Business Case Title: SCADA CRW Operational Technology Network Systems Engineer

Date: 11/21/2024

Total Cost: (2025 IT Grade 22 Employee and Benefit)

Submitted By: Shawn Griffith Operations AD

Department/Fund: SCADA – 100% SCADA Water/Waste Water/ 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 Network Systems Engineer (OT Engineer) Full Time Equivalent (FTE) to Castle Rock Water (CRW). This position will be responsible for assisting in the design, implementation, support, and maintenance of technology solutions in the areas of Operational Technology (OT) including industrial security controls, networking (switching, routing, segregation, subnets, redundancy protocols), firewalls and data diodes, servers, virtualization, and related technologies. This position will also assist in the development and implementation of cybersecurity policy, procedures, and regulatory compliance.

This position will perform these functions with minimal direction and will collaborate with various internal stakeholders and external consultants, contractors, and vendors as needed. 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 MP identified in Section 5.1 to hire a "Network Engineer", as the individual who maintains the network and maintains CRW's SCADA/OT servers. This person will also be responsible for:

- Implementing and maintaining operational technology solutions based on proven security architectures, including virtualization, networks, security platforms, and various other OT technologies.

- Participating in the design, documentation, implementation, and maintenance of Industrial Control System (ICS) networks.
- Securing ICS projects and processes, including backup and disaster recovery, following industry best practices, NIST guidelines for ICS security, and Castle Rock Water requirements.
- Install and configure network switches, routers, firewalls, virtualized servers, client workstations, and various cybersecurity platforms and tools.
- Provide support and troubleshooting for network communications, hardware, firmware, and security settings.

The need to provide current tools and architecture in the fast-paced environment of technology is essential. Cyber hackers have consistently attacked Utilities over the past few years. Power is a primary target and water/wastewater is a very close second. Water utilities have been able to learn from Power utilities and are now implementing many of the same protocols and equipment that Power uses. The design, maintenance, and repair of a protected SCADA system is now a full-time specialty job.

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)***.

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 Engineer would manage network and server security.
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 SCADA OT Engineer would be a dedicated Cybersecurity Engineer with the expertise to Implement and maintain cybersecurity procedures for complex SCADA networks and servers. There is a unique distinction between IT and OT network engineers.
3	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.

Narrative

The benefits of adding new technical team members 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:

- Data Diode replacement and implementation
- System segregation
- Cybersecurity- policies, equipment, and implementation
- Recommend and install servers and the replacement of end-of-life equipment

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."

It is essential to have high-level oversight with an active, informed, and responsive OT Engineer to fulfill this vision fully. A skilled OT Engineer with technical knowledge in the industry is essential.

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 SCADA System networks and servers, 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, an active, informed, and responsive OT Engineer with industry-specific technical knowledge is crucial for effective implementation and management. 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) OT Engineer, 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.