Business Case Title: SCADA CRW OT Systems Administrator

Date: 11/21/2024

Total Cost: (2025 IT Grade 20 Employee and Benefit)

Submitted By: Shawn Griffith Operations AD

Department/Fund: SCADA –SCADA 50% Water/ 25% Waste Water/ 25% Water Resources

Rates/SDF Impact: Base Rate Charges

Request

The purpose of this request is to add a Supervisory Control and Data Acquisition (SCADA) Castle Rock Water Operational Technology Systems Administrator (OT Systems Administrator) Full Time Equivalent (FTE) to Castle Rock Water (CRW). This new position will allow for the SCADA team to manage critical servers, and data recovery systems, and provide 2nd level support for complex server and network issues. This position would be responsible for managing and maintaining CRW's virtual environment (VMware) as well as having a significant emphasis on implementing and maintaining an Active Directory for user authentication and security. This systems administrator will also be responsible for SCADA's Backup and Archiving system. The quantity of assets to be managed is approximately 415, with an approximate value of $2,000,000.

Background (Deficiency or Condition that exists)**:**

Castle Rock Water (CRW) has recently completed an in-depth update of its SCADA Master Plan (MP) for 2025-2029. This analysis assessed CRW's needs for instrumentation and controls, associated hardware and software, and the critical requirement for cybersecurity protocols and staffing.

The SCADA Master Plan (MP) identifies the need to hire a "Systems Administrator" in Section 5.1. This individual will be responsible for maintaining CRW's SCADA/Operational Technology (OT) servers, managing the SCADA domain, overseeing Active Directory, and ensuring the functionality and security of domain-linked computers, including client computers, and SCADA service laptops.

Currently, CRW operates a segregated network with no external connections to the internet or outside servers. This isolation is achieved through a Data Diode, which provides an 'air-gap' style of protection. The Data Diode allows for one-way communication with the Business/IT network, enabling information to exit the SCADA system without permitting external access.

This effective security measure will likely remain in place, albeit with some adjustments and modifications to enhance its functionality.

Due to this network isolation, CRW's servers, ASA switches, and computers require manual updates, as they cannot receive automatic updates from the internet. The Systems Administrator will manage these manual updates to maintain a robust security posture and protect against potential cyber threats.

In today's fast-evolving technological landscape, maintaining current tools and architecture is vital. Utilities, particularly in the water and wastewater sectors, are frequent targets for cyber-attacks, often following the patterns established in the power sector. As a result, water utilities are adopting similar protocols and equipment to enhance their cybersecurity defenses.

The design, maintenance, and protection of a SCADA system has evolved into a full-time specialty role. Therefore, the addition of a Systems Administrator is not just beneficial but critical to safeguarding CRW's operations against emerging cyber threats.

The recommendations below are excerpted from the SCADA MP 2025-2029 5.2 Staffing Gap Analysis Reasoning and Recommendations and the 7.2 Cybersecurity Gap Analysis and Recommendations ***(see Attachment A)***.

Staffing Gap Analysis Reasoning and Recommendations:

NO	GAP	Reasoning	Recommendation
1	SCADA Division Workload	The SCADA Supervisor and staff do not have the time and resources available to perform needed cybersecurity functions, including oversight/development of systems, policies, and practices, and analytical support for operational security optimization. An additional SCADA staff position is needed to manage both this work and facility security maintenance.	A SCADA OT Systems Administrator would manage the physical SCADA system oversight and equipment and facility maintenance functions.
2	SCADA Network & Server Experience	Current SCADA staff have very limited experience managing networks and SCADA system servers. The complexity of networks and servers requires dedicated staff.	A dedicated OT SCADA Systems Administrator would define clear responsibility guidelines for the SCADA network and servers. There is a unique distinction between IT and OT network engineers.

3	Cybersecurity Program Creation and Management	Federal cybersecurity regulations require a dedicated Chief Information Security Officer (CISO) to oversee both enterprise and ICS cybersecurity to develop, implement, monitor, and maintain cyber policies and procedures.	The SCADA OT Systems Administrator would be appointed Chief Information Security Officer to ensure that a cybersecurity program is created and that all Federal and State guidelines are met.
4	Cybersecurity Training Program	Cybersecurity knowledge is critical to prevent system risks, threats, and vulnerabilities. These risks and threats change daily. This training program will also be included in SCADA staff career progression documentation.	A dedicated cybersecurity SCADA staff member will develop and implement an ongoing training program specific to the needs of CRW.

The SCADA Master Plan 2025-2029 (section 7: SCADA Cybersecurity) also specifies additional areas of concern that would be addressed by the SCADA Systems Administrator:

- SCADA disaster recovery plan
- Demilitarized Zone (DMZ) upgraded firewalls
- Network Monitoring
- Complex password program
- Onsite server backups
- Facility network traffic policies

Narrative

The benefits of adding a new SCADA OT Systems Administrator to the SCADA staff are numerous. One of the biggest benefits, however, is realized in cost savings. Utilizing internal staff to assist with or even complete some capital projects would reduce the cost of the project from a capital funding perspective. As more staff are added, the workload on current SCADA team members will be alleviated, allowing time for SCADA team members to assist with capital projects. Several of the capital projects identified in this SCADA master plan update require CRW SCADA staff participation:

- Field tag update implementation project
- SCADA drawing standardization project
- SCADA specification standardization project

Program Description and Benefit to Customers:

The SCADA Master Plan outlines the need for cybersecurity as a way to protect CRW infrastructure and the Town's water supply. The Colorado Department of Public Health and Environment (CDPHE) evaluates and recommends physical security in the Sanitary Surveys, which are conducted every three to four years. When Sanitary Survey security issues are discovered, SCADA is expected to bring CRW into security compliance immediately. CRW has lacked upper-level staff with the specialty training and education required to oversee physical and cyber security issues.

This program description is supported and described in the SCADA MP 2020-2024 and 2025-2029, finalized in January 2021 and September 2024, respectively both were adopted and are shown below:

“The Castle Rock Water (CRW) Supervisory Control and Data Acquisition (SCADA) Master Plan is the starting point for the development of the CRW SCADA system functional requirements, which for this Master Plan includes cybersecurity, operational technology (OT), telemetry, backhaul, programmable logic controllers (PLCs), and human-machine interface (HMI). During the master planning effort, investigations were performed to determine all desired functions, features, and requirements for each subsystem (PLC, HMI, OT, cybersecurity, telemetry, backhaul). This Master Planning effort provides an opportunity to identify deficiencies within the existing system, consider new technologies, and document present and future system requirements.”

Next Best Alternative(s): Is there an alternative that would meet or partially meet the requested objective? Are there any consequences?
To enhance CRW’s OT Systems Administration, the best alternative is to subcontract oversight to a qualified firm. This would involve having a contract employee on-site dedicated to monitoring and maintaining the current SCADA system, thereby strengthening our defenses against cyber threats.

For the past five years, CRW has contracted Network Engineers, Systems Administrators, and Cyber Security experts. While this approach has had its successes—particularly in recommending specific devices and providing training on Best Management Practices (BMPs)—it has also revealed consistent drawbacks. The immediate availability of contractors has been a challenge, compounded by their lack of investment in CRW’s unique environment. While contractors meet their obligations, they often lack familiarity with our assets, their locations, and their critical importance.

To fulfill our vision of robust cybersecurity and operational efficiency, high-level oversight is essential. An active, informed, and responsive Systems Administrator with industry-specific technical knowledge is crucial for effective oversight. This individual would not only address immediate technical needs but also ensure that our systems are safeguarded against evolving threats.

In summary, having on-site support from a Full-Time Equivalent (FTE) Systems Administrator, complemented by contracts with qualified firms, will significantly enhance CRW’s ability to protect its systems and respond swiftly to challenges.

Approved or Rejected:

Backup Attached:

Attachment A: SCADA Master Plan 2025-2029 Chart 5.2 and 7.2.