WEST YOST ASSOCIATES
Consulting Engineers

1/4/19

TECHNICAL MEMORANDUM

DATE: May 4, 2018 (Draft)
August 16, 2018 (1st Revision)
September 12, 2018 (2nd Revision)
November 21, 2018 (Final)

Project No.: 693-20-16-01
SENT VIA: EMAIL

TO: SRWA Technical Advisory Committee

FROM: Daniel Groves, PE, RCSE #7454
Joel Cox, CCNA, GPEN
Jeff Hesse, PE, RCE #53769 (Arizona)

REVIEWED BY: Andy Smith, PE, RCE #74673
Gerry Nakano, PE, RCE #29524
Lindsay Smith, PE, RCE #72996
Pat Ryan

SUBJECT: Operations Technology Preliminary Design

INTRODUCTION

The Stanislaus Regional Water Authority (SRWA) is planning to construct a new surface water treatment plant (WTP) as part of a Surface Water Supply Project (Project) to provide a new, supplemental drinking water supply to the cities of Ceres and Turlock (Cities). An agreement has been executed for SRWA to purchase raw water from Turlock Irrigation District (TID) for treatment and distribution to the Cities by SRWA. The majority of the conveyance and treatment facilities will be wholly-owned and operated by SRWA, however, several of the raw water facilities will be owned by TID but leased to and operated by SRWA.

Raw water will be withdrawn from an existing infiltration gallery (constructed and owned by TID) located within the Tuolumne River bed and pumped to the WTP from a new raw water pump station adjacent to the infiltration gallery via a new raw water pipeline[1]. Treated water from the new WTP will be pumped to the Cities in new finished water transmission mains. Together, these

[1] During future phases of the Project, a portion of the raw water in the pipeline may be diverted at a flow split structure within the WTP site and sent to TID's nearby Ceres Main Canal. Initially, however, such diversions will only occur on an emergency basis. The raw water pump station, raw water pipeline, flow split structure and Ceres Main Canal outlet structure will be owned by TID; SRWA will operate all facilities with the exception of the canal outlet structure.

facilities will comprise the Project's "regional water facilities" operated by SRWA. SRWA intends to design and construct the regional facilities utilizing a Design-Build (DB) procurement method.

PURPOSE AND ORGANIZATION

The purpose of this Technical Memorandum (TM) is to document the recommended approaches to operations technology (OT) design and construction of the Project, including secure data exchange between SRWA's, TID's and the Cities' facilities. In turn, this information is used to establish preliminary design criteria for a "Reference" OT system design. Design criteria and approaches presented in this TM are expected to inform the development of technical requirements for the DB contract that will govern the design and construction of the new SRWA facilities.

This TM is organized as follows:

- Introduction
- Purpose and Organization
- Background
- Data Exchange and Cybersecurity Requirements
- Preliminary OT System Design Criteria
- Preliminary OT Staffing Recommendations

BACKGROUND

An OT and cybersecurity kickoff workshop was held on February 20, 2018 with representation from SRWA, the Cities, TID and the West Yost Program Management Team (West Yost). The purpose of the workshop was to discuss current roles and responsibilities for staff members relevant to the OT systems currently in use by the respective organizations. The workshop also examined potential procedures for operational data exchange and interface between SRWA facilities, the Cities and TID. Additionally, the importance of cybersecurity when sharing data across different agencies was stressed. It was noted in the meeting that facilities overseen by TID's Electrical Department must comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards; facilities overseen by TID's Water Department may not be required to conform to NERC CIP, but careful consideration and coordination with TID will be required when implementing communications with these facilities.

DATA EXCHANGE AND CYBERSECURITY REQUIREMENTS

Because the SRWA project will require communication between four separate entities (SRWA, the City of Ceres, the City of Turlock, and TID), the compatibility, reliability and security of information exchange between the entities is of paramount concern. The following paragraphs describe the recommended approaches to data exchange and cybersecurity for the Project and its participants.

Based on discussion at the February 20th kickoff meeting and subsequent phone conferences with TID, a framework for data exchange between the SRWA and TID has been developed and is

documented in Attachment A. Data exchange and real-time control functionality exchange between SRWA and the Cities is shown in Attachment B.

The data exchange between the facilities (both TID and the Cities) will be handled by a secure communication method that can be monitored and controlled using enterprise-grade Information Technology (IT) equipment and implemented in a way that meets recommendations in industry cybersecurity standards for Industrial Control Systems. To ensure compliance with such standards, the design and implementation of the Project should adhere to the cybersecurity best practices identified through the use of the American Water Works Association (AWWA) Cybersecurity Guidance & Tool. More specifically, the DB contractor should utilize the AWWA tool and implement the resulting recommendations in the following manner:

- The DB contractor should use the AWWA Cybersecurity Guidance & Tool to document control system use cases for the Project, including a summary of why each use case is (or is not) applicable.
- The DB contractor should generate and submit the report using the AWWA Cybersecurity Guidance & Tool documenting all recommended controls.
- For each of the Priority 1 through Priority 3 controls recommended by the AWWA Cybersecurity Guidance & Tool, the DB contractor shall implement controls in accordance with the standards generated and/or referenced by the Tool for each specific control (e.g., NIST 800-53).
- The DB contractor should provide a summary for each the recommended Priority 4 controls explaining how the Regional Water Facilities will meet the recommended control, or recommended staffing for the SRWA to address the recommended control.

Adherence to the above requirements is expected to include, but not be limited to, conformance to the following industry standards and practices:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1
- NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-184, Guide for Cybersecurity Event Recovery
- ANSI/ISA-62443-2-1 (99.02.01)-2009 - Security for Industrial Automation and Control Systems
- Establishing an Industrial Automation and Control Systems Security Program (www.isa.org/standards)

The data exchange method must also be dynamic and scalable to accommodate additional data exchange needs (e.g., additional data points or changes in data exchange frequency) that may become necessary during operation of the Project.

The exchange of data required between SRWA, the Cities and TID necessitates a secure communications interface. The Reference OT System includes a Programmable Logic Controller (PLC) in a "Demilitarized Zone" (DMZ) with capabilities to communicate with controllers provided by the Cities and TID. In computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an "untrusted" network. Attachment B provides a high-level, schematic overview of the recommended system design for data exchange via network communications. The DB Contractor should be required to work closely with system integration staff and/or consultants employed by the Cities and TID to ensure that data transfer provisions are adequate, effective and executed in a timely manner. Such coordination should include the exchange of hardware, software, programming and configuration details identified for use by each agency.

PRELIMINARY OT SYSTEM DESIGN CRITERIA

Based on feedback provided during the February 2018 OT and cybersecurity kickoff workshop, the Reference OT system includes the following preliminary design criteria.

Criteria for Programmable Logic Controllers

PLCs will be Allen Bradley ControlLogix or CompactLogix[2]. Specific family and model numbers will be determined by the DB contractor during design development based on overall plan layout and input/output count developed by the DB contractor.

Criteria for Communication Pathways with Remote Facilities

Communications between the Raw Water Pump Station and the WTP, and between the WTP and the Cities' terminal storage facilities, are proposed to be via fiber optic cable. Depending on the time-sensitive or process-critical nature of communication links between facilities, non-leased wireless communications may be considered as a redundant communication path. It is assumed that the cables would be designed and installed with the raw and finished water pipelines connecting the various SRWA and the Cities facilities. If a redundant, non-leased wireless communication system is desired by SRWA and/or TID, final hardware selections for communications with the Cities and TID, as well as remote access, will depend on additional desktop studies and field reconnaissance (e.g., by a wireless vendor to determine the feasibility of using wireless communications between sites). It is assumed that final hardware selections can be determined after selection of the DB contractor, and subsequently furnished and installed by the DB contractor under a bid allowance item.

Although other options for communications between remote facilities are expected to be evaluated in design, the following key criteria are important for all field communications.

Reliability

Fiber optics provide a highly reliable and secure communication path. Other options including non-leased wireless communications can provide levels of redundancy, but require additional

[2] Final product selections will depend on the required functionality and input/output (I/O) counts of individual controllers.

maintenance, are susceptible to obstructions and weather, and generally require a recurring usage fee when using a provider network. Privately owned wireless networks generally do not have recurring usage fees, but require ongoing system monitoring and maintenance. Fiber optics are susceptible to damage during construction of adjacent facilities, which should be considered by SRWA during the evaluation of potential redundant communications systems (e.g., wireless).

Security

As an isolated communication medium, private fiber optic communications provide a high level of isolation from potential cyber threats. Wireless communications can be secured but may require additional configuration and monitoring due to the open nature of the communication path (i.e., air).

Cost

In design applications where piping between facilities is existing and trenching is required for installation, fiber optic communications is generally cost-prohibitive. In these cases, wireless options are preferred to limit initial capital cost. For this Project, given that pipelines are being installed, inclusion of fiber optic cabling with the pipeline is expected to add marginal capital costs, with significant long-term benefits. For reference, typical unit pricing for fiber optic cable installation (not including trenching) is approximately $2.64 per lineal foot (RsMeans) for direct burial cable. For the raw water, the Cities finished water transmission mains, this unit cost would result in installed fiber optics cable for approximately $10,000, $76,000 and $99,000, respectively[3]. Costs for wireless systems can range from $50,000 to $250,000 and are significantly impacted by types and heights of towers, line-of-sight and required bandwidth. Wireless systems that serve as backups to fiber optics generally have low bandwidth requirements due to the nature of the design intent.

Flexibility and Scalability

The need for data generally increases with time. Additional equipment may be added between facilities, including equipment with high bandwidth requirements like video monitoring and access control and monitoring. Fiber optics communications speeds can be upgraded by simply replacing the fiber optic transmitters on both ends. Wireless communications speed upgrades, on the other hand, are limited by the media (air) and generally require complete replacement of combined communication equipment (radios) system-wide in order to gain speed improvements. In general, wireless communications options (other than microwave) are not designed to support high-bandwidth equipment.

Criteria for Instrumentation

Criteria for instrumentation will be developed in tandem with process design requirements. Instrumentation criteria to be considered include wetted parts/materials, electrical requirements and integration with PLCs. Many instrument vendors offer “smart” instruments that communicate with PLCs via field bus communications. In general, “smart” instruments require additional

[3] The estimated lengths of the raw water, Ceres finished water and Turlock finished water transmission mains are 3,910, 28,800 and 37,500 lineal feet, respectively.

software and hardware to maintain, versus traditional instrumentation that uses "hardwired" signals to communicate with the control system. Selection of smart vs. hardwired instruments will be coordinated with SRWA staffing plans and the anticipated level of staff required to maintain the system, and appropriately denoted in the DB RFP technical appendices.

Criteria for Electrical Equipment Communication

Similar to instrumentation manufacturers, many electrical equipment vendors offer "smart" Motor Control Centers (MCCs), Variable Frequency Drives (VFDs) and other electrical equipment. In general, "smart" equipment communicates via a communication protocol (e.g., Foundation Fieldbus, Modbus, Ethernet) and require additional software and hardware to maintain. It is noteworthy that some equipment offers both hardwired control and communication elements for monitoring. As with "smart" instruments, the selection of smart vs. hardwired electrical equipment will be coordinated with SRWA staffing plans and the anticipated level of staff required to maintain the system, and appropriately denoted in the DB RFP technical appendices.

PRELIMINARY OT STAFFING RECOMMENDATIONS

SRWA plans to hire operations and maintenance staff for the WTP and associated regional water facilities. West Yost recommends developing a combined IT/OT department within SRWA to support the regional facilities with as-needed support from local, third party systems integrators for significant system upgrades or improvements. Staffing recommendations will be provided for the categories of system maintenance and support listed below:

- Instrumentation maintenance – Day-to-day maintenance of field instruments and analyzers.
- HMI maintenance – Minor updates and edits to software to address additional instrumentation and equipment. Also includes maintenance of underlying operating systems and HMI software for operational efficiency and cybersecurity.
- PLC maintenance – Minor updates and edits to controller programming to address additional instrumentation and equipment. Also includes maintenance of PLC firmware and software to address system maintenance and cybersecurity.
- Network communications maintenance – General maintenance and monitoring of network communications and activities, change control and cybersecurity monitoring and response.
- General IT maintenance – General maintenance of business systems including workstations, e-mail, files, printers and other general IT services.

Although estimates of the number of full time equivalent (FTE) staff for each category have yet to be developed, it is reasonable to assume that the responsibilities identified below can be met by no more than one to two FTEs. Detailed staffing requirements will be developed during the design and construction phases of the Project, in collaboration with the WTP plant manager and/or superintendent that will be hired by SRWA to oversee regional facility operations