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.

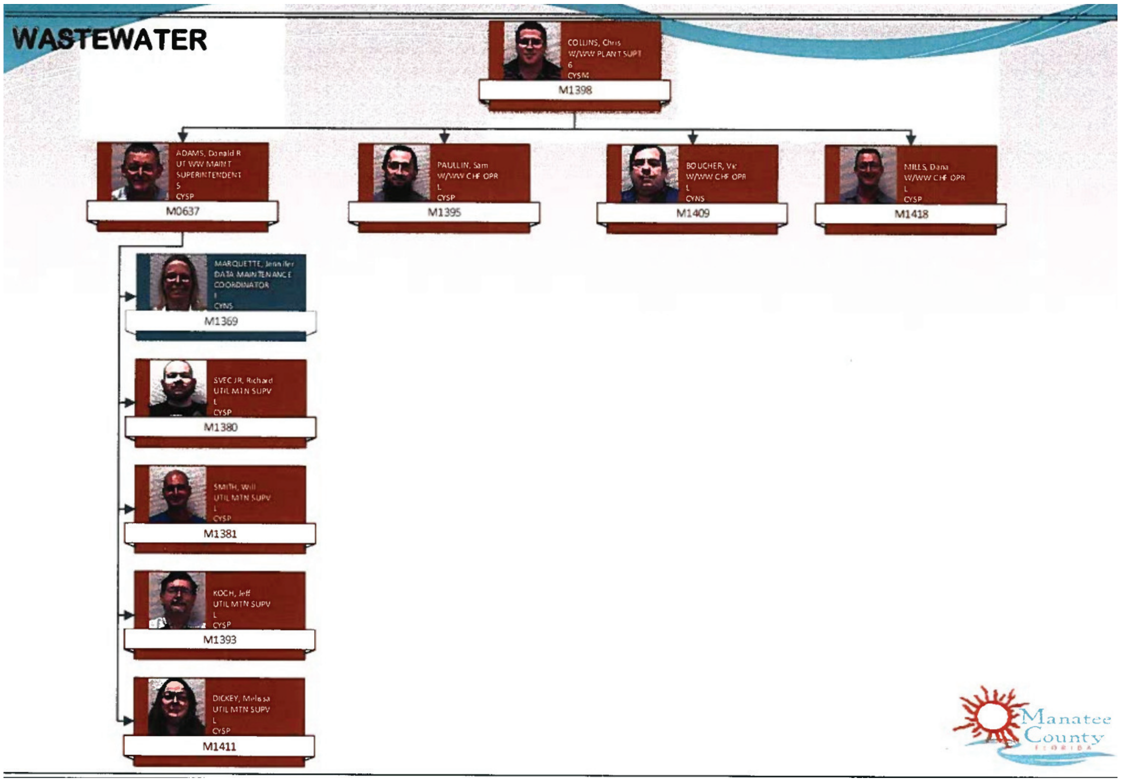


Figure 2.1 Wastewater Organization Chart - Wastewater Plant SCADA

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.

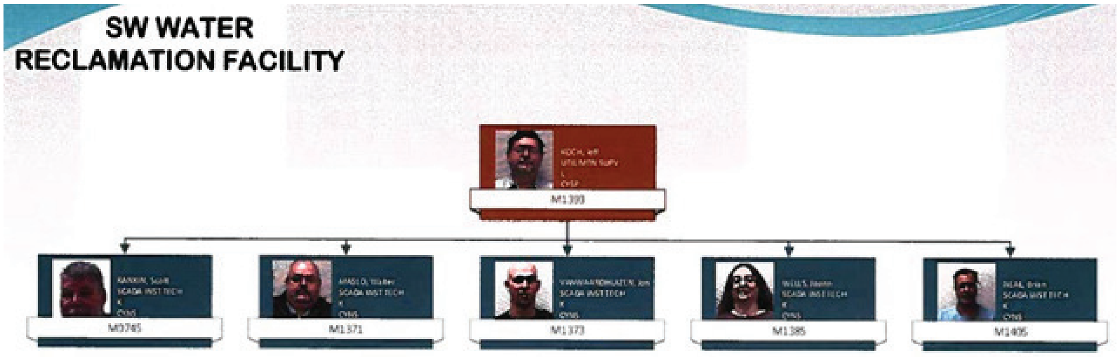


Figure 2.2 Title Group Organization under the Utilities Maintenance Supervisor

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:

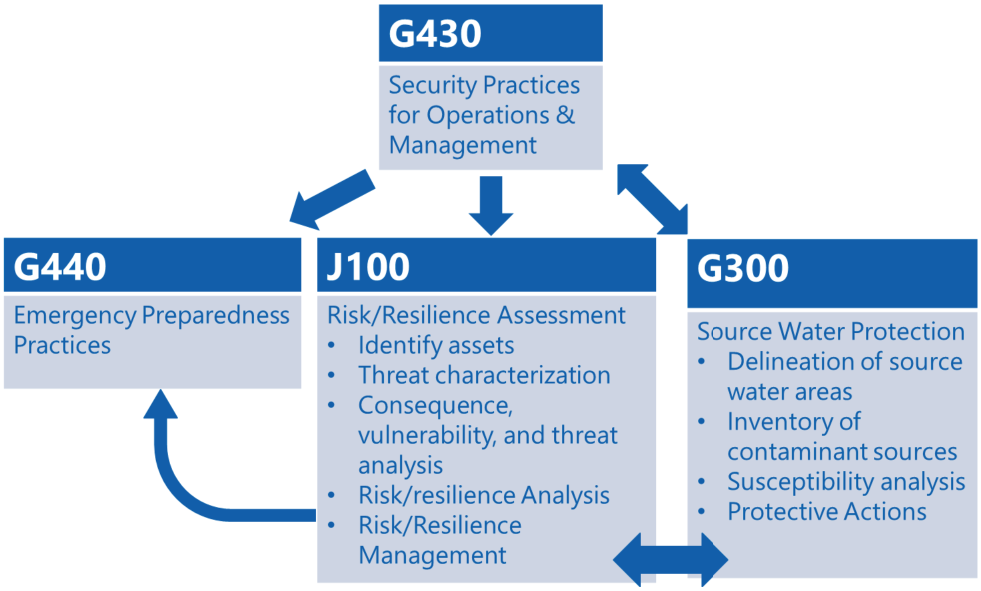

G430
Security Practices for Operations & Management
G440
Emergency Preparedness Practices
J100
Risk/Resilience Assessment
• Identify assets
• Threat characterization
• Consequence, vulnerability, and threat analysis
• Risk/resilience Analysis
• Risk/Resilience Management
G300
Source Water Protection
• 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.

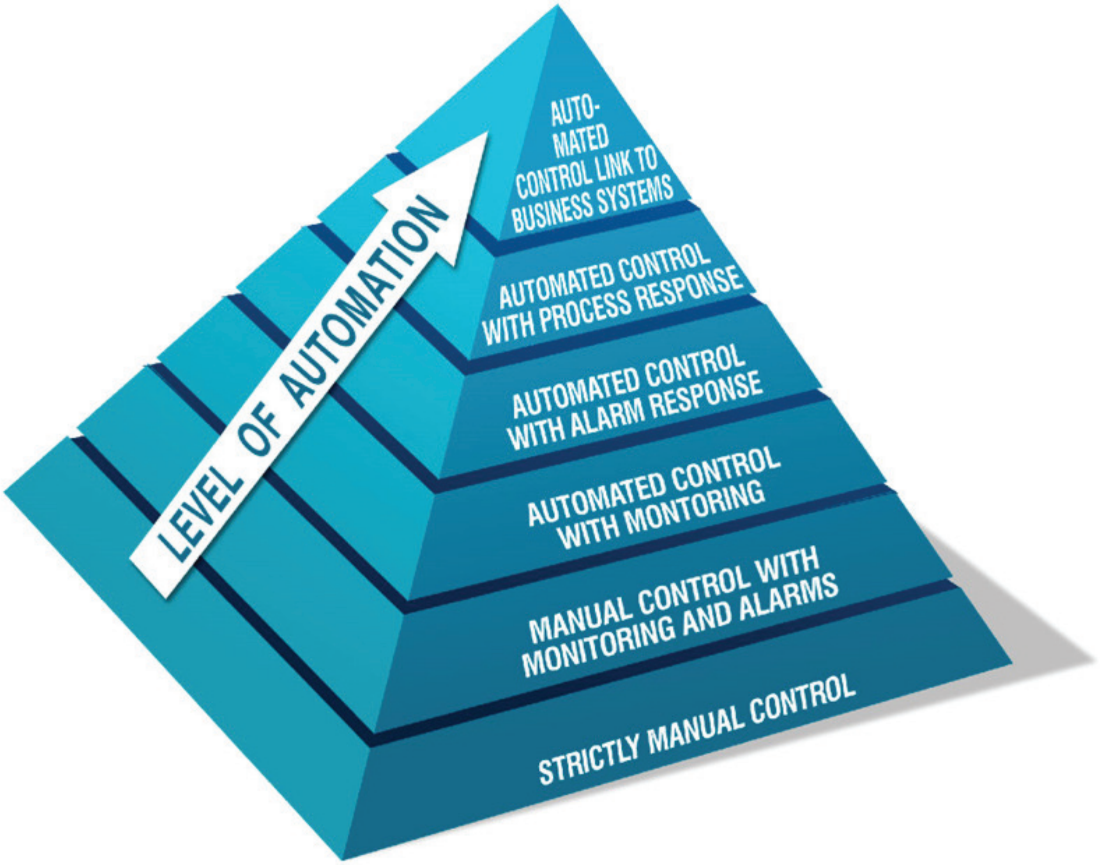

LEVEL OF AUTOMATION
AUTO-MATED CONTROL LINK TO BUSINESS SYSTEMS
AUTOMATED CONTROL WITH PROCESS RESPONSE
AUTOMATED CONTROL WITH ALARM RESPONSE
AUTOMATED CONTROL WITH MONTORING
MANUAL CONTROL WITH MONITORING AND ALARMS
STRICTLY MANUAL CONTROL

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.

Active
Mature
End of Life
Discontinued

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

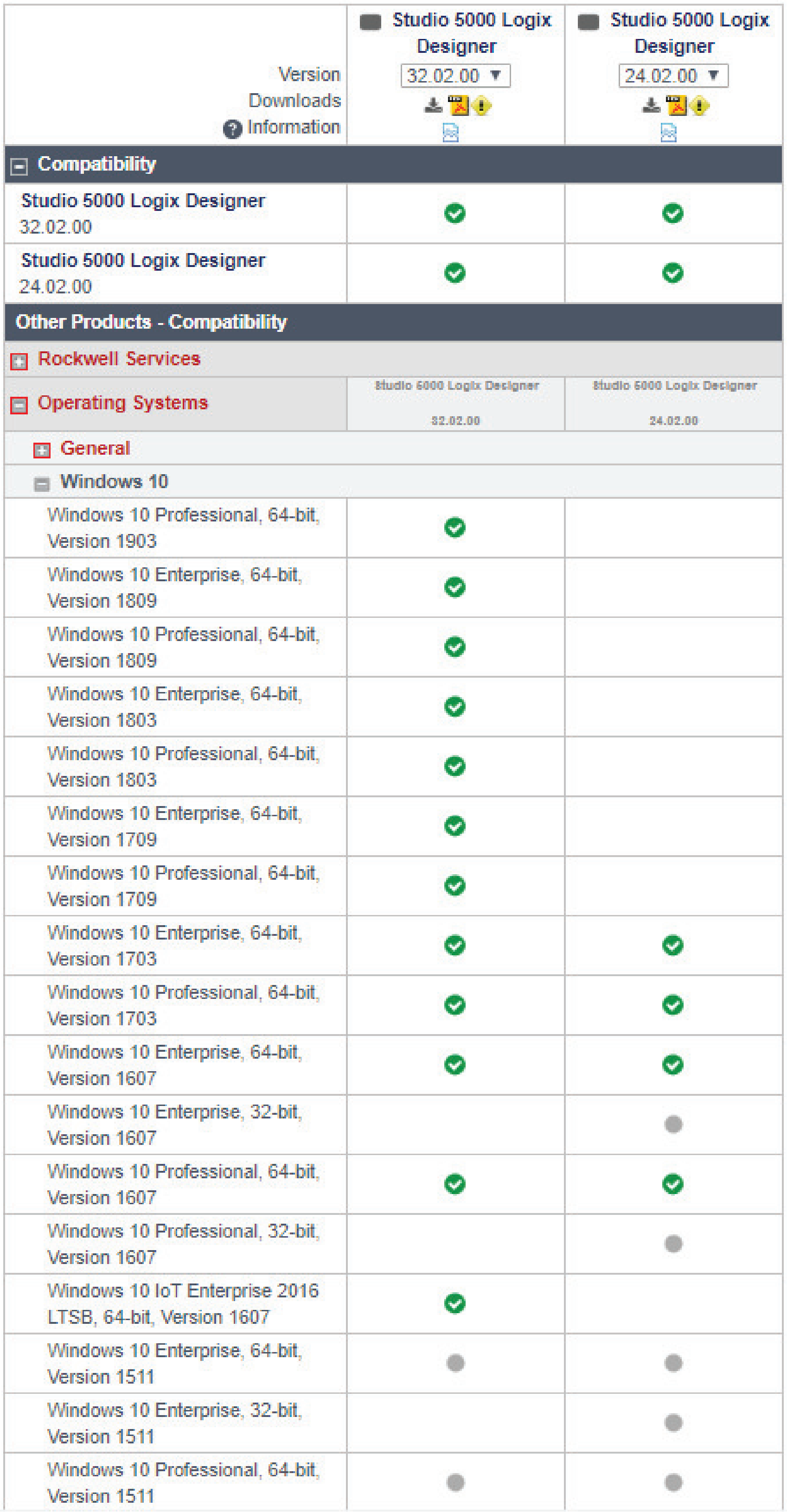
The County also utilizes GE MDS iNET 900 Ethernet radios, Engenius Ethernet bridges, and Digi One serial to IP converters for communication and communication protocol conversion. These devices are current and functioning properly. Continued maintenance is required for device replacement and upgrade as 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

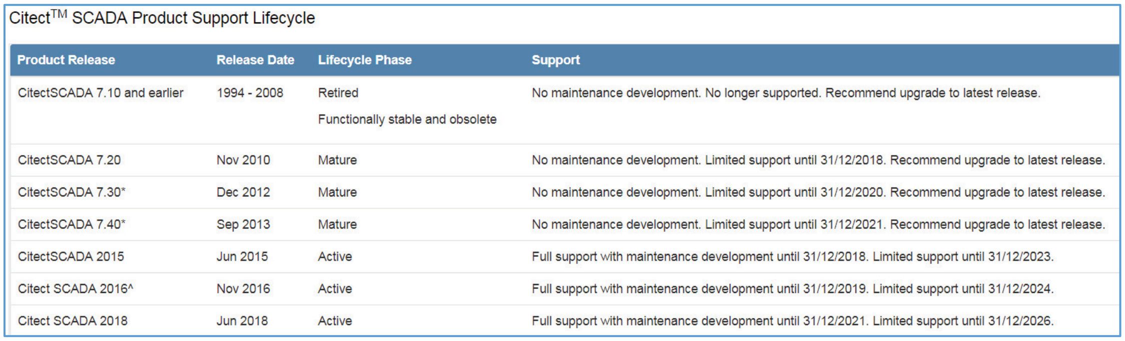
Table 4.1 County's Citect Licensing by Facility Summary (Continued)

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™ 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™ 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:

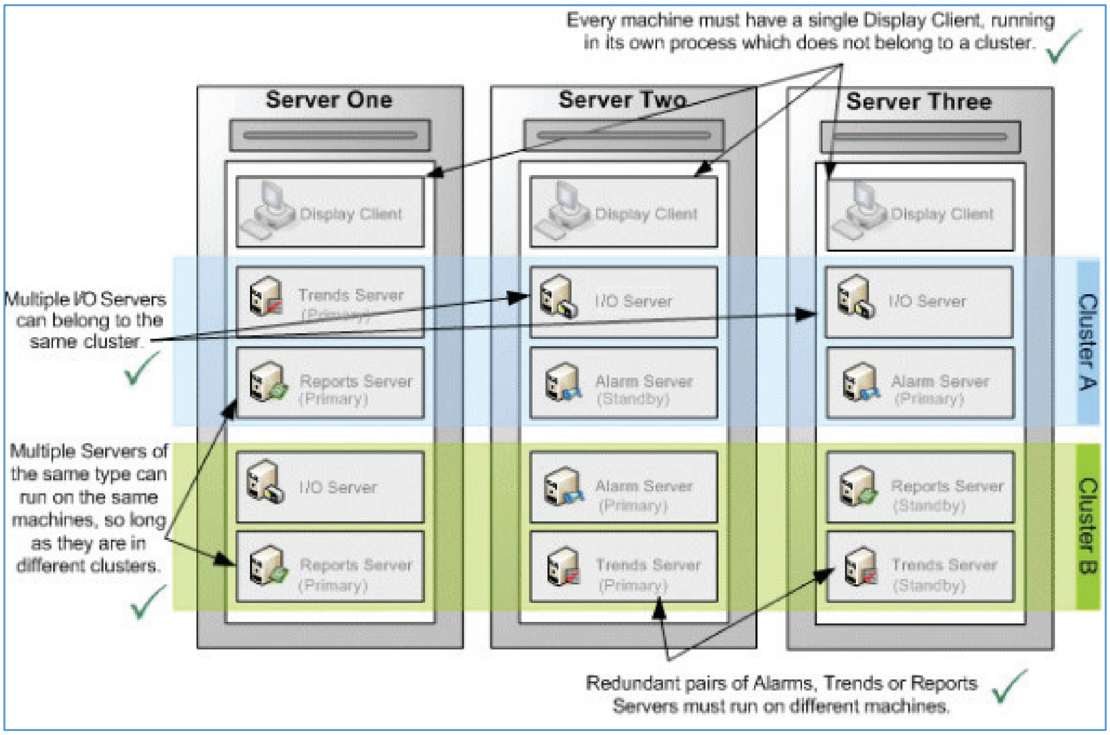

Every machine must have a single Display Client, running in its own process which does not belong to a cluster. ✓
Server One
Server Two
Server Three
Display Client
Display Client
Display Client
Multiple I/O Servers can belong to the same cluster. ✓
Trends Server (Primary)
I/O Server
I/O Server
Reports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

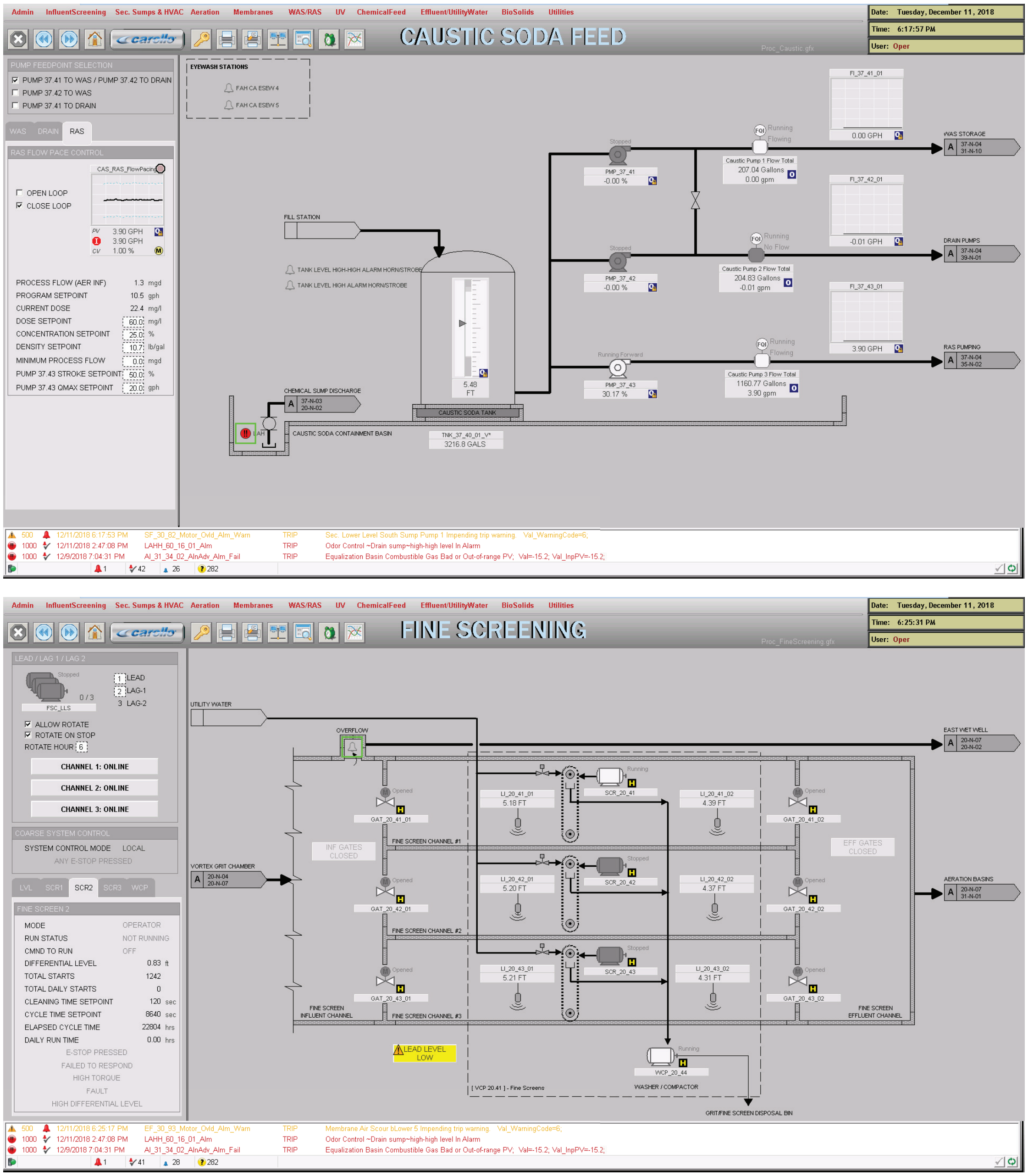
Equipment State	Color	Text
Running / Running Low Speed	Red	Black
Running High Speed	Orange	Black
Off	Green	Black
Open	Red	Black for position
Closed	Green	Black for position
Travelling / Midspan	?	
Failed / Trouble	Yellow	None
Alarm	Orange	None

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
FSC_LLS
0 / 3

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.

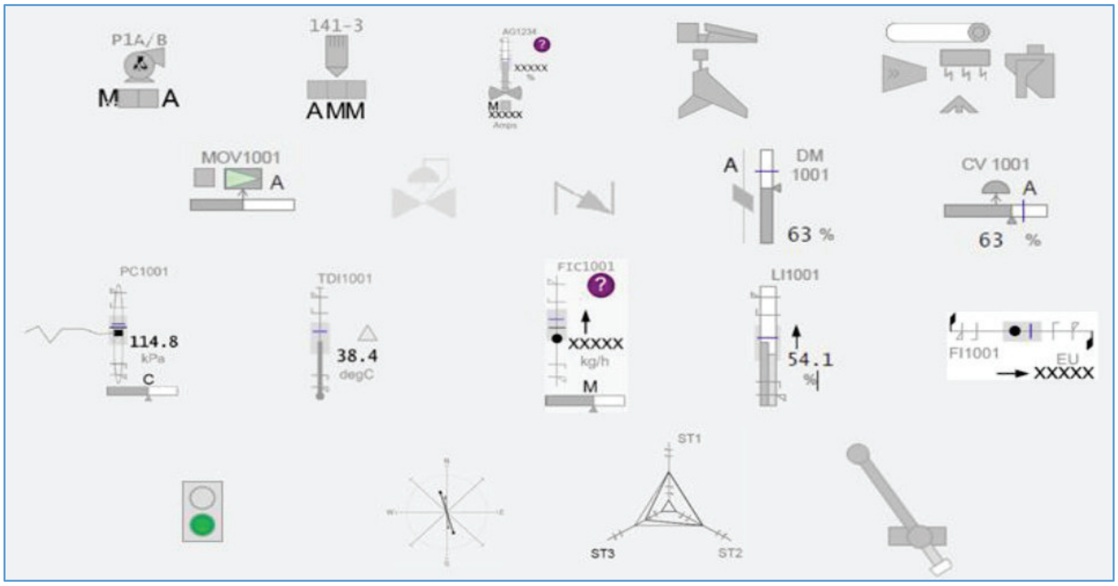
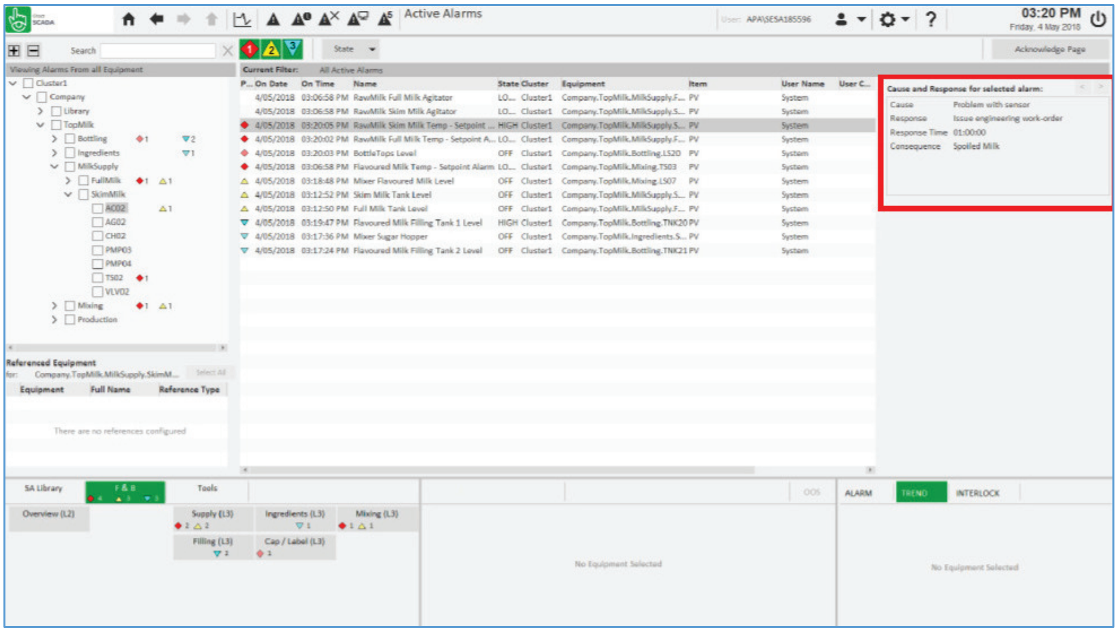


Figure 4.4 Example, Comprehensive Graphics Library

- 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

Referenced Equipment
for: Company.TopMilk.MilkSupply.SkimM...

Equipment	Full Name	Reference Type

There are no references configured

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:

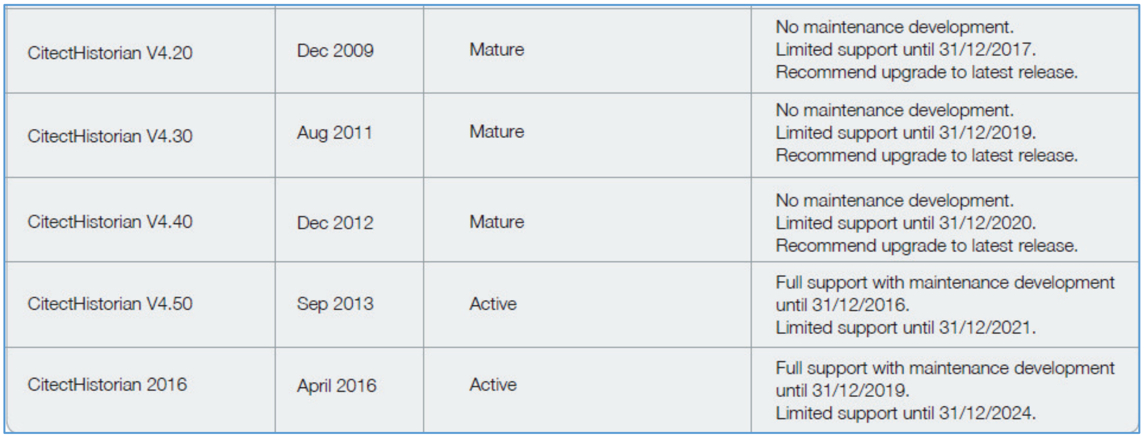
- Reliable communications both inside and outside of facility buildings for client operation.
- Mobile device security coordinated with IT.
- Consistent SCADA client application delivery for common access environment.
- Enhanced SCADA client authentication and security groups for application security.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

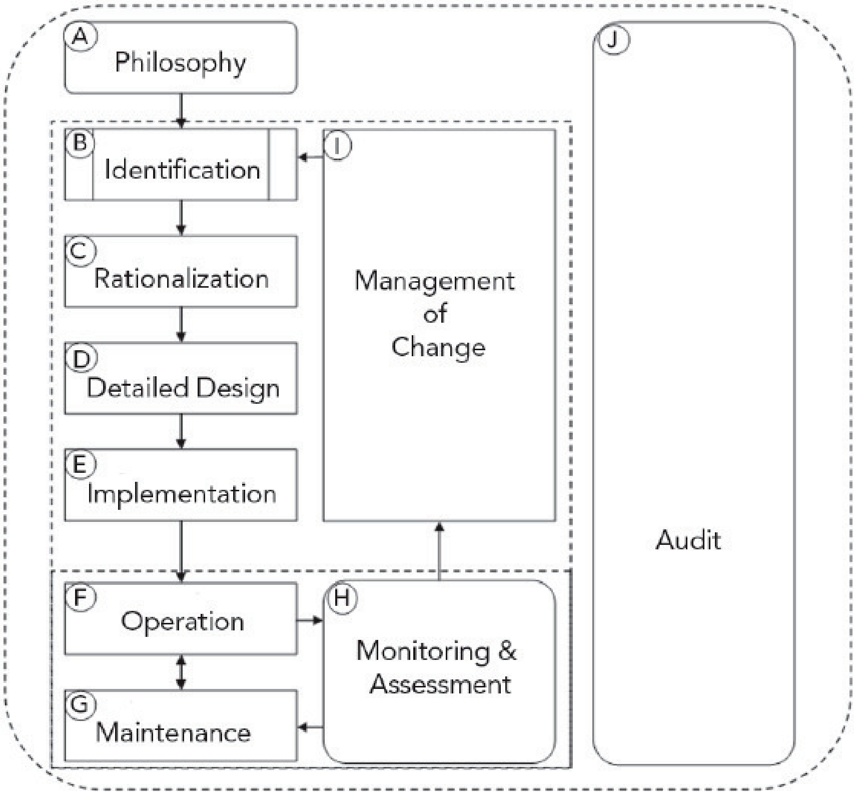


Figure 4.7 The Alarm Management Life Cycle

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.

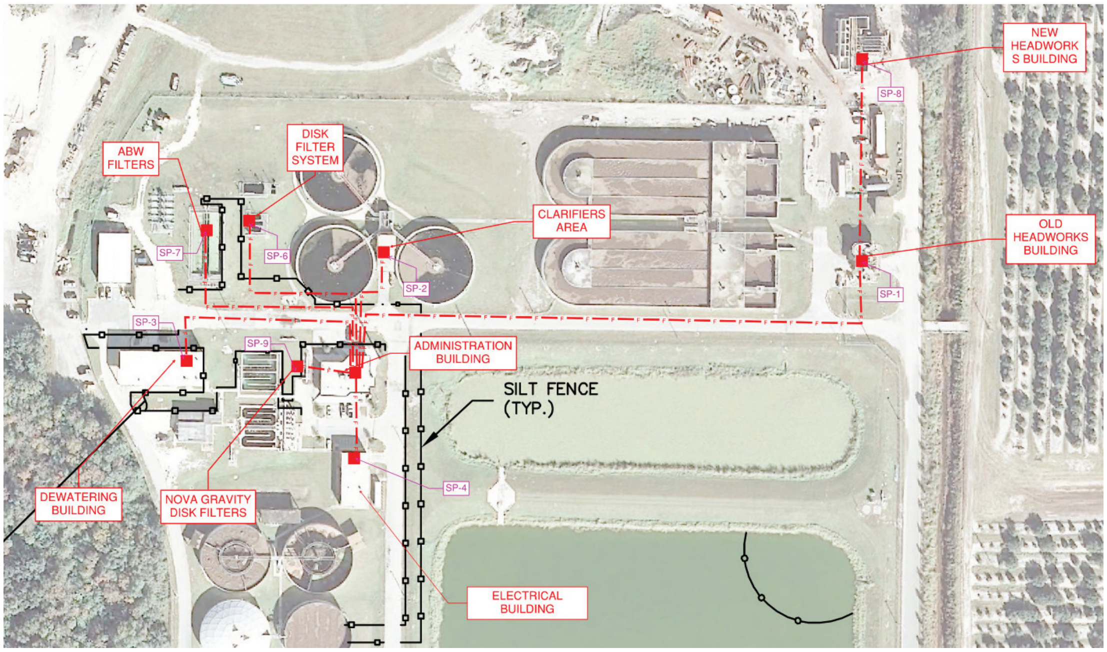


Figure 5.1 N WRF Existing Route is a Star Topology Originating From the Administration Building

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.

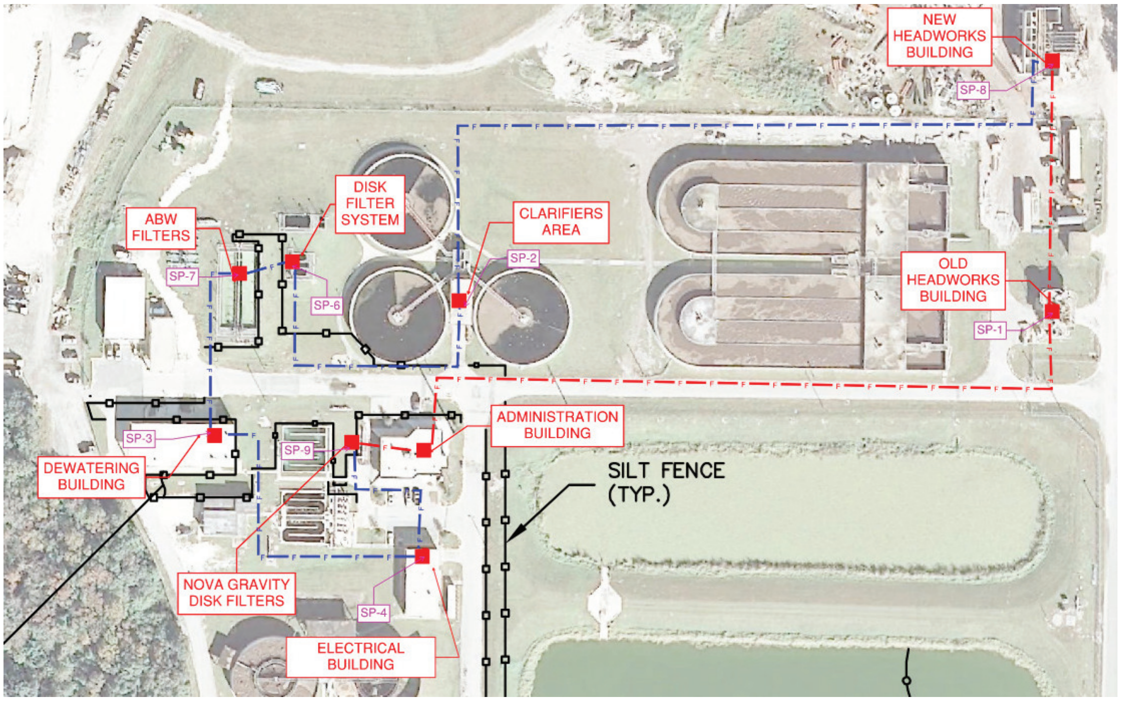


Figure 5.2 N WRF Route Proposes a Redundant Fiber Ring Around the Entire Plant Site.

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.

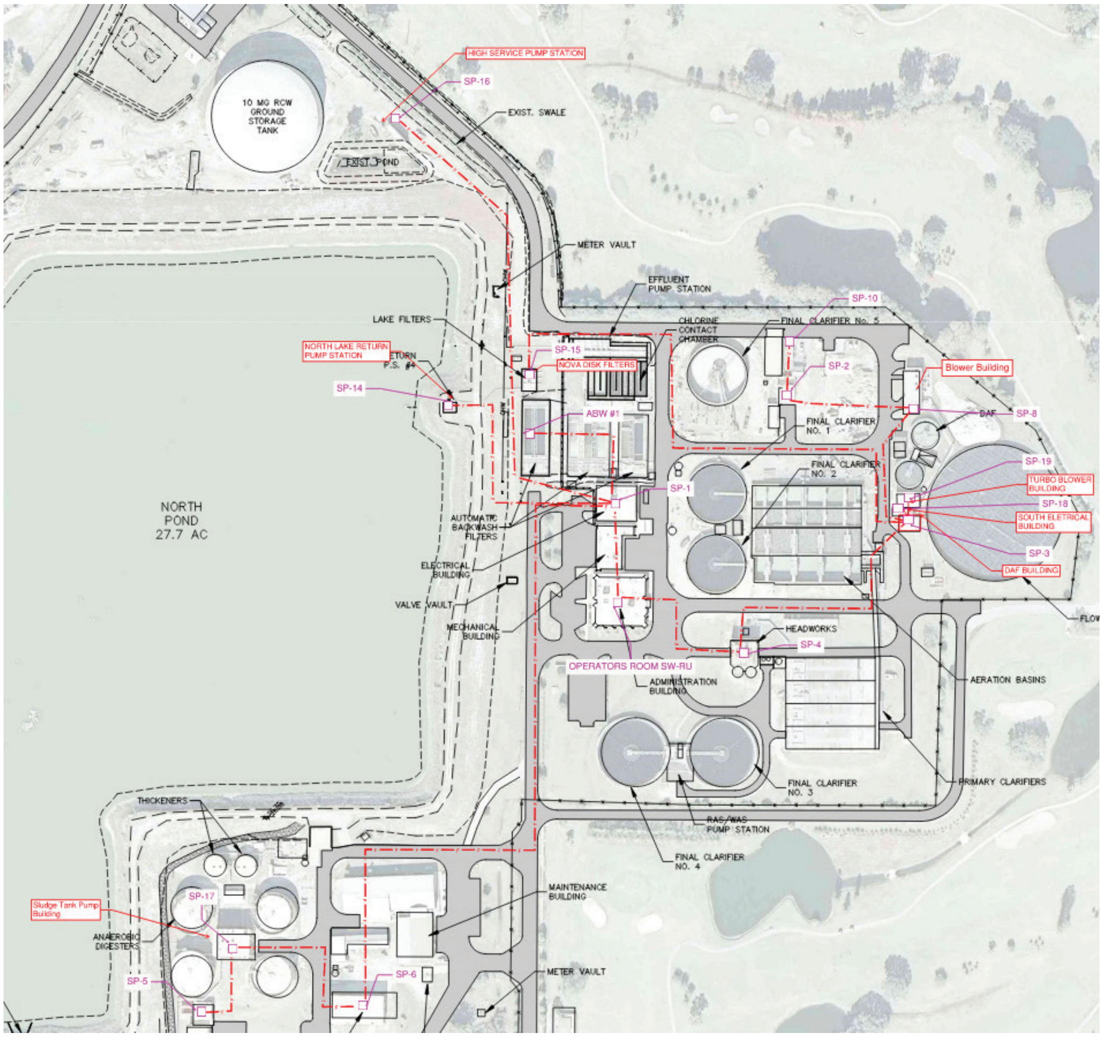


Figure 5.3 SW WRF Existing Fiber Route

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.

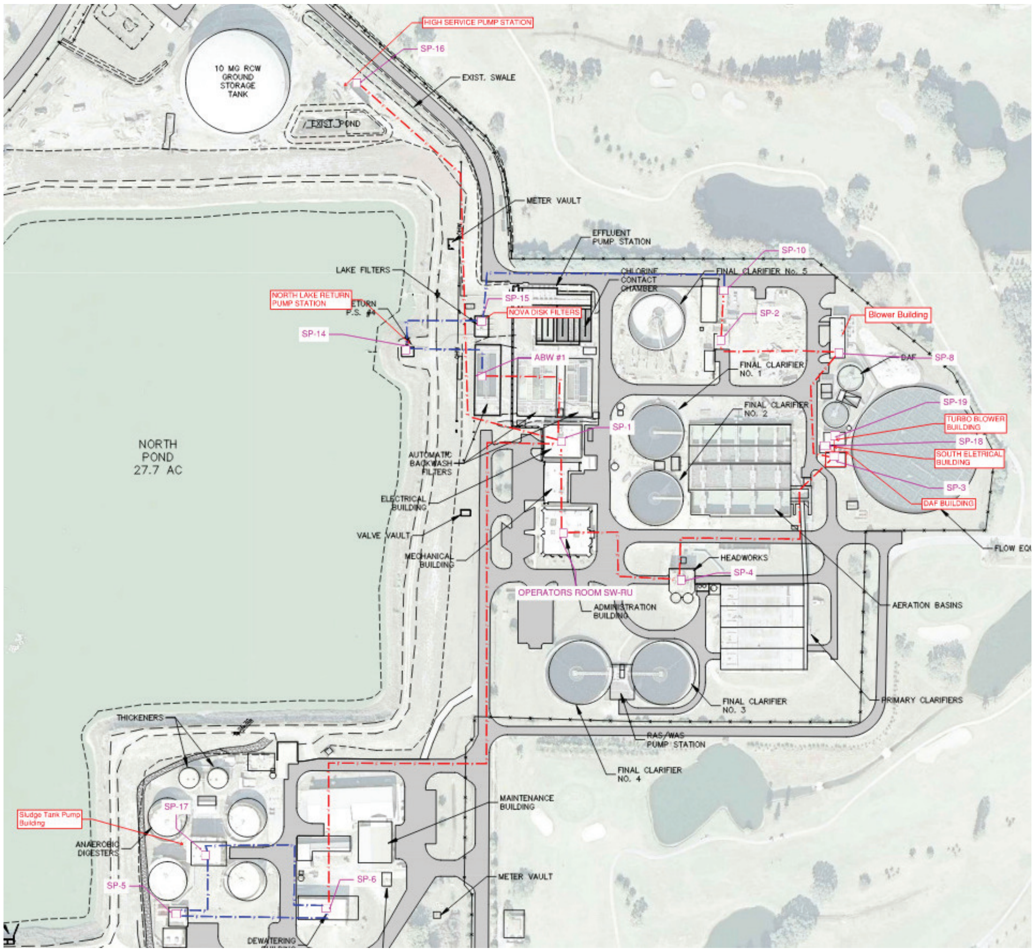


Figure 5.4 SW WRF Route Proposes Two Fiber Rings Around the Entire Plant Site

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.

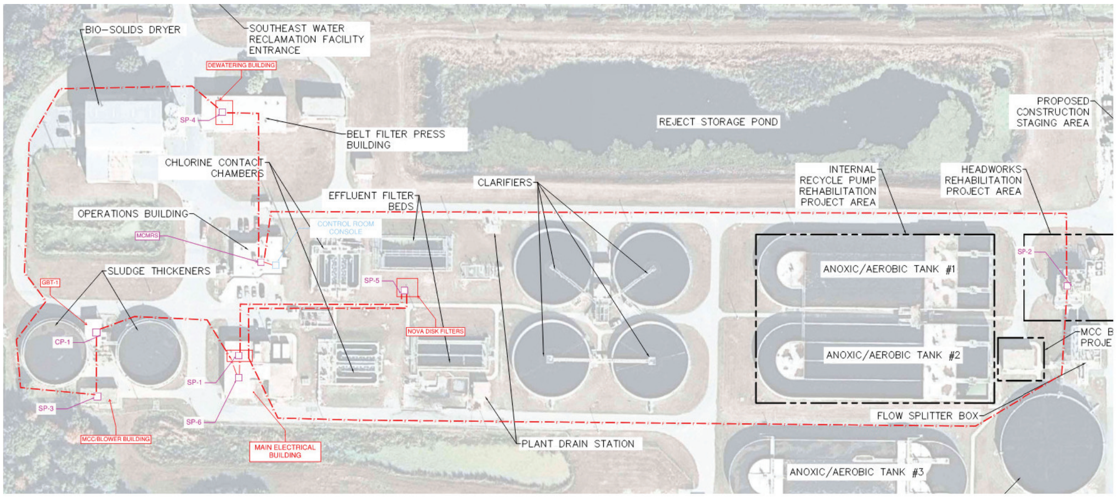
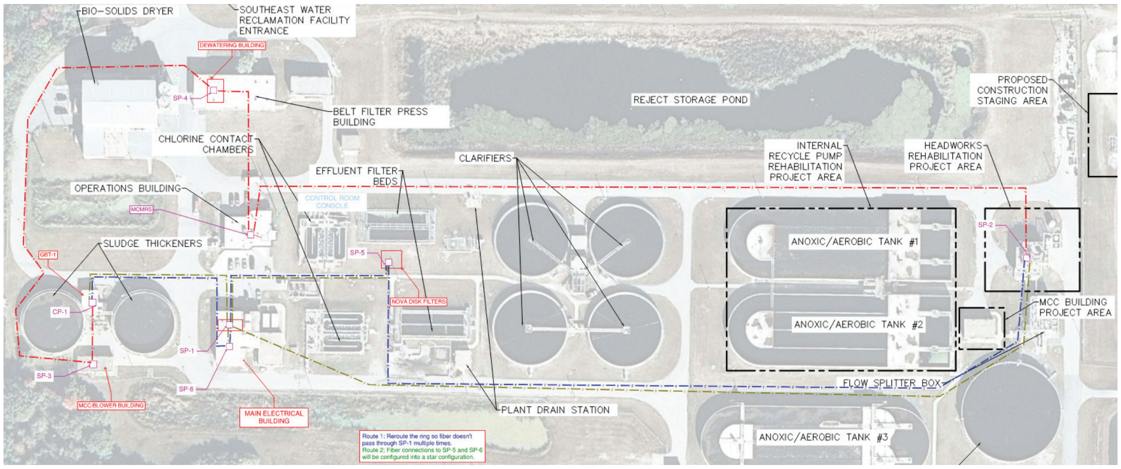


Figure 5.5 SE WRF Existing Fiber Route

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.

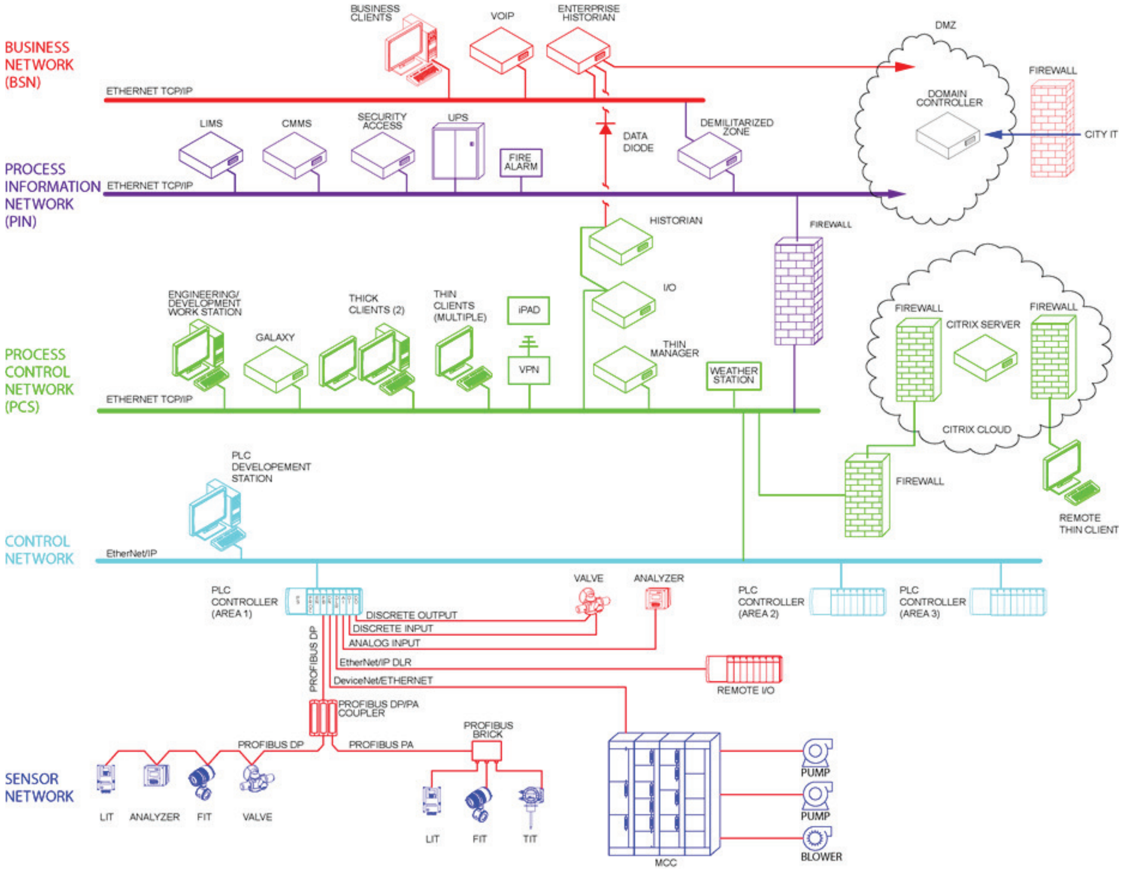


Figure 5.7 Example Control System Network Segmentation

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.

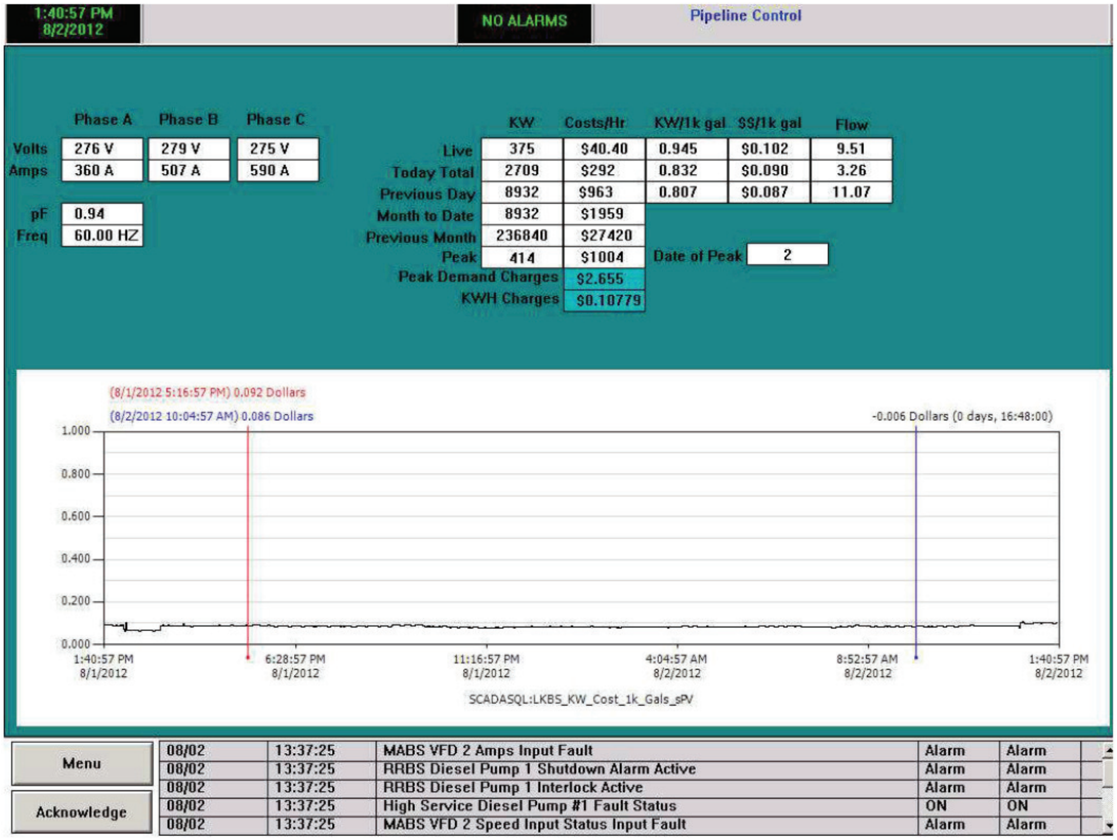
Most of this report information could be driven out of Hach WIMS with data from the SCADA system. Other daily and custom reports should also be developed in the HACH WIMS system to support operations and management. Additionally, engineering staff should be trained in the use of Hach WIMS and provided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



	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.

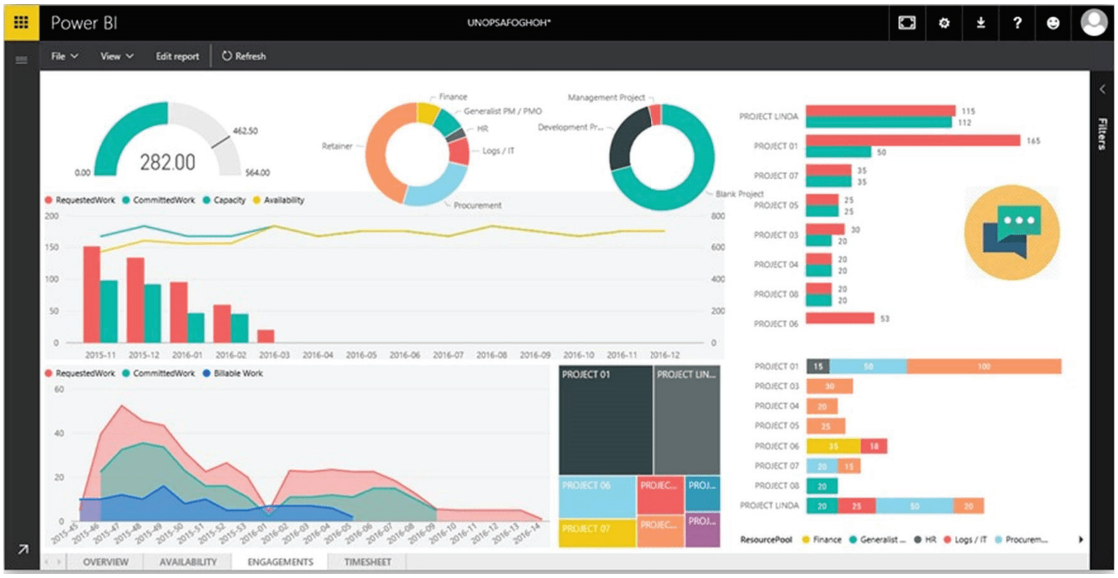


Figure 6.2 Example BI Dashboard

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.

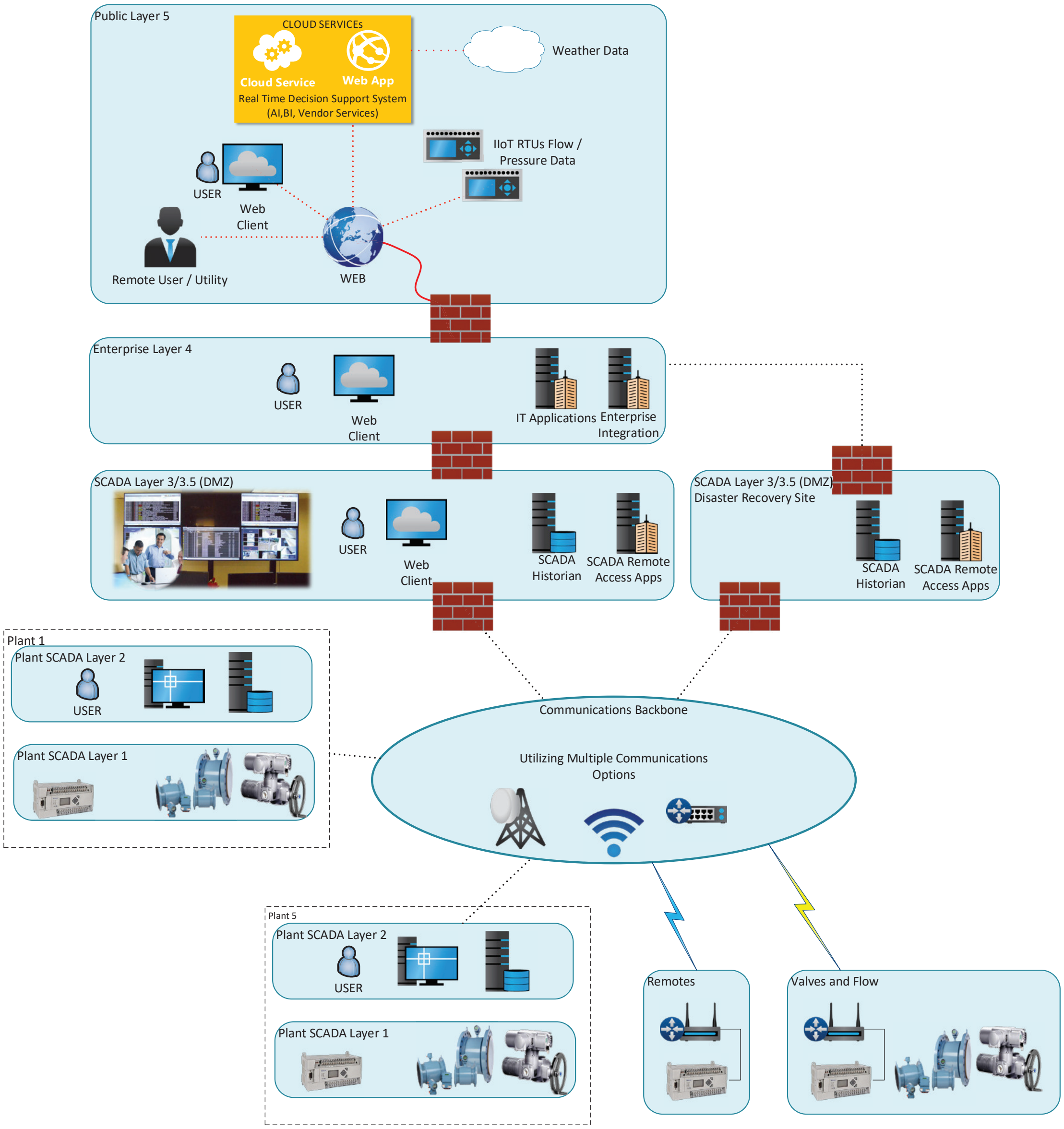


Figure 6.3 Example RTDSS System Architecture

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.

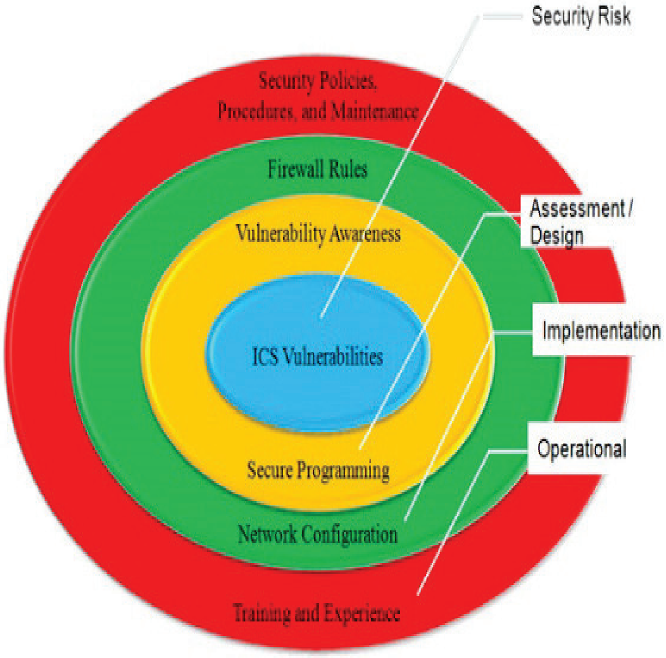


Figure 7.1 Defense-In-Depth Strategy

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.

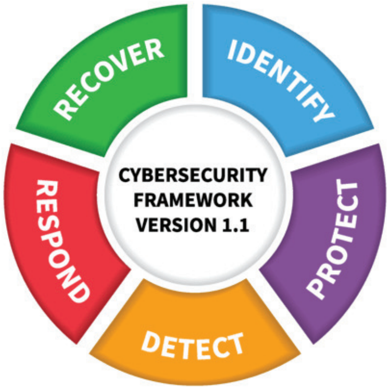


Figure 7.2 NIST Cybersecurity Framework

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

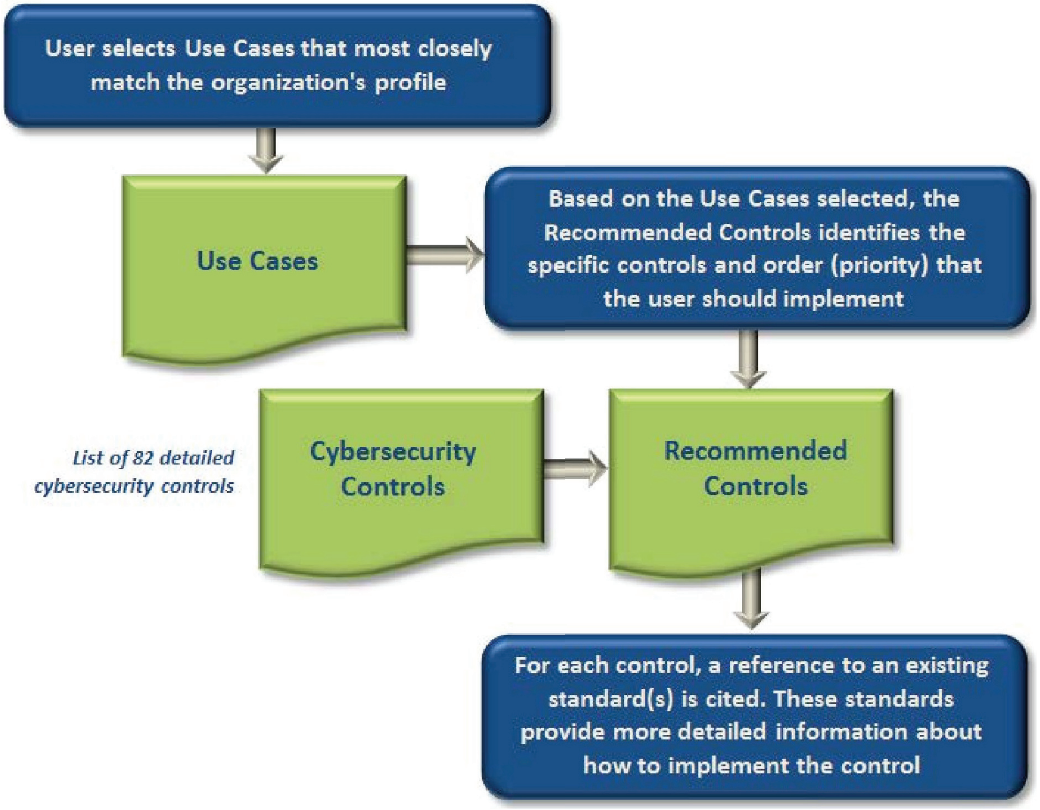
The AWWA Cybersecurity Use Case Tool was utilized to perform an initial analysis of the SCADA network. This tool is endorsed by the EPA as the minimum standard of care for cybersecurity compliance within the industry and was developed by the AWWA to provide water sector utility owner/operators with a 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

Based on the Use Cases selected, the Recommended Controls identifies the specific controls and order (priority) that the user should implement

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.

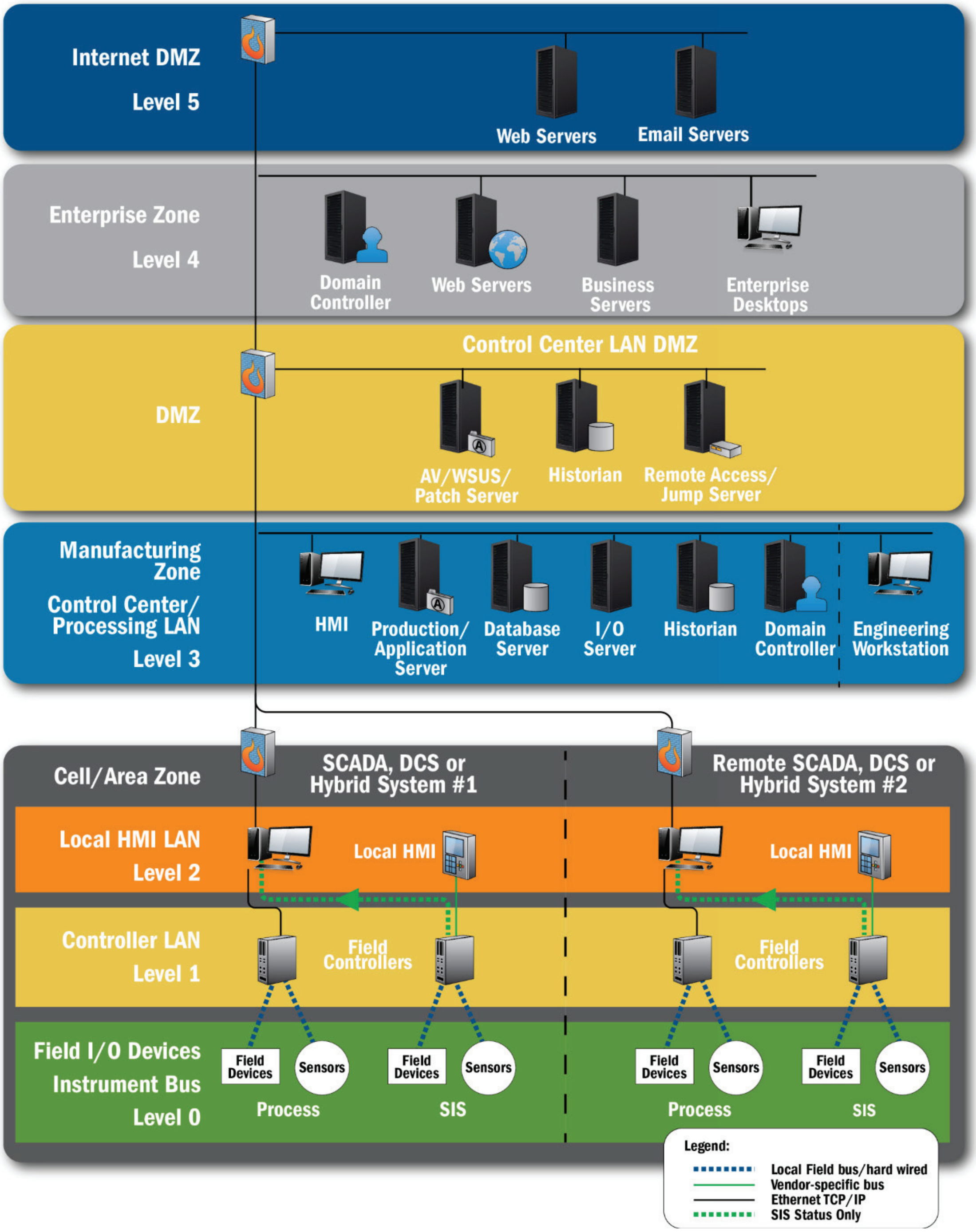


Figure 7.4 Title Recommended Secure Network Architecture

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