STAFF REPORT

To: Honorable Mayor and Members of Town Council

Through: David L. Corliss, Town Manager

From: Mark Marlowe, P.E., Director of Castle Rock Water
Shawn Griffith, Assistant Director of Operations

Title: **Discussion/Direction: Addition of Two New SCADA Positions, an Operational Technology Network Engineer and an Operational Technology Systems Administrator**

Executive Summary

The SCADA Master Plan (MP) was approved by the Town Council on December 17, 2019. The plan was updated in the 2025-2029 SCADA Master Plan in 2024. Additional needed work, not previously identified in the original SCADA MP scope, was included in the updated MP. Revised estimated costs for full implementation were updated to $15M. This cost may go higher and will be reviewed in the 3rd Quarter of 2025 by an outside firm.

The following program description is supported and described in both the 2020-2024 and 2025-2029 SCADA MPs, finalized and accepted in January 2021 and September 2024, respectively:

“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.”

As part of the 2025-2029 SCADA MP, finalized in September 2024, the document identified in Section 5.1, the need to hire an Operational Technology (OT) “Network Engineer”, as the individual who maintains the network and maintains CRW’s SCADA/OT servers as well as an OT “Systems Administrator”.

Discussion

The SCADA Master Plan outlines the need for cybersecurity as a way to protect CRW infrastructure and the Town's water supply. 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. CRW has lacked upper-level staff with the specialty training and education required to oversee physical and cyber security issues.

The OT Network Engineer will be responsible for:

- Implementing and maintaining OT 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.
- Installation and configuration of network switches, routers, firewalls, virtualized servers, client workstations, and various cybersecurity platforms and tools.
- Providing support and troubleshooting for network communications, hardware, firmware, and security settings.

The OT Systems Administrator will be responsible for:

- Maintaining CRW's SCADA/OT servers
- Managing the SCADA domain
- Overseeing Active Directory
- Ensuring the functionality and security of domain-linked computers, including client computers, and SCADA service laptops
- Manual updates, due to network isolation, for CRW's servers, ASA switches, and computers, 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.

The need to provide staff that can utilize 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 crucial to the safety of Town facilities and its residents.

For the past five years, CRW has contracted with firms that offer the services of 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, 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 SCADA environment. While contractors meet their obligations, they often lack familiarity with Town assets, their locations, and their critical importance to the operation of CRW.

To fulfill our vision of robust cybersecurity and operational efficiency, an active, informed, and responsive OT Network Engineer and System Administrator with industry-specific technical knowledge is crucial for effective implementation and management. These staff members would not only address immediate technical needs but also ensure that our systems are safeguarded against evolving threats.

Budget Impact

These two positions will be paid from the SCADA Water, Water Resources, and Wastewater funds through a first-quarter budget amendment, costs shown in the chart below:

Budget Year	**2025**	**2026**	**2027**	**2028**	**2029**
Annual Cost for two FTEs	$341,198	$356,455	$372,450	$389,223	$406,818

Staff Recommendation

Staff Recommends Approving the request for two new full-time equivalents, the SCADA Network Engineer and the Systems Administrator with a vehicle.

Attachments

Attachment A: SCADA OT Two Positions-Vehicle Worksheet
Attachment B: Business Case 2025 OT Network Engineer
Attachment C: Business Case 2025 OT System Administrator

2025-2029 Budget Request

Department: Castle Rock Water
Submitted By: Paul Rementer

Request Type Personnel **# of Vehicles** 2 **Year of Vehicle Addition** 2025

Request Name BCR for 2025 SCADA OT Network Engineer and a SCADA OT System Administrator

Is the requested expenditure one-time or recurring? One-time
Select the Strategic Priority addressed by this request:
Does this address a need in the community survey? If yes, please explain below
Does this address a level of service need? How do you classify this request?

Description and Justification

Please include details of the request and provide justification to support the need. Also address the following:
How does this align with Council established Strategic Priorities?
Explain how this will maintain your level of service. Or if this request increases your level of service please explain how and what the increased level of service benefit is.
How will the impact to your current level of service be measured?
Are there any alternatives or other potential solutions that would satisfy the need?
Please explain the operational impact if this request is not approved.
If a vehicle is needed for a new position enter a separate Budget Request

Estimated Expenditures

Personnel

Account Number	Acct Description	2023 Actuals	2024 Budget	2025	2026	2027	2028	2029	Total
Multiple-See Below	Personnel-Multiple			$ 341,198	$ 356,455	$ 372,450	$ 389,223	$ 406,818	$ 1,866,144
210-4200-442.61-23	Gasoline		78,950	$ 4,200	$ 4,200	$ 4,200	$ 4,200	$ 4,200	$ 21,000
210-4200-442.91-85	Vehicle Replace Program	352,135	394,208	8,974	8,974	8,974	8,974	8,974	$ 44,870
210-4250-442.40-33	Repair & Maint-Vehicles	370	430	1,584	1,584	1,584	1,584	1,584	$ 7,920
210-4290-442.91-80	Fleet Fund	238,832	285,000	40,000					$ 40,000
		-	-						$ -
		-	-						$ -
	Total Expenditures	**$ 591,337**	**$ 758,588**	**$ 395,956**	**$ 371,213**	**$ 387,208**	**$ 403,981**	**$ 421,576**	**$ 1,979,934**

Revenue Considerations

Account Number	Acct Description	2023 Actuals	2024 Budget	2025	2026	2027	2028	2029	Total
		$ -	$ -						$ -
		-	-						$ -
		-	-						$ -
	Total Funding Sources or Revenue Impacts	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**

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.

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.