City of Waterloo SCADA Modernization

Client	City of Waterloo
Version	3.0
Author	Brock Solutions
Reference	MG9068
Date	January 31, 2023

www.brocksolutions.com

Document Information

Revision History

Version	Date	Author	Summary of Changes
1.0	2022-12-21	Brock Solutions	Initial Draft
2.0	2023-01-24	Brock Solutions	Added Figure references
3.0	2023-01-31	Brock Solutions	Added section 5

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose and Audience

This report summarizes the inputs and deliverables for the SCADA Modernization project. For more details refer to the related artifacts below.

1.2 Related Artifacts

The following artifacts are related to the topics contained here within:

- Prior
  - City of Waterloo SCADA As Is Review.pptx
- With this scope of work
  - QMG10172CoW - SCADA Modernization.docx
  - MG9068 - SCADA Modernization Workshop - 2022.07.25.pptx
  - SCADA Modernization Functional Specification.docx
  - City of Waterloo - Cellular Network Study.docx
- Other References
  - Management of Alarm Systems for the Process Industries ANSI/ISA-18.2-2016: American National Standard: ISBD 978-1-941546-86-4
  - ANSI/ISA-101.01-2015 Human Machine Interfaces for Process Automation Systems
  - The Alarm Management Handbook: Bill Hollifield, Eddie Habibi: ISBN 978-0-977896-92-9

1.3 As-Is Review Highlights

A review was performed of the current system and identified the following themes in the findings:

- Limited Visibility
  - 99% Wastewater focus
  - WWTP Blind Spot
  - Storm Water System
  - External Connection Points
  - Cannot connect water and wastewater usage
  - Asset Maintenance Plan Data Lacking
- Security

- Physical security is present and functional at the stations; however, the Service Centre installation is accessible by personnel including non-wastewater resources
- Identity and Access Management requires management in multiple systems and third-party access is less transparent
- Change Management is lacking
- Vulnerability Management is informal and does not reflect current best practices
- City of Waterloo IT is not engaged for their services and expertise

- SCADA Support
  - Third Party Support
  - Lacking new ideas
  - No copy of code at CoW
  - Unsure on backups
  - Stressed alarm management
- Controls Environment
  - PLC & OIT modern
  - Similar Control Panels
  - Electrical Pump Control
  - Mix of MCC's
  - Minimal UPS monitoring
- SCADA
  - Vijeo Citect
  - Servers Windows 7
  - Clients – Tablet & PS OIT's
  - 3 months data SCADA
  - Historian long-term storage
- Network
  - Cellular networks (3G)
  - Unmanaged site switches
  - Growing with new devices
  - SCADA outside of domain
  - MGuard for Access Control

2 Visibility

Enable users to see the wastewater process at various levels of details, adjust operations, and view related systems.

2.1 Updated User Experience

Engaging users to make extensive use of the SCADA system necessitates understanding the requirements of each role, the nature of their workflow, and incorporating interface human factors.

2.1.1 Current Gaps

The current system has several significant challenges and gaps from a user experience perspective.

- The system is using a **dated**, old user experience approach. There is heavy use of text, tables, and colours.
- User experience **varies** depending on which platform is performing the function (Vijeo, Win911, OIT screen, SMS alerts from cellular modem). The user receiving differing levels of detail or text for the same event reduces clarity on how to respond.
- The current approach brings **users onto the server** to use the system and doesn't leverage any clients. When remote access is required VNC software is used to virtually hook the keyboard, mouse, and monitor providing a server level interaction.
- The remote access **tablet resolution is too low** and does not display the whole screen but requires scroll bars.
- Viewing report data or long-term historical records requires use of a second server leading to a **swivel chair experience**.

2.1.2 New Design

The new user interface is based on principles from the industry standard ANSI/ISA-101.01-2015 Human Machine Interfaces for Process Automation Systems, also known as High Performance Graphics. Many elements of this design have been used successfully in other water installations. The suitability of the design was confirmed with City stakeholders through workshops, review meetings, and feedback during the acceptance sessions.

Use of Colour

The scheme was developed with grayscale, reserving colour for display items requiring attention. At a glance, and at distance across the room, all grayscale and no colour denote a normal operating system with no alarms. Additionally, to adopt the individual user's style scheme for their operating system and applications there is a choice of either standard or dark mode backgrounds. Lastly, the approach also is helpful with the portion of the population who has colorblindness.

Use of Information

The design utilizes indicator graphics that display the normal ranges of operations to provide context for snapshots of data.

Keeping It Simple

Provide easy navigation buttons so that the user can move to the next process piece or drill down to extract more details. The system can be abstracted into varying levels of detail depending on if broader context is required or granular signals for troubleshooting. The levels are:

- Level 1 - Overview
  - High level view of the process
- Level 2 - Detailed View
  - Provides more details of the process
- Level 3 - Equipment Detail
  - Equipment specific
- Level 4 - Diagnostic
  - Detailed information about the device for troubleshooting

Declutter the display so that only the essential elements of the process are being shown.

Legend

Below is a sample of the common icons and their meanings (without animation).

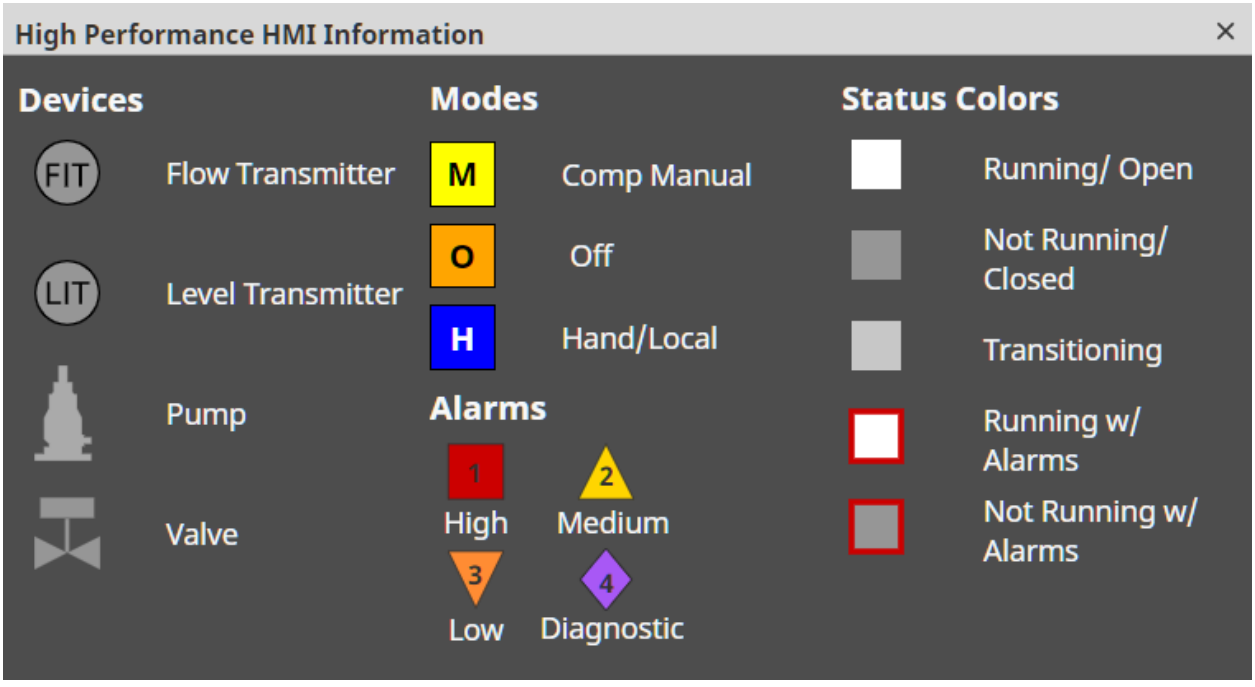

Figure 1: Sample Legend

2.1.3 Benefits

Using modern high performance industry standards and leveraging components of modern technologies brings the following benefits to the user experience:

1. Improves the user's abilities to detect, diagnose, and properly **respond to abnormal situations**.
    a. Dynamic colour is used to draw attention to notable conditions. Grayscale is used by default. Both light and dark screen modes are provided to the appropriate contrast level for differing environments.
    b. Alarms response is strengthened due to display elements invoking a stronger cognitive response since there are reserved for that purpose
    c. Various use cases are considered to minimize actions required (e.g., navigation steps and clicks)
    d. Data is presented in the units and fidelity required for effective operations
2. Enables **the users to be more effective** yielding improved safety, quality, productivity, and reliability
    a. Layout and display levels promote situation awareness
    b. Timely feedback is provided for user actions
    c. Error messages are descriptive
    d. Displays are used for more salient information and faceplate are used for more detailed data
3. The **needs of various users** are considered based on their varying job functions. Examples include reporting sections for secondary users and permission schemes based on role.
4. Elements and component are implemented in a **consistent** manner across the platform
    a. Applies within the project
    b. Applies between the Service Centre and the Pumping Stations
    c. Applies to notification elements (e.g., alarm tile, emails, and SMS texts)
5. Provides alignment with **industry best practices** as detailed in ANSI/ISA-101.01-2015 Human Machine Interfaces for Process Automation Systems

2.2 Scalable Integrations

Incorporating existing operational systems and keeping options open for future use cases and growth is in important factor when investing in a new technology platform. The selected SCADA platform provides a variety of common methods for connecting related systems.

2.2.1 Current Gaps

The current SCADA system has limited visibility into the broader context outside of wastewater pumping stations. **External and disparate systems** that can influence more effective operations at the City but are not present in the current system are:

- Storm water patterns
- Maintenance and Asset Management
- Quality systems
- Leak detection
- Geospatial and weather
- Clean water versus wastewater usage
- Engineering data (design and sampling programs)
- Connections to other jurisdictions (Kitchener, private pumping stations, St. Jacobs, Region of Waterloo WWTP)

2.2.2 New Design

The design considers the landscape of data sources, user clients, and external analysis tools. The following system drawing shows the relationship of the integrated components.

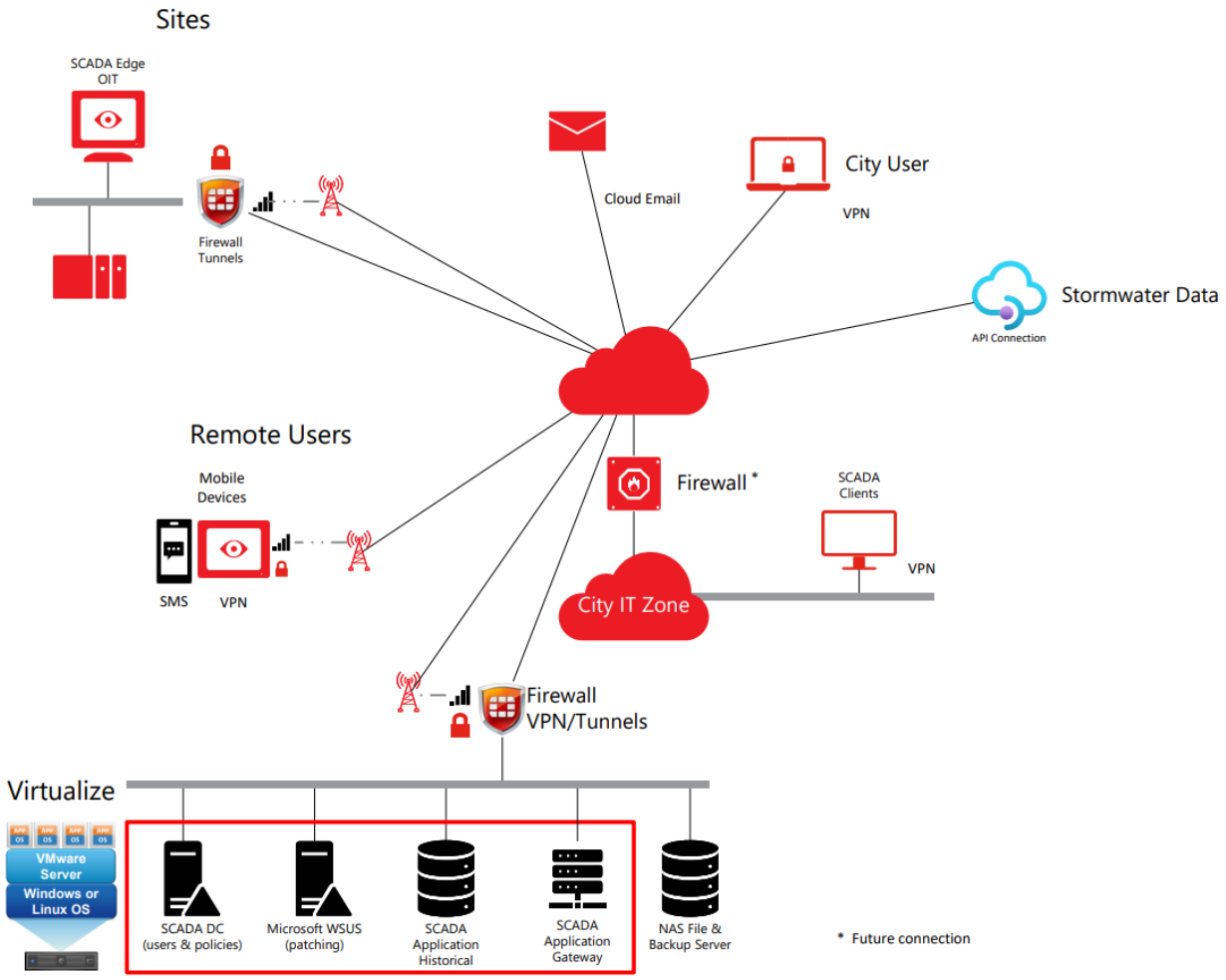

Figure 2: SCADA Architecture

External Endpoints and Integrations

The SCADA system obtains data from a few key sources but has the capability to incorporate other data streams. At the pumping stations the data items are populated via a set of core device drivers to read the PLC values. If different makes and models of PLCs are implemented in the future there are additional core drivers for the most prevalent PLC technologies and additional modules to incorporate driver software platforms for more niche scenarios (e.g., various OPC implementations). Similarly edge devices, IIoT devices, instruments can be integrated using PLC protocols or using MQTT, csv, json, etc.

The SCADA technology stack can also interact with relational or time-series database technologies (e.g., SQL) to display or broker external systems built on underlying databases (e.g., reconciling clean versus wastewater usage).

There are more details under the Alarms section, but external integrations include email, voice, and texting options enabling more forms of system connectivity and situational awareness for a broader user group in transit. Initially the email capability is being leveraged to generate both direct emails and texts.

As part of the initial considerations, storm water data is being integrated from two external sources. One source is the map background to provide geospatial context and the other external source is the consolidated field instrument data sets. The map background is populated from a GIS platform using geojson format and will be leveraged to provide the detailed area boundaries for the pumping station catchment basins. The storm instrument data sets are provided by a third-party cloud service and provided via an API web call returning a json data format. Storm water is a good illustrative example a single user experience within the SCADA platform and extends the historian and reporting capabilities developed for the wastewater use cases.

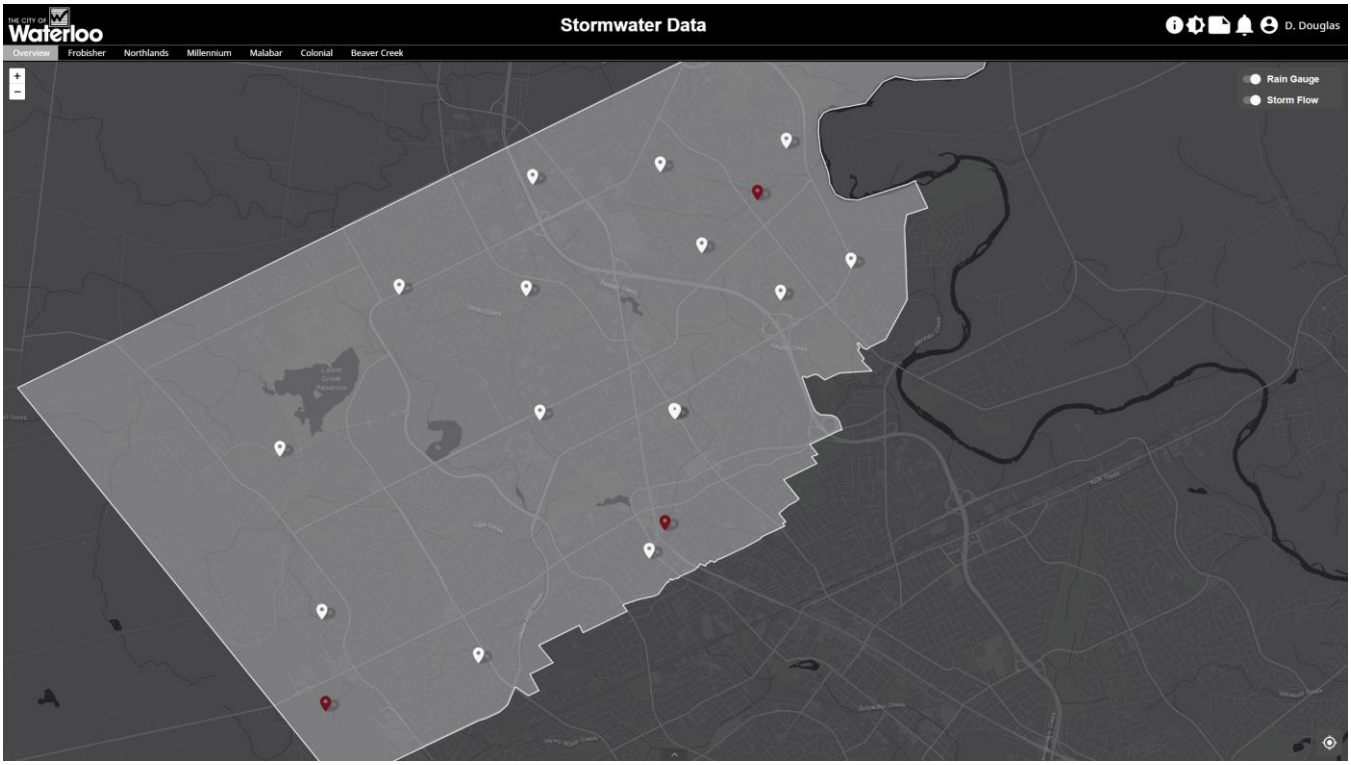

Figure 3: Storm Water Display

Leak Detection (Future Considerations)

The similar concepts and approaches for the Storm Water IIoT devices many be applied to lead detection use cases. Note the SCADA technology can support direct integration with edge IIoT field devices over many protocols including MQTT.

2.2.3 Benefits

The modernized SCADA implementation incorporates both new integrations and is a flexible foundation for future anticipated integrations:

1. **Storm water** instrumentation from external source telemetry is consumed, visualized, monitored, and historized. This modern platform supports these capabilities through:
   a. Integration of API endpoints flexible to various payload formats (xml, json, etc.)
   b. Geospatial widgets including the incorporation of GeoJSON

c. Value monitoring that can be used to trigger alarming and notifications
d. Time-series operational historian

2. **Export** of key data to Excel for offline analysis
   a. Alarms
   b. Alarm History
   c. User Event Log
   d. Process Analysis
   e. Reports for Pumps, Flow, and Generators
3. **Future integrations** with platforms leveraging database technologies. As other disparate systems are brought into a consolidated user experience, external systems that leverage modern technology stacks in the industry:
   a. Databases (SQL and related)
   b. MQTT (IIoT devices)
   c. Controller/RTU device protocols (native or OPC)
   d. Web services

3 Supportability

The new enhanced capabilities with alarms, alarming notifications, and the new online logbook will provide the City with modern tools to achieve greater supportability for operations.

3.1 Rationalized Alarms

This approach draws on guidance from standard ANSI/ISA-18.2-2016 Management of Alarm Systems for the Process Industries.

3.1.1 Current Gaps

The current alarm strategy and implementation was identified as being **stressed**. Some of the symptoms identified are:

- Lack of clarity to dispatch the correct personnel
- Alarms are reactive and not proactive
- Alarm fatigue from loss of communications events and weekly testing protocols

3.1.2 New Design

The new design approach for the alarm system followed guidance outlined in ISA standard 18.2 as well as the related book "Management of Alarm Systems for the Process Industries"

Fundamentally, an alarm system is about how control systems interact with operations. The goal is to avoid operational consequences by engaging operators to act. This is required when the process equipment or automation is unable to reject disturbances or experiences failures.

The performance of an alarming system is a function of both its configuration and its dynamics.

Design Principles

From an enumeration perspective the following principles were used to rationalize if the alarm provided value and which modifications would be required from the current configurations

- Does the occurrence require operator action?
- Is the alarm indicative of the situation's root cause?
- Is the alarm flagging an abnormal scenario (versus an expected transition between steady-state operational levels)?

Assumptions

The following assumptions are made to ensure that alarm has utility once it satisfies the design principles

- Notifies for events that require action.
  - One exception that the City opted for, stakeholders will be notified when the alarm is cleared

- Ongoing monitoring is still required
- Users are trained
- Enhances decision-based actions
- All alarms will be responded to
  - The system must not produce more alarms than operator(s) can respond to.
  - Alarms are not created solely upon assuming the operator will fail to respond to a different alarm.
- Alarm priorities dictate response order
- Alarms are kept up to date

Determining Priorities

For the purposes of triaging alarms and to determine level of response the following guidelines were used to determine alarm priorities:

Response Time

Time to Respond	Urgency	What This Means
> 30 min	Not Urgent	Re-engineer for urgency
10-30 min	Promptly	This alarm can wait while you queue up the next task
3-10 min	Rapidly	Quickly wrap your activity and proceed to the alarm
< 3 min	Immediately	Drop what you are doing and respond now

Pending Consequences

Impacts	Minor	Major	Severe
Safety	Highest Priority		
Report To	Department	City	Public Record
Costs	Minimal	Notable	High
Radius	On Site	Noticeable	Community

Mapped Priorities

Response	Minor	Major	Severe
> 30 min	Re-engineer for urgency		
10-30 min	Low	Low	Medium
3-10 min	Low	Medium	Medium
< 3 min	Medium	High	High

For faulted equipment and some events, a lowest priority designation of "Diagnostic" was added.

Alarm Historical Dynamics

The effectiveness of the interface between the automated process and operation alarms can be viewed through historical analysis. Patterns that can challenge operators and erode effectiveness include:

- Chattering alarm (on/off more than 3 times per minute)
- Fleeting alarm (short time in alarm)
- Stale alarm (in alarm for more than a day)
- Duplicate alarm (clusters of alarms due to common root cause)
- Bad Measurement alarm (instrument failure)
- Surges and Flooding (a burst of alarms)

Statistical and analytical observations showed some stress in the system:

- 9.4 per day, typically under 8 min
- Daily surges - Not flooding yet
- Problem alarms
  - Duplicates: Frobisher & Northlands
  - Fleeting: Generator & Power
- Most Frequent
  - (14) Northlands SCADA Comm
  - (22) Northlands Generator Running
  - (7) Malabar Low Alarm Level
  - (6) Colonial Comm Alarm
- No stale alarms

Alarm Durations

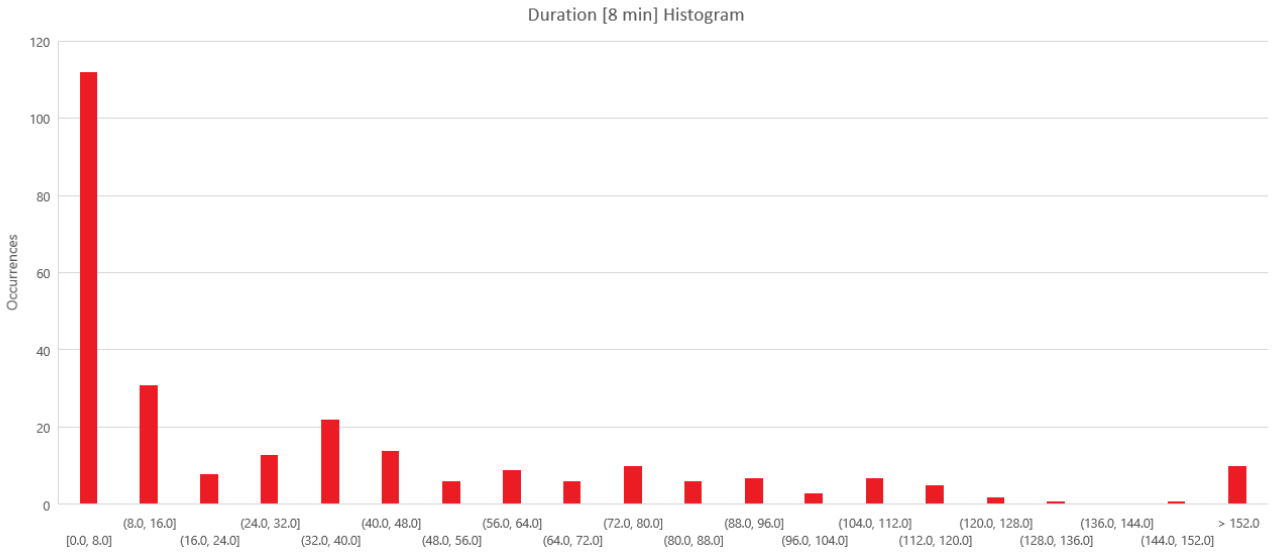

Figure 4: Alarm Durations

Alarm Occurrences

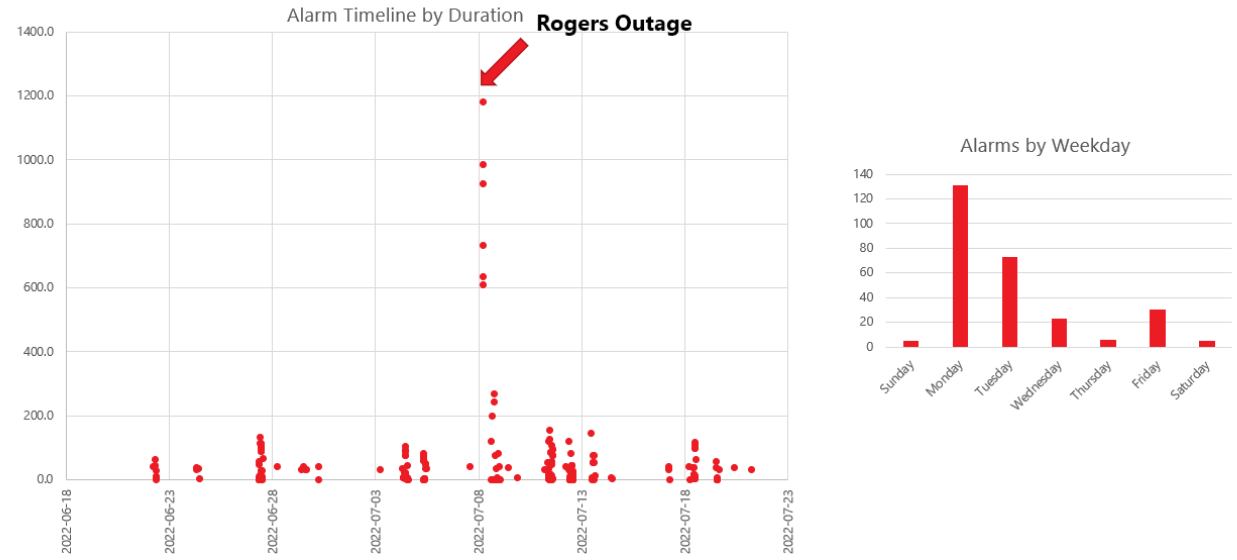

Figure 5: Alarm Occurrences

Note weekly testing is done on Mondays typically and is not readily distinguishable from real alarms.

Tuning of alarms currently is done in the PLC and in SCADA with an on-delay time and in a few cases analog signal deadband. There are opportunities to introduce off-delay times in the PLC if certain alarms chatter or are fleeting.

Alarm Configuration List

A list of currently implemented alarms was tallied with their configuration details from all current sources, which are loosely coupled with each other:

- Site devices
- Site OIT
- Texting from site
- SCADA annunciation on screen
- Emailing

Details were provided on the conditions and logic to trigger, the notification message, time delays, thresholds, parameters, and latching behavior. The rationalization of each enumerated alarm was facilitated through workshops and internal City sessions. Modifications included:

- Removing duplicates
- Clarifying message text based on the sources of the signals and likely actions to remedy the situation
- Reprioritizing based on urgency and pending consequences
- Adjusting triggers based on system dynamics

Notifications

In the new design alarms will be generated in the PLC, however modifications will be made in the PLC to allow for individual alarm acknowledgements. This has two benefits: better granularity and improved reset behaviour for latched alarms. Also in the new design, notifications will occur solely through the SCADA platform.

Several notification methods will used:

- On screen icons and indicators for key alarms or a flashing icon for sub-systems.
- Top display header will show an alarm status with the bell icon
- Bottom display footer tray will show individually any active alarms
- Alarms associated with a device are shown in it's device faceplate
- Alarm is displayed in Alarms tab of Alarms Display
- An alarm notification pipeline is executed
  - A set of users receives a notification via their primary method
  - Methods include email or SMS/text
- Priority of the alarm is denoted by explicit text, colour, and where displayed shape

Note that notification methods will be primarily executed at the Service Centre. If an individual station loses connectivity with the central SCADA server but still has internet access, the station/Edge OIT has the capability of generating notifications itself.

Below are the icons for process displays delineated by priority. Note the information is conveyed by shape, by number, and by colour.

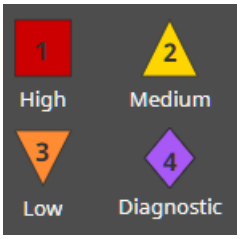

Figure 6: Alarm Priority Icons

Test Mode

Current practice is to exercise the process and the equipment weekly to fully trigger alarms. One of the larger drawbacks of this approach is that it requires communication and coordination to have the operations team supress their respond processes. The ensuing alarms then become a nuisance and are counterproductive is keeping the response reaction heighten for when actual alarms are triggered.

With the new design when a station is in test mode, the notification pipeline is automatically disabled, and emails and texts won't be sent. Alarms are still generated on the display for local observation to indicate the trigger conditions have been met. In addition, when the station is in Test Mode the alarm text is modified with a prefix of "TEST - " to highlight what conditions it was generated under.

3.1.3 Benefits

Performing alarm rationalization with the current processes and operations provides the following benefits:

1. Improved alarm response.
    a. Ability to triage response **order** by alarm priority and time of trigger
    b. Ability to optimize response **timing** based on urgency of potential consequences
    c. Improved **dispatching** based on enhanced descriptions versus current SCADA and SMS notifications
    d. Improved response **coordination** among managers, operators, and technicians with multi-user tablet and mobile phone integrations
    e. Relieve fatigue due to nuisance triggering and **restore confidence** in notifications
    f. Ability to **individually** acknowledge alarms and not retrigger active alarms
2. **Reduction in site visits** due to increased visibility into the process.
3. Improvement in **testing protocols**.
    a. Modify alarm descriptions to indicate generation during a test process
    b. Supress notifications to other users (i.e., no mobile SMS texts)
4. Reduction in configured alarms through **deduplication**.

a. Removal of duplicates in related systems (i.e., configured alarm in SCADA paired with configured alarm in OIT paired with)
b. Removal of duplicates in the same system (i.e., existing SCADA has abandoned-in-place duplicates)
c. Reduction in notifications by emphasizing triggering and avoiding notifying on acknowledgement or the clearing of alarms

3.2 Online Logbook

3.2.1 Current Gaps

Today's operational practice **uses paper**-based in-person on-site logbooks and taped sheets of paper to track:

- Communication notes
- Self-reminders
- Performance data
- Generator metrics

This system presents challenges in that it is only viewable locally, relies on its physical integrity, and needs to be legible.

3.2.2 New Design

The new design incorporates an onscreen text and attachment ledger that is stored with the central instance and therefore is viewable by all users thereby de-paperizing operations.

To create a new entry:

1. User clicks paper icon on the header
2. "New Entry" tab is selected
3. Relevant facility is selected (or none)
4. Text is entered
5. Optionally pdf, jpg, or png files may be attached using the upload icon
6. Submit by clicking "Add Entry"

To view entries:

1. Optionally type in text to filter by
2. Optionally sort data by column headers
3. Optionally use the vertical right scroll bar or mouse scroll
4. If an entry is selected or highlighted and if it has an attachment the "Download Attachment" button can be used to retrieve it

To delete an entry:

1. Use any navigation options from "view entry"
2. Once selected click "Delete Entry" button

To close the logbook:

1. Click "X" in top-right of the widget frame

3.2.3 Benefits

The data aspects of the paper-based systems are addressed through historian data collection and dashboards. The aspects of using paper as a communication tool have addressed through a Logbook component of the solution and provides the following benefits:

1. **Common visibility** - the notes may be added and viewed from any SCADA client, remote or local
2. **Integrity of Records** - the notes will be digitally stored and therefore will be stored and retained by the backup strategies with the rest of the system
3. **Legibility** - digitally entered information has the inherent ability to enhance fonts, colours, size, etc. to be more readable and not subject to penmanship or staining
4. **Contextual Enhancement** - with the feature of attached images, notes will have reinforced clarity with visual aids

4 Modernization

Adopting modern tools and technologies is a great starting point for enabling new capabilities and provides a better foundation for implementing current best practices. Additionally, modernization provides better operational resilience and resilience against cybersecurity threats.

4.1 Current and Widely Adopted Technology

4.1.1 Current Gaps

The technology components of the current SCADA system pose the following concerns:

- Overall, the City expressed a **dissatisfaction** with the tools in place to gain insights
- The reporting tool Dream Reports is **not well integrated** with the SCADA Vijeo platform
- SCADA **servers are obsolete**
  - Operating system is end of support
  - Hardware is at least 7 years old and susceptible to failure
  - No use of virtualization or containerization
- The current owner of Vijeo has other similar software products. It is **unclear** what the **roadmap** or long-term support model will be for this product.
- Software versions are behind in patching and **missing** important engineering and security **patches**
- Secure communication tunnels to the sites are dependent on the cellular modems which are past their best before date
- City users cannot be both on City networks and SCADA networks
- Data for analysis needs to be exfiltrated via a non-City account to transfer it to other City systems

4.1.2 New Design

The new design begins with a refresh of hardware for servers, OITs, and communications. As part of that refresh modern operating systems and software versions will be installed.

Virtualization

Virtualization is a well adopted and very beneficial approach for modern SCADA systems. The four servers that are identified in the SCADA as good virtual machine candidates are:

- SCADA domain controller - This will provide the management of users, groups, and operating system policies. Additionally, this server will provide DNS and time synchronization services for the environment.

- Microsoft patching server - This server will be used to pull updates from Microsoft and manage when and how they get applied to the centralized and remote sites. Using this tool will aid in more continual and disciplined update management.
- SCADA application and historian server - This will hold the main SCADA application that clients will connect into, the historian data capture functions, and the Edge EAM component.
- SCADA gateway - This holds the component of the SCADA platform that communications with device drivers to the PLCs.

This approach:

- **Decouples hardware lifecycle from system lifecycle**. In the future if hardware needs to be upgraded or replaced this can be done on the virtual host without necessitating resource changes in the guest machines. Likewise, if a virtual machine operating system needs to be upgraded that can be done in place or side-by-side with a new virtual machine without necessitating new or transitional hardware. Third, virtual networks add flexibility as network configurations can evolve a may need to put virtually repatched into virtual machines independently of host hardware.
- **Optimizes hardware resources**. When using a hardware based, non-virtualized environment hardware capacity must be sized for the maximum requirements of each server instance. This aggregates and exposes peaks costs. When hosting a virtual environment, the surges in hardware resource demands can be levelled out across all the hosted virtual machines.
- **Provides flexible management** due to virtual machine portability. VMs can be added, copied, moved, removed, backed-up, etc. as use cases are presented.
- Note containerization was considered but requires an elevated level of management and skills. Using virtual machine operating systems is a more familiar experience for the SCADA stakeholders and the City IT group has well established skills and procedures to support this approach on behalf of Water Services.

SCADA Capabilities

The selected SCADA platform includes many components and capabilities not listed below, but initially these are the items required to support the current design. Additionally the selected vendor has an ecosystem of partners which provide third-party components (including Brock Solutions). This ecosystem of capabilities supports integrations with **Analytics Platforms**.

- Standard Edition
  - Core
    - Unlimited: tags, clients, designers
    - Database connector
    - Drivers to talk to the station PLCs
  - HTML5 Based Web GUI - component to display screens to a web browser, mobile device, or desktop

- Reporting
  - Design and view within the same environment
  - Scheduling to automatically run
  - Publish to email, pdf, file share
  - This is a key capability for the **Data Visualization for Pumps** and can support reviewing pump metric history
- SQL Bridge - provides a method to interact with other database sources and to merge queries with PLC data
- Tag Historian
  - Stores time series data values
  - Works with both short-term and long-term data stores concepts
  - Supports purging of data work in concert with the **Data Retention Strategy**
- Alarms
  - Notification workflow including escalation
  - External methods including email (which is leveraged for SMS via carriers)
- EAM - facilitates central monitoring, deployment, and updating

- SCADA Edge
  - Panel - local OIT displays
  - Sync - provides the synchronization and resilience to the central Standard edition
  - EAM - facilitates central monitoring, deployment, and updating

Fit-For-Purpose Systems

Some functions of the new architecture are better served by fit-for-purpose technologies. In this design file storage and pumping station SCADA control are two key systems identified as great candidates for fit-for-purpose technologies:

- NAS file storage using a Synology unit
  - The file shares **support change management** and can preserve the last good state for the configuration of SCADA, network device, PLCs, and drives
  - Provide a **backup** mechanism and storage location working in tandem with the virtual servers
  - **Optimizes disk drive hardware** by using hardware specifications suitable for read and write operations and provides RAID based redundancy
- Site OITs
  - **Dedicated hardware** terminal - Use a large industrial rated touch screen to mirror at the stations what the user experience is on the central SCADA server.

- **Autonomous SCADA mode** - The SCADA Edge application has the capability to run disconnected when the central server is not available. This allows the pumping station to maintain its operational capabilities including sending alarms independently.
- **Shared Technology** - This reduces training, streamlines use of the system, and reduces development time for new features.

4.1.3 Benefits

The following benefits are available from this modern and broadly adopted technology stack.

1. **Optimized** host environment leveraging virtualization use cases
2. **Mobile** app that runs projects natively on lower resolution
3. **Flexible** to operating systems
4. **Flexible** to database source
5. SCADA platform **capabilities are modular** and can be sized to fit the current adoption level for what use cases are providing value.

4.2 Modern Best Practices

Refreshed practices can aid in aligning with many objectives including increased visibility, better supportability, and improved resilience.

4.2.1 Current Gaps

The following gaps have been identified with respect to modern best practices:

1. The user experience is dated and hard to read and hampers effectiveness (see Section 2.1.3)
2. Multiuse environments where privileges and functions are too broad and bring cybersecurity risks. Mixed functions include:
   a. SCADA server with
   b. SCADA client activities and with
   c. Designer software that can change code
3. Installed applications which are no longer in use
4. Use of remote presence (VNC) software in lieu of a proper SCADA client
5. Informal patching and update process
6. Formalized weekly rebooting of server
7. Duplication of applications and inconsistencies of the installations between the server pair

4.2.2 New Design

The new design incorporates modern best practices falls into several categories:

Enhanced User Experience

See Section 2.1 and Section 3.1 where industry standards are applied

Cybersecurity Concepts

- **Least Privilege** keeps digital activities within the guardrails of expected use cases.
  - SCADA clients only access the SCADA server with the protocols and network ports required to perform its function. Unrelated access to the servers is excluded
  - SCADA user roles have been rationalized to allow individuals to perform their tasks, no more and no less. An unauthenticated user mode has been implemented and the City is comfortable with that format of read-only access.
  - Domain and operating system maintenance is separated to other servers (DC and WSUS)
  - Site to central communications is a key capability and site to site communication is not provisioned for. Locations will continue to be segmented within their own subnets.
  - SCADA components will not have any access to or relationship with City networks implicitly since City capabilities will not be leveraged at this time. The City user on City networks will have a similar user experience to the work-from-home scenario.
  - PLC software will be separated from the SCADA installation. It is recommended that the servers stay separated and don't adopt an additional engineering workstation role.
  - Fresh install which avoids remote presence software (e.g., VNC) which is over privileged for what is required (as a SCADA client)
  - Fresh install which cleans up abandoned software in the legacy system
- **Vulnerability Management** will be equipped with improved tools
  - Microsoft patching from a patching server and guided by group policies
  - The SCADA EAM module will facilitate central management of the Edge installations at the stations
- **Monitoring & Auditing**
  - The SCADA platform will contain a system log and user event log which will aid in troubleshooting the timeline of changes.
- **Improved Alarm Statistics**
  - The SCADA platform will keep a log of all alarms events which will aid in providing useful analytical data. The data can be used to determine the frequency of a particular alarm that may require more attention than others.

4.2.3 Benefits

The following benefits are realized by using best practices from a leading technology provider:

1. Modern best practices include the benefits outlined for High Performance Graphics in 2.1.3
2. Mobile devices are supported through several methods
   a. Screens that render on both desktop clients, tablets, and phone
   b. Notification component that can send messages to email or to SMS
3. Centralized and consolidated to streamline administration and support
   a. Pumping station OIT (a.k.a., Edge) installations can be managed from a central console
   b. Users can be provisioned and deprovisioned from SCADA Active Directory
4. Methodologies and configuration portions of the solution have been developed, commissioned, and production-proven in the water industry with other solution spaces.
5. Use of virtualization technologies to provide flexibility in backup strategies and greater ease in migrating through iterations of uplifted hardware

4.3 Resilient Operations

Operating critical infrastructure requires a high degree of availability and resilience of the overall system to perform its intend functions.

4.3.1 Current Gaps

The current SCADA infrastructure suffers from multiple resiliency concerns:

- SCADA **servers are obsolete**
  - Operating system is end of support
  - Hardware is at least 7 years old and susceptible to failure
- Site communications through **cellular is a single point of failure**, does cause data loss, and 3G is becoming obsolete
- Applications are obsolete and would be a **challenge to rebuild**
- **Lack of backups** to recover from

4.3.2 New Design

The design elements address many of the failure modes of the wastewater system.

Equipment

- Equipment Availability - The SCADA design and screen employ colours and alarm notifications to indicate when equipment is not available to perform its functions including faults, hand mode, and duty sharing
- Equipment Performance - A piece of equipment may be available to perform its function but still may be ineffective if its performance level is degraded. SCADA design displays

realtime values and historian trends to indicate performance levels. If performance levels degrade too much process alarms will trigger and notify personnel.

Site Integrity

- The automation design has signals for both building intrusion and for extreme indoor temperature through SCADA alarms.
- Auxiliary power systems such as a site generator are included in the SCADA signals and alarms.

SCADA as a Visualization Platform

- The PLC controllers continue to be the primary mechanism for managing and controlling the process. If disturbance levels are minimal the station can run without any SCADA for a period.
- SCADA configuration does not incorporate process logic but may issue optional commands, adjust parameters, and reset latched alarms.

Service Centre as an Operations Hub

- The Edge installation of the SCADA platform by design can operate from the remote hub autonomously
- Notifications for alarms can continue to be sent out if internet is available
- Data is preserved and forwarded to the hub later as long as the OIT has available disk storage

Site Connectivity

- A separate activity during this scope of work surveyed cellular signals and network performance for the sites. On of the key findings is that 4G LTE is feasible and would help move away from 3G which is targeted to be deprecated shortly.
- Increased reliability and performance can also be gained by using a cabled land-line connection as it would be less susceptible to over the air signal disruptions and provides higher bandwidth rates.
- In either scenario ensure the service carrier or provider is aware that this service connection is for a critical infrastructure operation. This would enable them to provide an elevated level of support and service to meet the mission.
- The City will continue to maintain a separate and distinct street connection to the SCADA environment at the Service Centre. This decouples its network configurations and access from the management of the City systems

Site	Inside Panel	On Panel	Outside	Recommendation
Colonial				Rogers On Panel + Bell or landline
Malabar				Rogers On Panel + Bell or landline
Millennium				Rogers Outside + Bell or landline
Northlands				Rogers On Panel + Bell or landline
Frobisher				Rogers On Panel + Bell or landline
Beaver Creek				Rogers Outside + Bell or landline

Figure 7: Summary of 4G LTE Performance by Antennae Mounting Location

Legend

- Blue - Bell recommended
- Red - Rogers recommended
- Green - Both Bell and Rogers would be viable
- Black - Both Bell and Rogers offer poor or inadequate speeds.

Distinct Clients

- Since servers will not be used for the client sessions, clients accessing the SCADA application may be interchanged with each other. The failure of one client does not impact or preclude the use of another clients
- Client requirements are flexible and light allowing the rapid provisioning of additional client devices as needed. It is flexible with respect to operating system and form factor (desktop, laptop, tablet, or mobile). Some graphics and displays may experience a diminished user experience at lower resolutions but at a general level client access is streamlined.

Hardware

- Since virtualization feature will be leveraged, the system has a tolerance for hardware failure and can be restored (versus reinstalled) on new hardware should the virtual host fail.

- Using a NAS that support various RAID formats the file storage and backups can still be available and preserved during a disk (or cluster) failure. Additionally, hot swappable disks allow for dynamic refresh of disk capacity.

City Outage

- If the City networks experience an outage the SCADA will continue to operate independently. Clients can connect in as a remote connection.

Disaster Recovery

- As change management processes mature, the NAS will be able to store snapshots of PLC and SCADA code for recovery. In addition, it can act as a staging point for off-site storage processes.
- The NAS can facilitate and be a destination for SQL database backups
- Th NAS can facilitate and be a backup for virtual machine backups

4.3.3 Benefits

The City will benefit from improved resilience given improvements to the system architecture:

1. Uplifting to a more **modern communications** method (4G LTE) will avoid end-of-service issues, leverage more modern infrastructure, and improve data throughput.
2. Improved **independent operations** at the pumping stations with the enhanced user experience at the Service Centre being mirrored at the sites including screens, alarms, and notifications. Sites will have the capability to run without the Service Centre being connected or available.
3. Improved **application availability** from virtual host hardware redundancies (e.g., RAID10 storage)
4. Enhanced **data capture** from store-and-forward value read at the remote stations using the SCADA Edge solution
5. Improved **data persistence** from fit-for-purpose NAS and RAID capabilities
6. Improved **disaster recovery** from automated system and data backups
7. Improved **change management** controls through periodic configuration backups
8. Enhanced **auditing** capabilities both for key process value via the historian and through user event logs to document actions taken by personnel

5 Cost Impact

With the re-prioritization of alarms and the enhanced remote access, cost savings are expected to be realized upon implementation of the modernized system. Additionally, it is anticipated that the upgrade to a 4G communications environment will reduce the communications alarms, that currently are the most frequently responded to alarms.

Table 1: Estimated Cost Savings from 2023-2026

Item	**Estimated Annual Savings**			
	2023	**2024**	**2025**	**2026**
Operational Response	$13,600	$13,600	$13,600	$13,600
System Administration Support	$7,950	$7,950	$7,950	$7,950
Cumulative Total Cost Savings	$21,550	$43,100	$64,650	$86,200