Systemwide Documentation to Prepare for Disaster Recovery

Mike Stoup and Mike Skrzypek

Pinellas County is the sixth most populated county, and the most densely populated, in the state of Florida. It maintains and operates two water plants, three wastewater plants, a solid waste facility, six pump stations, and approximately 330 remote lift and pumping stations to service the residents and businesses of the county. The supervisory control and data acquisition (SCADA) process control systems at these locations communicate using a combination of microwave, cellular, radio, and fiber optics as part of one large, comprehensive SCADA system.

In late 2015, Pinellas County Utilities received the results of a Department of Homeland Security (DHS) audit that indicated its SCADA system had missing and inaccurate documentation and lacked a disaster recovery plan. The utility contacted McKim & Creed to rectify the deficiencies cited in the report.

One of the first things mentioned during the initial call was the importance of the project, and the consultant team responded by reprioritizing staff to start working on the project immediately. Eager to resolve the issues identified in the report, the county requested to accelerate the schedule from four months to six weeks, targeting to complete the project before the end of 2015.

The project was executed using a combination of staff interviews, document collection and analysis, field research, vendor consultation, and Ethernet network diagnostic tools. The county staff was included as a major part of the project execution and played a critical role in providing documentation, making systems

Mike Stoup, P.E., is instrumentation and controls group manager/project manager with McKim & Creed in Clearwater. Mike Skrzypek is supervisory control and data acquisition/security systems manager, water and sewer division, with Pinellas County Utilities in Tampa.

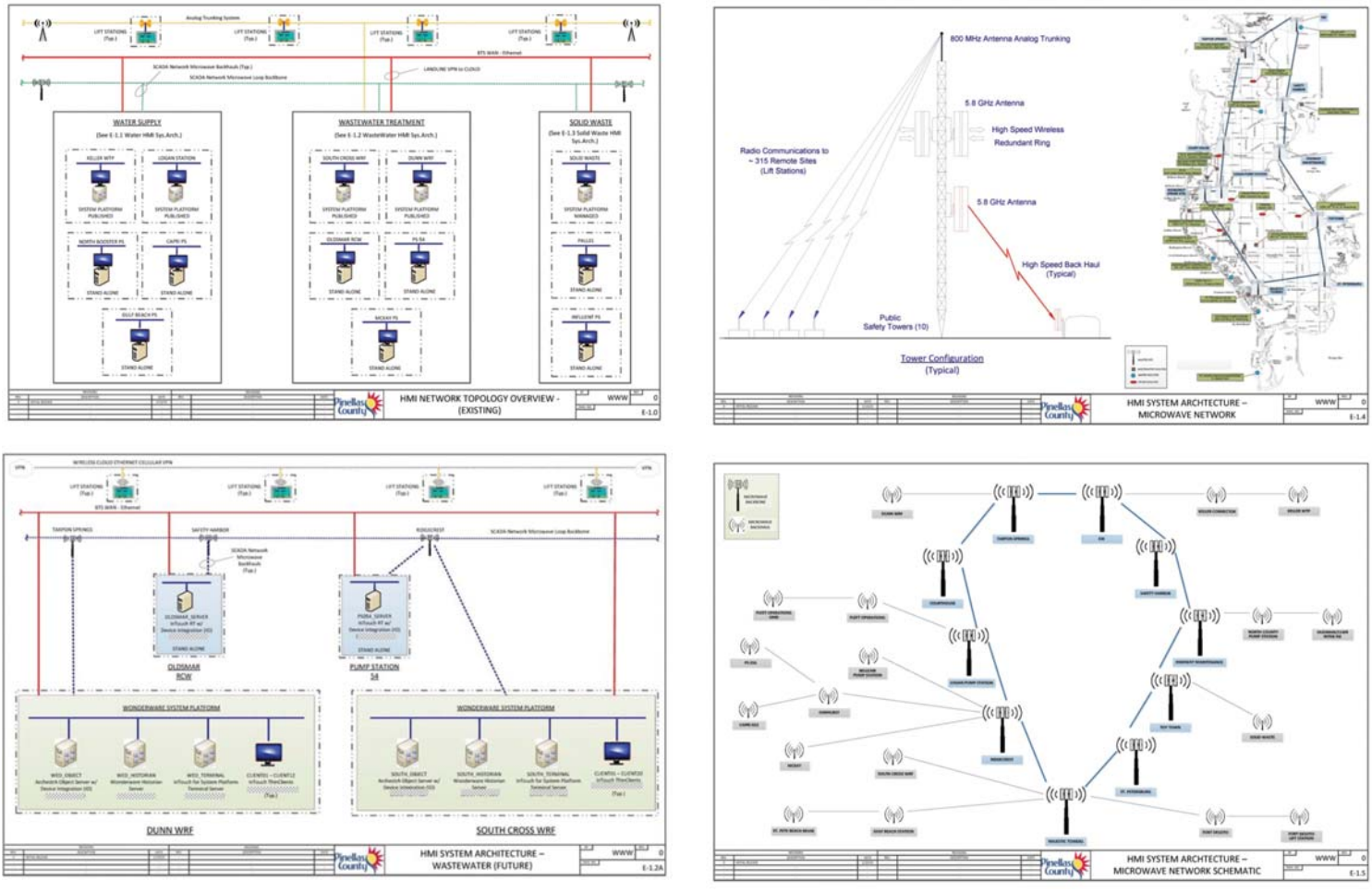


Figure 1. Network Drawings

available for research, and reviewing documents and drawings in a timely manner.

The deliverables of the project were detailed topological schematics of the SCADA system (both existing and future), a comprehensive SCADA network device listing, geographical location maps, and backup and restore procedures tailored to the county's SCADA visualization, database, and historical data servers.

The project deliverables were submitted on Dec. 18, 2015, two weeks ahead of schedule.

Existing Conditions

Two primary events within the county over the course of many years contributed to the conditions found when the security audit was performed:

1. During the previous few years, multiple integration firms had been hired through competitive bidding to perform SCADA projects for the county. The deliverables from these projects varied widely in substance and format, and were stored by project instead of integrated into an overall SCADA system design set. Similarly, the software implementation of SCADA system upgrades and additions varied by integrator and plant site, resulting in different programming approaches, deployment solutions, and software platforms.
2. The county had experienced a recent and sudden departure of a majority of the technical staff familiar with the SCADA system. Due to inadequate documentation, much of the SCADA system knowledge and information was lost when these staff members left the county. At the time of the audit, only two people remained on staff sufficiently familiar with the SCADA system for troubleshooting and general software maintenance.

Due to the integrator's focus on project deliverables, instead of the overall SCADA system design set, and with limited county staff, backups of the SCADA system after changes were made were rarely performed. Additionally, although offline backups had been performed, the county information technology staff had implemented firewalls that prevented live data backups, so they were only as accurate as they were old. A documented backup and restore practice was never developed, leaving only two of the staff familiar with performing the tasks. With little information available regarding the procedures to perform the system backup and restore function—in case these two individuals left or were not available—it would be extremely difficult for any contractor or any other technician to restore the application software in case of a software-related problem.

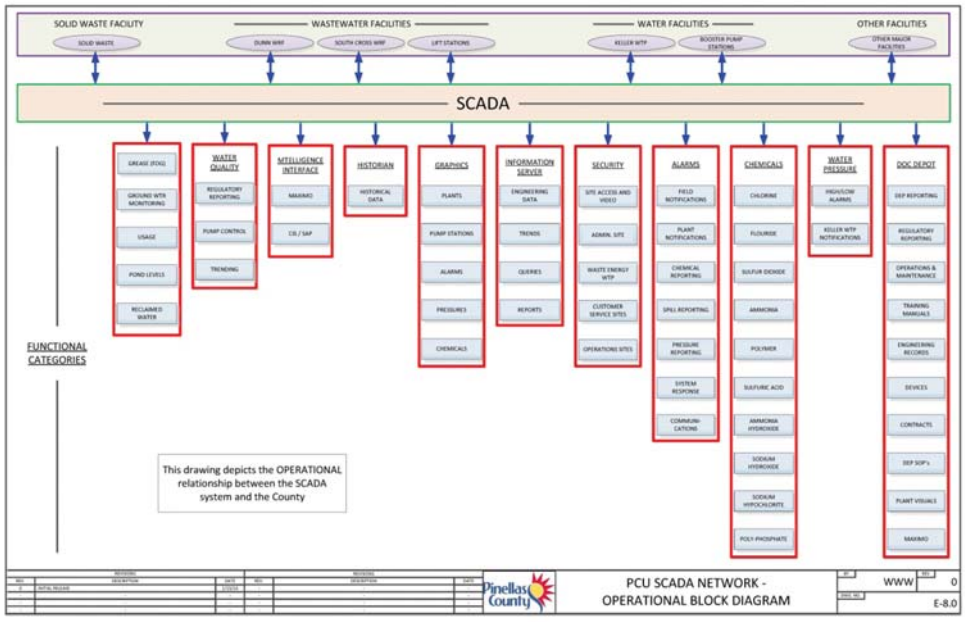


Figure 2. Supervisory Control and Data Acquisition System Operational Block Diagram

In addition to this, the county was preparing for a complete overhaul of its SCADA system communications to the remote lift and pumps stations over the next three years, converting from radio-based communications to cellular. Accurate documentation of the system, current backups, and the knowledge of how to restore them were critical before the overhaul began.

Project Justification

Many risks were identified as justification for the project. The SCADA system is the brain of the entire water and wastewater operation throughout the county. Loss of this system, or critical components of it, could be catastrophic. Risks due to system failures included extended downtime, environmental spills, contaminated water distribution, and financial penalties. The costs to repair or replace the failures, along with the financial penalties, could be immense, depending on where the failures occurred and how large they were.

The lack of available technical resources to repair or replace system failures, as well as available materials and components, were of great concern. The county has a long history with many engineering companies and integrators, but without accurate documentation or people who know the system well, its replacement or repair could be a lengthy and expensive process. Even with the right people, equipment, and hardware, reprogramming the SCADA system could take weeks or months.

Strategy for Project Execution

The first challenge was to define the scope of the project and the boundaries of research and documentation. The county's SCADA system is a large and complex entity, and it was important to focus the efforts on the primary goals. The scope was limited to the human machine interface (HMI) system and the networking between plants and remote stations. At the plant level, only Ethernet devices related to process control were included. Inclusion of the programmable logic controllers (PLCs) was discussed, but it was ultimately decided to leave them out of this scope. By focusing efforts at the HMI and network level, no process downtime was required for the research, and the scope could be completed within the required time frame.

Another consideration was the sensitivity of the project and the information that was to be collected and recorded. Network protocols, equipment locations, Internet Protocol addresses, and system configuration parameters needed to be protected from the public for security purposes. As part of the project execution strategy, the county took the role of data protection using its standard procedures and guidelines.

The overall approach was to work with county management, technical, maintenance, and operations staff, to find and review existing documentation, interview county staff, field research the SCADA system, and compile the information into one comprehensive set of documents, drawings, and procedures. The

Continued on page 8

Continued from page 7
county agreed to prioritize the project by committing staff resources to aid in the effort as needed, due to the critical nature of the project.

Finally, all documents, drawings, and procedures were submitted to the county in their native format for future use as a living document.

Project Execution

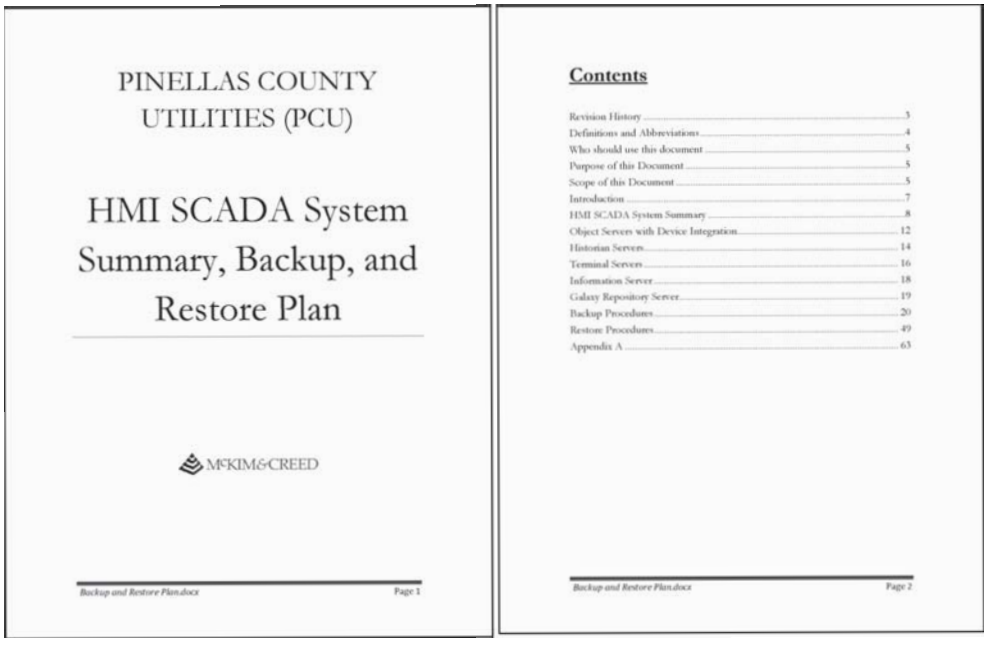
The first activity was to assemble all plant managers, utility management, and the SCADA technical resources within the county, as well as the consultant team, in a project kickoff meeting. At this meeting, utility management clearly defined the purpose, goals, and sensitivities of the project. This further ensured that all plant managers understood that consultant staff would need access to the plant SCADA systems and that their support was necessary, required, and expected. Points of contact were established within each plant to optimize the project communications. The decisions and directives were summarized in meeting minutes distributed to all attendees.

Data were collected over the next few weeks via field research, staff interviews, and collection and analysis of existing documentation. Each plant site was researched. The instrument technician assigned to each plant, along with the consultant team, located drawings and SCADA equipment, performed network identification queries, and shared knowledge of past projects and how they affected the SCADA system. In many cases, conflicting information was uncovered, and the engineer and technician had to dig deep into the system to determine the existing state of the equipment.

Members of management, technical, maintenance, and operations at each plant were interviewed. Each brought his or her own unique view of the SCADA system, its components, and its history. This inclusive research process ensured that every experience and story responsible for the current state of the system was identified. Once this information was gathered, it was cross-referenced and reviewed for inconsistencies and gaps. A review of existing documents revealed that the quality, format, and completeness of documentation varied widely from site to site.

The consultant team worked with Wonderware, the SCADA software manufacturer, to develop the customized backup and restore procedure. The county's SCADA system is a combination of the Wonderware App Server, which uses a single galaxy deployed across all plants, InTouch applications incorporated into the App Server galaxy, and stand-alone InTouch applications. The vendor's standard backup and restore procedure was used as a starting point, and the procedures were customized to the county's specific filename, path, and server information. This customized set of procedures eliminated the guesswork and inconsistencies when performing backups, and provided a faster and clearer set of procedures to be used during restore activities.

The draft documents, drawings, and procedures were submitted to the county for review and comment, and a workshop with its staff members was held to review their remarks. The results of the workshops were incorporated into the drawings and documents for final issue in native file format.



PINELLAS COUNTY
UTILITIES (PCU)

HMI SCADA System
Summary, Backup, and
Restore Plan

McKIM&CREED

Backup and Restore Plan.docx Page 1

Contents

Backup and Restore Plan.docx Page 2

Figure 3. System-Specific Backup and Restore Procedure

Deliverables

The deliverables included documents, drawings, and procedures specific to the county's SCADA system, and they were compiled into a single, comprehensive set of documents. All project documentation included a revision history section. Examples of project deliverables are listed in figures 1 through 4.

Potential Project Roadblocks

Due to the aggressive scope and schedule of the project, it was critical to identify potential roadblocks and address them before they could impact the project.

Technical and Operations Staff Refuses to Share Information

It is very common for the personnel responsible for maintaining operations to develop and keep their own set of documents, drawings, and procedures for use in troubleshooting and maintaining the system. These "shop drawings" are typically filled with hand-drawn information that does not exist on any other drawing. Because these drawings contain information that cannot be found anywhere else, and because these people are responsible for keeping the plant operational, they can be very reluctant to admit they have such a drawing set, let alone share it with anyone else. The information on those drawings, however, was exactly what was needed for this project to be successful.

Another possibility when documenting a system in this fashion is the fear of job security. The fear that "Once they know the system, why do they need me?" could have been a hindrance to this project.

In both of these situations, the practice of involving plant management in the project eased the concerns of staff, and neither of these situations were issues.

Operations Prevent Sufficient Access to System for Research

Being the brain of plant operations, SCADA keeps the plant running and can, likewise, shut it down. Depending on the type of information to be collected, it can be a requirement to have the system off so the right location or equipment can be accessed.

By purposely limiting the scope to the HMI portion of the SCADA system and the networking, the system could stay operational while the data were collected. Had the scope been extended to the PLCs, it is likely downtime would have been required to collect the necessary information.

Extensive Outdated or Missing Documentation

Years of project-focused deliverables resulted in disorganized system documentation that did not follow a standard and varied widely in quality; therefore, the availability and accuracy of documentation was highly unknown at the start of the project. With a system this large, a severely deficient amount of data would require extensive field investigation, which would be difficult, costly, and very time-consuming. The result would have been a much higher project budget and a much longer schedule.

Through multiple interviews and workshops, the collective knowledge of everyone was assembled into a single, comprehensive understanding of the system.

OBJECT SERVER BACKUP DIRECTORIES

ArchestrA Object Servers

Name	Location	Site ID	Server Full Backup Method	Notes
1. SOUTH_OBJECT	South Coast WRF	SOUTH/SCB	CLONE	
2. WED_OBJECT	Dunn WRF	WED		
3. KELLER_OBJECT	Keller WTP	KELLER		
4. WASTE_OBJECT	Solid Waste Facility	WASTE		

Software	Backup Type	Backup Method	Source	Backup Location - Software
DA Server ABTCP	File Backup Initial	Manual	Manufacturer Disks	
DA Server MBTCP	File Backup Initial	Manual	Manufacturer Disks	
IO Server MBENET	File Backup Initial	Manual	Manufacturer Disks	
Wonderware SMC	File Backup Initial	Manual	Manufacturer Disks	
Keyware DNP3	File Backup Initial	Manual	Manufacturer Disks	

Configurations	Backup Type	Backup Method (Section)	Source	Backup Location - Configurations
DASABTCP	File Backup Daily	Auto Windows Backup (A)		
DASMBTCP	File Backup Daily	Auto Windows Backup (A)		
MBENET	File Backup Daily	Auto Windows Backup (A)		
System Management Console	File Backup Daily	Auto Windows Backup (A)		
DNP3	File Backup Daily	Auto Windows Backup (A)		
Wonderware	Buffered as needed (store-forward)	Auto Wonderware		
Wonderware Intouch	File Backup Daily	Auto Windows Backup (A)		

Licenses	Backup Type	Backup Method	Source	Backup Location - Licenses
Wonderware	File Backup Initial	Manual		
Wonderware	File Backup Initial	Manual		

Figure 4. System-Specific Server File Locations and Names

Benefits of the Project

There were many benefits realized from this project, and future SCADA projects will continue to reap these benefits for years. The major benefits include:

Accurate Documentation of the SCADA System

The extensive research performed, information collected, and documentation developed resulted in a single, very comprehensive, and accurate set of documents, drawings, and procedures. These represent the most current state of the SCADA system.

Launching Point for Larger Planning Effort

Master and system planning require an understanding of the current system and the identification of the goals for the future system. A migration plan is then developed that details the transitional steps to accomplish the goals of the plan. This project lays a foundation for the planning project by identifying the current state of the system.

Better-Defined Scopes for Subsequent Projects

One of the first steps in executing a project is to determine the current state of the system to be modified. The documents, drawings, and procedures developed for this project satisfy that first step and will provide for faster project execution for future projects. Without this information, the bidding contractor will include assumptions and estimations, which turn into dollars in the form of contingency and risk avoidance. By having accurate documentation before project scopes are developed, the scopes can be more accurate and concise, thus limiting contractor risk, contingency, and the overall project budget.

Backup and Restore Plan for the System

Disasters can strike at any time, and all utilities must be prepared for the worst scenarios. Disasters can take on many forms: cyberattacks, weather-related events, manmade actions, accidental occurrences, and equipment failures. Even the smallest processes can have large operational impacts if they experience extended, unanticipated downtime.

A current backup of the system is critical to ensure that it can be returned to operation as quickly as possible. An accurate restore procedure, customized to the specific system, is as crucial as the backup, for without the ability to restore the system, the backup is useless.

Documents in Native Format

The documents, drawings, and procedures developed during this project recorded the existing state of the county's SCADA system; however, the county will continue to execute projects and SCADA will be part of the scope of those projects in the future. All documents were submitted to the county in their native format so they could be provided as part of future projects to represent the existing conditions. In addition, as part of future project scopes, contractors and integrators will be required to update the documents, drawings, and procedures that are developed with their project modifications. This will ensure the documents remain current, should they be needed for future projects or disaster recovery.

Conclusions

The initial purpose of this project was to address the issues discovered during a DHS security audit performed on the SCADA system at Pinellas County Utilities. During the execution of the project, and to meet the requirements of the audit report, the HMI portion of the SCADA system and the network were researched, reviewed, inspected, and documented. Furthermore, a customized backup and restore procedure was developed.

Once the data were collected and reviewed, documents and drawings were developed to represent the SCADA system. These were reviewed by the county in a workshop environment and resulted in highly accurate and thorough documents.

A backup and restore procedure was developed specifically for the county using its server, network, equipment, and software names and settings. This set of procedures clarifies the process of backing up and restoring the SCADA system, resulting in a more frequent and standard backup and a more guaranteed restore function.

Finally, the documents, drawings, and procedures provided to the county at the completion of the project were in native format so they can be easily updated during future projects by contractors, engineers, and integrators.

The execution of this project was a success due to the collaborative working relationship between the county and McKim & Creed. Furthermore, the early establishment of the expectations and importance of the project with county staff was critical for successful data collection.

This project addressed a serious deficiency in the county's documentation and maintenance of its SCADA system. This deficiency, during certain conditions, could have caused extensive downtime, environmental impacts, contaminated water distribution, other extensive costs, and financial penalties. By making the documents and drawings current with the existing SCADA system, and by developing a customized backup and restore procedure, the county is now prepared to return to operations should a condition happen to render part of, or the entire system, inoperable.