.50	0	$ -	44	$ 2,750.00	$ 2,750.00	$ 1,287.00	$ 891.00	$ 7,968.00	$ 222.75	$ 8,190.75				
Spencer Parish PLC Panel	16	$ 145.00	16	$ 145.00	12	$ 652.50	0	$ -	44	$ 2,750.00	$ 2,750.00	$ 1,287.00	$ 891.00	$ 8,620.50	$ 222.75	$ 8,843.25				
Spencer Parish Radio	16	$ 145.00	16	$ 145.00	12	$ 652.50	0	$ -	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,318.50	$ 243.00	$ 9,561.50				
MARS_NE	16	$ 145.00	16	$ 145.00	8	$ 435.00	4	$ 217.50	44	$ 2,750.00	$ 2,750.00	$ 1,287.00	$ 891.00	$ 8,620.50	$ 222.75	$ 8,843.25				
SP-1	32	$ 290.00	16	$ 145.00	8	$ 435.00	4	$ 217.50	60	$ 3,750.00	$ 3,750.00	$ 1,755.00	$ 1,215.00	$ 11,557.50	$ 303.75	$ 11,861.25				
SP-2	16	$ 145.00	16	$ 145.00	8	$ 435.00	4	$ 217.50	40	$ 2,500.00	$ 2,500.00	$ 1,170.00	$ 810.00	$ 7,922.50	$ 202.50	$ 8,125.00				
SP-3	64	$ 580.00	16	$ 145.00	16	$ 870.00	0	$ -	104	$ 6,500.00	$ 6,500.00	$ 3,042.00	$ 2,106.00	$ 19,743.00	$ 526.50	$ 20,269.50				
SP4_N	96	$ 870.00	16	$ 145.00	24	$ 1,305.00	8	$ 435.00	136	$ 8,500.00	$ 8,500.00	$ 3,978.00	$ 2,754.00	$ 26,487.00	$ 688.50	$ 27,175.50				
NE_Everfilt	80	$ 725.00	48	$ 435.00	4	$ 217.50	0	$ -	132	$ 8,250.00	$ 8,250.00	$ 3,861.00	$ 2,673.00	$ 24,411.50	$ 668.25	$ 25,079.75				
Lake Filter North	80	$ 725.00	48	$ 435.00	4	$ 217.50	0	$ -	132	$ 8,250.00	$ 8,250.00	$ 3,861.00	$ 2,673.00	$ 24,411.50	$ 668.25	$ 25,079.75				
ADF12PLC	80	$ 725.00	48	$ 435.00	8	$ 435.00	0	$ -	144	$ 9,000.00	$ 9,000.00	$ 4,212.00	$ 2,916.00	$ 26,723.00	$ 729.00	$ 27,452.00				
Micro Clarifier Pump	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00				
Sludge Pump #1	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00				
Sludge Pump #2	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00				
Headworks MCC SP2-A	48	$ 435.00	32	$ 290.00	32	$ 1,740.00	8	$ 435.00	112	$ 7,000.00	$ 7,000.00	$ 3,276.00	$ 2,268.00	$ 22,444.00	$ 567.00	$ 23,011.00				
Headworks MCC SP2-B, rack 1	48	$ 435.00	0	$ -	8	$ 435.00	0	$ -	56	$ 3,500.00	$ 3,500.00	$ 1,638.00	$ 1,134.00	$ 10,642.00	$ 283.50	$ 10,925.50				
Headworks MCC SP2-B, rack 2	48	$ 435.00	48	$ 435.00	8	$ 435.00	0	$ -	112	$ 7,000.00	$ 7,000.00	$ 3,276.00	$ 2,268.00	$ 20,849.00	$ 567.00	$ 21,416.00				
Headworks Spiragrit	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	44	$ 2,750.00	$ 2,750.00	$ 1,287.00	$ 891.00	$ 8,838.00	$ 222.75	$ 9,060.75				
Belt Press office	16	$ 145.00	32	$ 290.00	32	$ 1,740.00	4	$ 217.50	88	$ 5,500.00	$ 5,500.00	$ 2,574.00	$ 1,782.00	$ 17,748.50	$ 445.50	$ 18,194.00				
Biosolids building -RTO	64	$ 580.00	32	$ 290.00	24	$ 1,305.00	8	$ 435.00	120	$ 7,500.00	$ 7,500.00	$ 3,510.00	$ 2,430.00	$ 23,550.00	$ 607.50	$ 24,157.50				
Biosolids building -R10-10 (PLC10)	16	$ 145.00	32	$ 290.00	8	$ 435.00	0	$ -	64	$ 4,000.00	$ 4,000.00	$ 1,872.00	$ 1,296.00	$ 12,038.00	$ 324.00	$ 12,362.00				
Biosolids buidling - Burner Mgmt.	16	$ 145.00	0	$ -	4	$ 217.50	8	$ 435.00	32	$ 2,000.00	$ 2,000.00	$ 936.00	$ 648.00	$ 6,381.50	$ 162.00	$ 6,543.50				
Blower building - SP-3	64	$ 580.00	16	$ 145.00	16	$ 870.00	12	$ 652.50	104	$ 6,500.00	$ 6,500.00	$ 3,042.00	$ 2,106.00	$ 20,395.50	$ 526.50	$ 20,922.00				
Main MCC SP1-A	48	$ 435.00	32	$ 290.00	16	$ 870.00	8	$ 435.00	108	$ 6,750.00	$ 6,750.00	$ 3,159.00	$ 2,187.00	$ 20,876.00	$ 546.75	$ 21,422.75				
Main MCC SP1-B Rack 1	32	$ 290.00	16	$ 145.00	16	$ 870.00	12	$ 652.50	64	$ 4,000.00	$ 4,000.00	$ 1,872.00	$ 1,296.00	$ 13,125.50	$ 324.00	$ 13,449.50				
Main MCC SP1-B Rack 2	64	$ 580.00	0	$ -	24	$ 1,305.00	0	$ -	88	$ 5,500.00	$ 5,500.00	$ 2,574.00	$ 1,782.00	$ 17,241.00	$ 445.50	$ 17,686.50				
Nova Filters (SP5)	64	$ 580.00	0	$ -	0	$ -	0	$ -	64	$ 4,000.00	$ 4,000.00	$ 1,872.00	$ 1,296.00	$ 11,748.00	$ 324.00	$ 12,072.00				
Main MCC (HS - SP6)	32	$ 290.00	16	$ 145.00	8	$ 435.00	0	$ -	60	$ 3,750.00	$ 3,750.00	$ 1,755.00	$ 1,215.00	$ 11,340.00	$ 303.75	$ 11,643.75				

GBT Panel	48	$ 435.00	32	$ 290.00	8	$ 435.00	4	$ 217.50	92	$ 5,750.00	$ 5,750.00	$ 2,691.00	$ 1,863.00	$ 17,431.50	$ 465.75	$ 17,897.25
GBT2 Panel	48	$ 435.00	48	$ 435.00	8	$ 435.00	4	$ 217.50	112	$ 7,000.00	$ 7,000.00	$ 3,276.00	$ 2,268.00	$ 21,066.50	$ 567.00	$ 21,633.50
RTD HSP1	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
RTD HSP2	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
RTD HSP3	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
RTD HSP4	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
RTD Jockey P1	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
RTD Jockey P2	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
Polymer Mixing Pnl.	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
Generator Controller	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
Landfill flame station	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
Operations Rm SW RU	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
Low Service PS (LSPS)	96	$ 870.00	16	$ 145.00	40	$ 2,175.00	8	$ 435.00	164	$ 10,250.00	$ 10,250.00	$ 4,797.00	$ 3,321.00	$ 32,243.00	$ 830.25	$ 33,073.25
Chem Bldg. SP-2	48	$ 435.00	16	$ 145.00	32	$ 1,740.00	12	$ 652.50	104	$ 6,500.00	$ 6,500.00	$ 3,042.00	$ 2,106.00	$ 21,120.50	$ 526.50	$ 21,647.00
DAF Bldg. SP-3	48	$ 435.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	88	$ 5,500.00	$ 5,500.00	$ 2,574.00	$ 1,782.00	$ 16,806.00	$ 445.50	$ 17,251.50
Headworks Bldg. SP-4	96	$ 870.00	32	$ 290.00	32	$ 1,740.00	16	$ 870.00	164	$ 10,250.00	$ 10,250.00	$ 4,797.00	$ 3,321.00	$ 32,388.00	$ 830.25	$ 33,218.25
Digester Bldg. SP-5	64	$ 580.00	16	$ 145.00	32	$ 1,740.00	4	$ 217.50	116	$ 7,250.00	$ 7,250.00	$ 3,393.00	$ 2,349.00	$ 22,924.50	$ 587.25	$ 23,511.75
Dewatering Bldg. SP-6	16	$ 145.00	16	$ 145.00	8	$ 435.00	4	$ 217.50	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,318.50	$ 243.00	$ 9,561.50
Electric South Bldg.	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	52	$ 3,250.00	$ 3,250.00	$ 1,521.00	$ 1,053.00	$ 10,234.00	$ 263.25	$ 10,497.25
Blower building SP-8	96	$ 870.00	0	$ -	16	$ 870.00	12	$ 652.50	112	$ 7,000.00	$ 7,000.00	$ 3,276.00	$ 2,268.00	$ 21,936.50	$ 567.00	$ 22,503.50
Sludge Pump Bldg.	64	$ 580.00	16	$ 145.00	16	$ 870.00	0	$ -	104	$ 6,500.00	$ 6,500.00	$ 3,042.00	$ 2,106.00	$ 19,743.00	$ 526.50	$ 20,269.50
ASR Well SP-10	0	$ -	0	$ -	12	$ 652.50	8	$ 435.00	20	$ 1,250.00	$ 1,250.00	$ 585.00	$ 405.00	$ 4,577.50	$ 101.25	$ 4,678.75
North Lake Level SP-11	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	40	$ 2,500.00	$ 2,500.00	$ 1,170.00	$ 810.00	$ 8,140.00	$ 202.50	$ 8,342.50
North Lake Reject PS SP-12	16	$ 145.00	0	$ -	0	$ -	0	$ -	24	$ 1,500.00	$ 1,500.00	$ 702.00	$ 486.00	$ 4,333.00	$ 121.50	$ 4,454.50
Plant Reuse PS SP-13	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
ABW	32	$ 290.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	56	$ 3,500.00	$ 3,500.00	$ 1,638.00	$ 1,134.00	$ 11,077.00	$ 283.50	$ 11,360.50
North Lake PS SP-14	32	$ 290.00	32	$ 290.00	8	$ 435.00	0	$ -	80	$ 5,000.00	$ 5,000.00	$ 2,340.00	$ 1,620.00	$ 14,975.00	$ 405.00	$ 15,380.00
Nova Filters (SP-15)	64	$ 580.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	88	$ 5,500.00	$ 5,500.00	$ 2,574.00	$ 1,782.00	$ 16,951.00	$ 445.50	$ 17,396.50
HS SP-16	48	$ 435.00	16	$ 145.00	8	$ 435.00	0	$ -	80	$ 5,000.00	$ 5,000.00	$ 2,340.00	$ 1,620.00	$ 14,975.00	$ 405.00	$ 15,380.00
HS (HSPS)	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	48	$ 3,000.00	$ 3,000.00	$ 1,404.00	$ 972.00	$ 9,536.00	$ 243.00	$ 9,779.00
HS (LSPS)	16	$ 145.00	16	$ 145.00	8	$ 435.00	8	$ 435.00	42	$ 2,625.00	$ 2,625.00	$ 1,228.50	$ 850.50	$ 8,489.00	$ 212.63	$ 8,701.63
HSPS 1 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
HSPS 2 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
HSPS 3 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
HSPS 4 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
HSPS 5 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
LSPS 1 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
LSPS 2 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38

LSPS 3 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
LSPS 4 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
LSPS 5 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
LSPS 6 VFD	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
South Elec. Bldg. SP-18	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
Turbo Blower Bldg. Blower 1	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
Turbo Blower Bldg. Blower 2	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	10	$ 625.00	$ 625.00	$ 292.50	$ 202.50	$ 2,288.75	$ 50.63	$ 2,339.38
Turbo Blower Bldg. (SP-19)	0	$ -	0	$ -	8	$ 435.00	2	$ 108.75	16	$ 1,000.00	$ 1,000.00	$ 468.00	$ 324.00	$ 3,335.75	$ 81.00	$ 3,416.75
Dewatering Bldg. Polymer Pumps 5 & 6	16	$ 145.00	16	$ 145.00	12	$ 652.50	8	$ 435.00	52	$ 3,250.00	$ 3,250.00	$ 1,521.00	$ 1,053.00	$ 10,451.50	$ 263.25	$ 10,714.75
Dewatering Bldg. Polymer Mixing System	16	$ 145.00	16	$ 145.00	12	$ 652.50	8	$ 435.00	52	$ 3,250.00	$ 3,250.00	$ 1,521.00	$ 1,053.00	$ 10,451.50	$ 263.25	$ 10,714.75
Headworks - Grit Classifer	16	$ 145.00	16	$ 145.00	12	$ 652.50	8	$ 435.00	44	$ 2,750.00	$ 2,750.00	$ 1,287.00	$ 891.00	$ 9,055.50	$ 222.75	$ 9,278.25
																$ 981,323.38

HSPS SP16 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
1	1769-OA16	16 Point AC Output Module	$	656.00	$	656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
0	1769-OF4	4 Channel Analog Output Module	$	793.00	$	-
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
3	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	759.00
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	11,536.08
			8.25% Sales Tax:		$	951.73
			Total		$	12,487.81

NF SP15 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
1	1769-OA16	16 Point AC Output Module	$	656.00	$	656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
4	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	1,012.00
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	13,375.08
			8.25% Sales Tax:		$	1,103.44
			Total		$	14,478.52

NL SP14 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
2	1769-OA16	16 Point AC Output Module	$	656.00	$	1,312.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
0	1769-OF4	4 Channel Analog Output Module	$	793.00	$	-
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
2	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	506.00
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	11,939.08
			8.25% Sales Tax:		$	984.97
			Total		$	12,924.05

ABW Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
1	1769-OA16	16 Point AC Output Module	$	656.00	$	656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
2	1769-IF8	8 Channel Analog Input Module	$	834.00	$	1,668.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
2	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	728.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	13,925.08
			8.25% Sales Tax:		$	1,148.82
			Total		$	15,073.90

ASR Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
3	1769-IF8	8 Channel Analog Input Module	$	834.00	$	2,502.00
3	1769-OF4	4 Channel Analog Output Module	$	793.00	$	2,379.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	14,168.08
			8.25% Sales Tax:		$	1,168.87
			Total		$	15,336.95

BB SP8 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
2	1769-IF8	8 Channel Analog Input Module	$	834.00	$	1,668.00
3	1769-OF4	4 Channel Analog Output Module	$	793.00	$	2,379.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
6	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	1,518.00
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	14,852.08
			8.25% Sales Tax:		$	1,225.30
			Total		$	16,077.38

SP SP17 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
1	1769-OA16	16 Point AC Output Module	$ 656.00	$ 656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
2	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 1,668.00
0	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ -
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
4	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,456.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
0	1769-IB6F	3 wire DC input module	$ 505.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 13,067.08
			8.25% Sales Tax:	$ 1,078.03
			Total	$ 14,145.11

DW SP6 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
1	1769-OA16	16 Point AC Output Module	$ 656.00	$ 656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
1	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 253.00
0	1769-IB6F	3 wire DC input module	$ 505.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 11,823.08
			8.25% Sales Tax:	$ 975.40
			Total	$ 12,798.48

STP SP5 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
2	1769-OA16	16 Point AC Output Module	$	656.00	$	1,312.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
4	1769-IF8	8 Channel Analog Input Module	$	834.00	$	3,336.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
4	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	1,012.00
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	15,740.08
			8.25% Sales Tax:		$	1,298.56
			Total		$	17,038.64

HW SP4 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
2	1769-OA16	16 Point AC Output Module	$ 656.00	$ 1,312.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
4	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 3,336.00
4	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 3,172.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
6	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 1,518.00
0	1769-IB6F	3 wire DC input module	$ 505.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 18,625.08
			8.25% Sales Tax:	$ 1,536.57
			Total	$ 20,161.65

LSPS SP1 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
1	1769-OA16	16 Point AC Output Module	$	656.00	$	656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
5	1769-IF8	8 Channel Analog Input Module	$	834.00	$	4,170.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
1	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	364.00
6	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	1,518.00
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	17,581.08
			8.25% Sales Tax:		$	1,450.44
			Total		$	19,031.52

CB SP2 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
4	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 3,336.00
3	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 2,379.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
3	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 759.00
0	1769-IB6F	3 wire DC input module	$ 505.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 16,088.08
			8.25% Sales Tax:	$ 1,327.27
			Total	$ 17,415.35

DAF SP3 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
3	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 759.00
0	1769-IB6F	3 wire DC input module	$ 505.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 12,000.08
			8.25% Sales Tax:	$ 990.01
			Total	$ 12,990.09

OPS SW Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
1	1769-OA16	16 Point AC Output Module	$ 656.00	$ 656.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
1	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 364.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
1	1769-IB6F	3 wire DC input module	$ 505.00	$ 505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 12,439.08
			8.25% Sales Tax:	$ 1,026.22
			Total	$ 13,465.30

GBT2 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
3	1769-OA16	16 Point AC Output Module	$ 656.00	$ 1,968.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
3	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
1	1769-IB6F	3 wire DC input module	$ 505.00	$ 505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 10,529.08
			8.25% Sales Tax:	$ 868.65
			Total	$ 11,397.73

Poly Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
3	1769-OA16	16 Point AC Output Module	$	656.00	$	1,968.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
3	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	14,479.08
			8.25% Sales Tax:		$	1,194.52
			Total		$	15,673.60

RTD HSP1 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
1	1769-OA16	16 Point AC Output Module	$	656.00	$	656.00
1	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	986.11
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
0	1769-IB6F	3 wire DC input module	$	505.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
0		Industrial Computer	$	3,950.00	$	-
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	8,606.19
			8.25% Sales Tax:		$	710.01
			Total		$	9,316.20

GBT1 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
2	1769-OA16	16 Point AC Output Module	$	656.00	$	1,312.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
3	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	13,823.08
			8.25% Sales Tax:		$	1,140.40
			Total		$	14,963.48

SP1 B R1 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
1	1769-OB16	16 Point DC Output Module	$	327.00	$	327.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
2	1769-IF8	8 Channel Analog Input Module	$	834.00	$	1,668.00
3	1769-OF4	4 Channel Analog Output Module	$	793.00	$	2,379.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
2	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	728.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
0		Industrial Computer	$	3,950.00	$	-
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	10,944.08
			8.25% Sales Tax:		$	902.89
			Total		$	11,846.97

SP1 B R2 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
3	1769-IF8	8 Channel Analog Input Module	$	834.00	$	2,502.00
0	1769-OF4	4 Channel Analog Output Module	$	793.00	$	-
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
4	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,456.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
0		Industrial Computer	$	3,950.00	$	-
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	9,800.08
			8.25% Sales Tax:		$	808.51
			Total		$	10,608.59

SP5 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
0	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ -
0	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ -
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
4	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 1,012.00
0	1769-IB6F	3 wire DC input module	$ 505.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 6,349.08
			8.25% Sales Tax:	$ 523.80
			Total	$ 6,872.88

SP1 A Panel BOM

Qty	**Part #**	**Description**	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
2	1769-OB16	16 Point DC Output Module	$	327.00	$	654.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
2	1769-IF8	8 Channel Analog Input Module	$	834.00	$	1,668.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
3	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	14,792.08
			8.25% Sales Tax:		$	1,220.35
			Total		$	16,012.43

SP3 Panel BOM

Qty	**Part #**	**Description**	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
2	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 1,668.00
3	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 2,379.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
4	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,456.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
1	1769-IB6F	3 wire DC input module	$ 505.00	$ 505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 11,672.08
			8.25% Sales Tax:	$ 962.95
			Total	$ 12,635.03

Burner Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
2	1769-OB16	16 Point DC Output Module	$ 327.00	$ 654.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
1	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 364.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
1	1769-IB6F	3 wire DC input module	$ 505.00	$ 505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 8,487.08
			8.25% Sales Tax:	$ 700.18
			Total	$ 9,187.26

RT10 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
2	1769-OB16	16 Point DC Output Module	$	327.00	$	654.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
0	1769-IF8	8 Channel Analog Input Module	$	834.00	$	-
0	1769-OF4	4 Channel Analog Output Module	$	793.00	$	-
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
1	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	364.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	10,810.08
			8.25% Sales Tax:		$	891.83
			Total		$	11,701.91

RTO Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
2	1769-OB16	16 Point DC Output Module	$	327.00	$	654.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
4	1769-IF8	8 Channel Analog Input Module	$	834.00	$	3,336.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
4	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,456.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	16,824.08
			8.25% Sales Tax:		$	1,387.99
			Total		$	18,212.07

Headworks Grit Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
1	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 364.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 7,655.08
			8.25% Sales Tax:	$ 631.54
			Total	$ 8,286.62

SP4 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
2	1769-OB16	16 Point DC Output Module	$ 327.00	$ 654.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
4	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 3,336.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
1	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 253.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 10,373.08
			8.25% Sales Tax:	$ 855.78
			Total	$ 11,228.86

Headworks SP2-B Rack 1 Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OB16	16 Point DC Output Module	$ 327.00	$ -
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
2	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 1,586.00
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 860.22
3	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
1	1769-AENTR	Ethernet adapter	$ 852.00	$ 852.00
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 14,081.19
			8.25% Sales Tax:	$ 1,161.70
			Total	$ 15,242.89

Headworks SP2-B Rack 2 Panel BOM

Qty	**Part #**	**Description**	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
3	1769-OA16	16 Point AC Output Module	$	656.00	$	1,968.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	860.22
3	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
1	1769-AENTR	Ethernet adapter	$	852.00	$	852.00
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	16,049.19
			8.25% Sales Tax:		$	1,324.06
			Total		$	17,373.25

Headworks SP2-A Rack 0 Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
0	1769-OB16	16 Point DC Output Module	$	327.00	$	-
2	1769-OA16	16 Point AC Output Module	$	656.00	$	1,312.00
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
4	1769-IF8	8 Channel Analog Input Module	$	834.00	$	3,336.00
2	1769-OF4	4 Channel Analog Output Module	$	793.00	$	1,586.00
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	860.22
3	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	1,092.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
1	1769-AENTR	Ethernet adapter	$	852.00	$	852.00
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	17,895.19
			8.25% Sales Tax:		$	1,476.35
			Total		$	19,371.54

SP2 PLC Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
1	1769-OB16	16 Point DC Output Module	$	327.00	$	327.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
1	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	253.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
0		Industrial Computer	$	3,950.00	$	-
1	1784-SD1	Secure Digital Card	$	80.19	$	80.19
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	7,463.89
			8.25% Sales Tax:		$	615.77
			Total		$	8,079.66

M Clarifier Pump West PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
1	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 253.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 7,463.89
			8.25% Sales Tax:	$ 615.77
			Total	$ 8,079.66

SP1 PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
1	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 253.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
0	1769-AENTR	Ethernet adapter	$ 852.00	$ -
0		Industrial Computer	$ 3,950.00	$ -
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 7,463.89
			8.25% Sales Tax:	$ 615.77
			Total	$ 8,079.66

ADF12 PLC Panel BOM

Qty	**Part #**	**Description**	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
3	1769-OB16	16 Point DC Output Module	$ 327.00	$ 981.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
0	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ -
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 860.22
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
5	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 1,265.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
1	1769-AENTR	Ethernet adapter	$ 852.00	$ 852.00
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 13,649.19
			8.25% Sales Tax:	$ 1,126.06
			Total	$ 14,775.25

SP-2 PLC Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
1	1769-OB16	16 Point DC Output Module	$	327.00	$	327.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
1	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	253.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
1		Industrial Computer	$	-	$	-
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	7,544.08
			8.25% Sales Tax:		$	622.39
			Total		$	8,166.47

SP-3 PLC Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
1	1769-OB16	16 Point DC Output Module	$	327.00	$	327.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
2	1769-IF8	8 Channel Analog Input Module	$	834.00	$	1,668.00
0	1769-OF4	4 Channel Analog Output Module	$	793.00	$	-
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
4	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	1,012.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	12,294.08
			8.25% Sales Tax:		$	1,014.26
			Total		$	13,308.34

SP-4 N PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
3	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 2,502.00
2	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 1,586.00
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 860.22
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
6	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 1,518.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
1	1769-AENTR	Ethernet adapter	$ 852.00	$ 852.00
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 16,502.19
			8.25% Sales Tax:	$ 1,361.43
			Total	$ 17,863.62

Lake Filter North PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
3	1769-OB16	16 Point DC Output Module	$ 327.00	$ 981.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
0	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ -
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 860.22
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
5	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 1,265.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$ 2,640.60	$ 2,640.60
1	1769-AENTR	Ethernet adapter	$ 852.00	$ 852.00
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 13,649.19
			8.25% Sales Tax:	$ 1,126.06
			Total	$ 14,775.25

NE Everfilt PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
3	1769-OB16	16 Point DC Output Module	$ 327.00	$ 981.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
0	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ -
2	1769-PA4	120/240V AC Power Supply (5V @ 4	$ 430.11	$ 860.22
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
5	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 1,265.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2I	$ 2,640.60	$ 2,640.60
1	1769-AENTR	Ethernet adapter	$ 852.00	$ 852.00
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 13,649.19
			8.25% Sales Tax:	$ 1,126.06
			Total	$ 14,775.25

63rd Street PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OW8	8 Point AC/DC Relay Output Module	$ 380.70	$ -
1	1769-OA16	16 Point AC Output Module	$ 656.00	$ 656.00
3	1769sc-IF4IH	4 Channel Analog Input Modules with HART Protocol	$ 986.11	$ 2,958.33
1	1769-PA4	120/240V AC Power Supply (5V @ 4 Amp)	$ 430.11	$ 430.11
3	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,092.00
0	1769-IQ16	16 Point 24 VDC Sinking/Sourcing Input Module	$ 229.23	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2Mb Memory	$ 2,640.60	$ 2,640.60
1	Industrial Computer		$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 13,993.41
			8.25% Sales Tax:	$ 1,154.46
			Total	$ 15,147.87

63rd Street Radio Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43

Sub Total:	$	2,153.86
8.25% Sales Tax:	$	177.69
Total	$	2,331.55

Rye Road PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OW8	8 Point AC/DC Relay Output Module	$ 380.70	$ -
1	1769-OA16	16 Point AC Output Module	$ 656.00	$ 656.00
3	1769sc-IF4IH	4 Channel Analog Input Modules with HART Protocol	$ 986.11	$ 2,958.33
1	1769-PA4	120/240V AC Power Supply (5V @ 4 Amp)	$ 430.11	$ 430.11
4	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,456.00
0	1769-IQ16	16 Point 24 VDC Sinking/Sourcing Input Module	$ 229.23	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2Mb Memory	$ 2,640.60	$ 2,640.60
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 14,357.41
			8.25% Sales Tax:	$ 1,184.49
			Total	$ 15,541.90

Rye Road Radio Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 2,153.86

8.25% Sales Tax:	$	177.69
Total	$	2,331.55

Spencer Parish PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
0	1769-OW8	8 Point AC/DC Relay Output Module	$ 380.70	$ -
1	1769-OA16	16 Point AC Output Module	$ 656.00	$ 656.00
3	1769sc-IF4IH	4 Channel Analog Input Modules with HART Protocol	$ 986.11	$ 2,958.33
1	1769-PA4	120/240V AC Power Supply (5V @ 4 Amp)	$ 430.11	$ 430.11
3	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ 1,092.00
0	1769-IQ16	16 Point 24 VDC Sinking/Sourcing Input Module	$ 229.23	$ -
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2Mb Memory	$ 2,640.60	$ 2,640.60
1		Industrial Computer	$ 3,950.00	$ 3,950.00
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 13,993.41
			8.25% Sales Tax	$ 1,154.46
			Total	$ 15,147.87

Spencer Radio Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 2,153.86

8.25% Sales Tax	$	177.69
Total	$	2,331.55

MARS NE PLC Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OB16	16 Point DC Output Module	$ 327.00	$ 327.00
0	1769-OA16	16 Point AC Output Module	$ 656.00	$ -
0	1769sc-IF4IH	4 Channel Analog Input Modules with HART Protocol	$ 986.11	$ -
1	1769-IF8	8 Channel Analog Input Module	$ 834.00	$ 834.00
1	1769-OF4	4 Channel Analog Output Module	$ 793.00	$ 793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4 Amp)	$ 430.11	$ 430.11
0	1769-IA16	16 Point 120VAC Input Module	$ 364.00	$ -
1	1769-IB16	16 Point 24 VDC Input Module	$ 253.00	$ 253.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2Mb Memory	$ 2,640.60	$ 2,640.60
1		Industrial Computer	$ -	$ -
2	1784-SD1	Secure Digital Card	$ 80.19	$ 160.38
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 7,544.08
			8.25% Sales Tax:	$ 622.39
			Total	$ 8,166.47

Spencer Radio Panel BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
1	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ 1,053.00
2	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ 369.36
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94

1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 2,153.86
			8.25% Sales Tax:	$ 177.69
			Total	$ 2,331.55

Tamiiami Well 42 BOM

Qty	Part #	Description	Unit Pricing	Total Pricing
1	1769-ECR	Right End Cap Terminator	$ 32.32	$ 32.32
1	1769-OW8	8 Point AC/DC Relay Output Module	$ 380.70	$ 380.70
2	1769sc-IF4IH	4 Channel Analog Input Modules with HART Protocol	$ 986.11	$ 1,972.22
1	1769-PA4	120/240V AC Power Supply (5V @ 4 Amp)	$ 430.11	$ 430.11
2	1769-IQ16	16 Point 24 VDC Sinking/Sourcing Input Module	$ 229.23	$ 458.46
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2Mb Memory	$ 2,640.60	$ 2,640.60
1	1784-SD1	Secure Digital Card	$ 80.19	$ 80.19
0	1783-BMS06SA	Stratix Switch	$ 1,053.00	$ -
0	1783-SFP100FX	Fiber Transceiver	$ 184.68	$ -
2	1489-M1C050	5amp Circuit breaker	$ 76.47	$ 152.94
2	1489-M1C100	10amp Circuit breaker	$ 76.47	$ 152.94
1	1606-XLE240EN	24vdc power supply	$ 345.43	$ 345.43
			Sub Total:	$ 6,645.91
			8.25% Sales Tax:	$ 548.29
			Total	$ 7,194.20

SP-1 PLC Panel BOM

Qty	Part #	Description	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
1	1769-OB16	16 Point DC Output Module	$	327.00	$	327.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
1	1769-IF8	8 Channel Analog Input Module	$	834.00	$	834.00
1	1769-OF4	4 Channel Analog Output Module	$	793.00	$	793.00
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
0	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	-
2	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	506.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
1		Industrial Computer	$	3,950.00	$	3,950.00
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	11,747.08
			8.25% Sales Tax:		$	969.13
			Total		$	12,716.21

SP6 Panel BOM

Qty	**Part #**	**Description**	Unit Pricing		Total Pricing	
1	1769-ECR	Right End Cap Terminator	$	32.32	$	32.32
1	1769-OB16	16 Point DC Output Module	$	327.00	$	327.00
0	1769-OA16	16 Point AC Output Module	$	656.00	$	-
0	1769sc-IF4IH	4 Channel Analog Input Modules wit	$	986.11	$	-
2	1769-IF8	8 Channel Analog Input Module	$	834.00	$	1,668.00
0	1769-OF4	4 Channel Analog Output Module	$	793.00	$	-
1	1769-PA4	120/240V AC Power Supply (5V @ 4	$	430.11	$	430.11
2	1769-IA16	16 Point 120VAC Input Module	$	364.00	$	728.00
0	1769-IB16	16 Point 24 VDC Input Module	$	253.00	$	-
1	1769-IB6F	3 wire DC input module	$	505.00	$	505.00
1	1769-L33ER	CompactLogix 5370 L3 Controller, 2M	$	2,640.60	$	2,640.60
0	1769-AENTR	Ethernet adapter	$	852.00	$	-
0		Industrial Computer	$	3,950.00	$	-
2	1784-SD1	Secure Digital Card	$	80.19	$	160.38
1	1783-BMS06SA	Stratix Switch	$	1,053.00	$	1,053.00
2	1783-SFP100FX	Fiber Transceiver	$	184.68	$	369.36
2	1489-M1C050	5amp Circuit breaker	$	76.47	$	152.94
2	1489-M1C100	10amp Circuit breaker	$	76.47	$	152.94
1	1606-XLE240EN	24vdc power supply	$	345.43	$	345.43
			Sub Total:		$	8,565.08
			8.25% Sales Tax:		$	706.62
			Total		$	9,271.70