Elgin/Lake Huron SCADA Upgrades
SCADA Standards
Section 500 Software Programming Guidelines

Version	Date	Description of Revision
v1	March 7, 2006	Preliminary Draft
v2	March 22, 2006	Second Draft
v3	December 2006	SCADA Tender Version
v4	May 2009	Fourth Draft
v5	August 2010	Final Draft
v6	January 2011	As Recorded

Elgin/Lake Huron SCADA Upgrades
SCADA Standards
Section 500 Software Programming Guidelines

Table of Contents

501 General Software Programming Requirements

1. General

1. The overall objective of the software programming standards is to ensure that all modifications are consistent with the overall software design and architecture.

2. As much as possible, all software subroutines should be based on the existing Joint Board, standard modules.

2. Hardware Redundancy

1. At the Elgin Area WTP and the Lake Huron WTP, the facility SCADA systems consist of redundant ControLogix PLC and redundant SCADA Servers. The software configurations to include hot standby switching upon a hardware failure, with no impact on the historical data collection or real time control.

502 Network Communication Configuration

1. General

1. This document is a standard specification for a communications protocol to be used by the various SCADA systems. It should be used as a guideline when installing new systems that must communicate over a LAN (local area network) or a WAN (wide area network).

2. TCP/IP - Addresses

2.1 PLC

1. Each node on a PLC communications network must have a unique address on that network. Node addresses shall be chosen to integrate into existing networks. Nodes shall be assigned in consecutive node addresses. PLC's in hot standby shall have duplicate node addresses to allow for continuous data collection in the event of a PLC failure.

2.2 SCADA Computers

1. Each SCADA Computer located on either the local area network or wide area network shall have a node address that allows it to be integrated into the existing network. SCADA computers configured for hot standby will have consecutive node addresses to allow for proper operation in the event of a system failure.

3. TCP/IP – Local Area Network/Wide Area Network

1. Each device on the local area network or wide area network will have a unique address. There will typically be two distinct SCADA LANs in each facility with one being used primarily for PLC to PLC communications and SCADA to PLC communications while the second will be integrated with the wide area network and allow for remote data monitoring and data manipulation between remote sites. This configuration will limit unnecessary traffic on the wide area network to minimize costs incurred with charges that are based upon traffic. Typically speeds on the local area network will be greater that with the wide area network and will have a higher level of reliability.

4. Network Configuration

1. Program all network equipment to enable the required VLAN'S, layers of Quality of Service, firewall, routing, and network redundancy.

2. The network programming to include the implementation of the OPC server for each switch and hub then transferring 10 key parameters per device into the SCADA Server database. Also include an overview graphic for each plant, and each group of remote sites, that indicates the current network performance and status. This includes monitoring the network switches at all of the remote sites.

3. For the firewalls, routers and switches, provide a table of the following parameters
   a. Connected device name and description
   b. Interface / Port
   c. Speed (10 vs. 100)
   d. Duplex (half vs. full)
   e. Media (FX vs. OTP)
   f. VLAN(s)
   g. Pruned VLAN(s)
   h. Quality of Service Priority

503 PLC Software

1. Standard Requirement

1.1 Introduction

1. This document is a guideline to the structure and documentation of PLC programs. PLC shall be used as a common term for both RPU and RTU.

1.2 Purpose

1. The purpose of this document is to establish standards for a consistent approach to programming. Consistency will enable:
   a. maximum re-use of programs
   b. reduced time to troubleshoot programs
   c. more confidence and usability of PLC-based control systems.

2. Application

1. This standard applies to all PLC's, which contain custom programs.

3. General

3.1 PLC Programming

1. PLC programming is to include system signals for monitoring the health of the communication link, detecting the PLC faults, alarming I/O points failure, AC power failed, errors during tasks execution, etc. All of them shall be assigned as critical alarms for immediate attention.

2. The PLC programming logic consists of three (3) blocks. The first block completes the mapping of the input signals to software equivalents. Next is the process control program and the last block consists of the PLC/HMI Interface mapping.

3. The field input/output block performs the following functions:
   a. For all DI, where required, a 1-2 second debounce timer is included.
   b. For all AI, the raw values are converted to engineering units.
   c. All DI, AI, DO, and AO are mapped to internal bits, which are then used throughout the PLC software.
   d. The internal bits are used to map into the PLC/HMI interface table where possible.

4. The PLC/HMI interface table, within the PLC program, collects and consolidates all I/O that must communicate between the PLC and the HMI software. This translator/mapping table shall be the only location that the HMI, or other PLC's, communicate with the PLC program.

5. In some situations, values are communicated directly between PLC's, or between an PLC and its related field bus/Ethernet/serially connected, field devices. Provide separate I/O interface tables for each communication interface.

6. The process control program, where appropriate, shall use either Ladder Diagram, Boolean and Math Operators, Modules, Function Blocks, or a combination thereof for programming sequential or digital logic. Programs shall be executed under multi-tasking environment with appropriate priority, monitoring and control. The preferred language is ladder logic whenever possible.

7. The software programming standard is to be based on the library of process control programs capable of controlling specific unit processes. The process control library shall contain function blocks, subroutines, or modules, which can be used extensively in order to simplify software implementation and maintenance. The process control library consists of, at least, the following functions as a minimum:
   a. Remote/Local control operation of all connected equipment using the device I/O standard modules;
   b. Alternating pumps based on duty cycle or failure;
   c. Alarm detection and annunciation c/w "Acknowledge", "Reset" and "Test" Pushbuttons' functions;
   d. Interface with local HMI or keyboard display;
   e. Program Flow Control (Proportional – P, Proportional plus Integral – PI, Proportional plus Integral plus Derivative – PID);
   f. Lead/Lag module to dampen analog signal;
   g. Averager, Totalizer, Integrator, Calculator, Comparator, etc.;
   h. Accept and store field data from field device;

i. Time and date stamping critical alarms.

8. Additional program standards are as follows:
   a. Use the status of any field input only once at the beginning of the ladder to drive the status of a logic relay/bit or register/word (point). Rungs that perform this "translation" of all field inputs form the top section of the ladder. Logic points are then used in all later rungs, rather than the field inputs.
   b. Use only logic points in the second section of the ladder. This section contains the rungs that form the actual control logic.
   c. Use logic points to drive the field outputs in the third section of the ladder. Place any field output coil as an output in only 1 rung.
   d. Place all checks for device response together with a timer for each. Certain controllers have a built in function to do feedback checks, so this section may not be necessary.
   e. Group all registers/words and relays/bits that are of interest to monitoring personnel in sequential blocks. This includes setpoints, timer limits, tuning constants, and status flags. This simplifies the transfer of this data to supervisory systems. Maintain the "translated" field inputs (as per B above) in separate block(s) from other data.
   f. Use constants in the code only where it is unlikely they will ever be changed.
   g. Layout I/O points having functions for successive devices in identical, consecutive blocks. For example, group the start/stop outputs for all low lift pumps in similar order and in adjacent terminals.
   h. Avoid latches.
   i. Avoid jumps.
   j. Avoid drum sequencers.
   k. Label every register/word, relay/bit, and rung with a name or comment.
   l. Don't sacrifice program clarity and simplicity to achieve higher execution speed and smaller code size.

9. All PLC programs shall conform to IEC-1131 and IEC-848. In addition, the programs written for critical or hazardous applications shall conform to CAN/CSA-Q396 *Quality Assurance Program for the Development of Software Used in Critical Applications*.

10. Each control program shall be identified by its version number (Vx.x) and its name. The location of each copy of the program shall be recorded.

4. Documentation

4.1 Program Listings

1. All applications programs shall be listed in the control language used by the hardware running the program. The listings should show the compiled control language if a compiler is required to convert the program into a runtime version.

2. The entire program shall be annotated. Each I/O, derived value, register and coil, subroutine and object shall be identified by descriptor. Values of tuning parameters and constants shall be included.

4.2 Parameter Listings

1. All parameters used in application programs shall be listed. These lists include I/O lists for controllers, historical data bases and operator stations. Software addresses for I/O and derived values shall be included for controllers that allow addresses to be used in applications programs. The list shall show the software address and descriptor for each point. For real I/O, the list must also show the hardware address.

5. Programming

5.1 Memory Organization

1. PLC memory shall be organized into three major sections:
   a. I/O Registers
   b. Control
   c. Communication

2. Each section should contain memory for expansion up to the overall limit defined in the technical specifications for the PLC. Within each section, the memory should be further organized into logical blocks as shown in the Memory Partition Table.

3. I/O Registers:

a. I/O should be organized in the same hierarchy as used for program structure. For PLC's in which I/O point numbering is not restricted to a pattern, the I/O should be assigned to addresses within the I/O register section. The I/O register should be split by type of I/O: analog inputs, analog outputs, digital inputs and digital outputs. I/O for similar devices should be put in the same order of address.
b. For PLC's in which I/O point numbering is restricted to a pattern, the assignment of addresses may be partially predetermined. As much as possible, follow the considerations for organization given in the preceding paragraph.

4. Control:
   a. Logic for control should be organized according to object composition.
   b. Logic for the watchdog timer and system clock should be located first in this section if they are not part of system software or hardware.

5. Communications:
   a. Blocks of memory should be allocated for communication with other intelligent devices. For communication with an operator station, a separate block or blocks should be set up for an alarm and event array. The alarm and event array may be split into separate blocks, one for alarms and one for events. Even if alarms are also used for control, they should be copied to the alarm block. Separation of alarms is useful for testing alarm reporting separate from control logic.
   b. Within the communication section, separate blocks should be set up for communication to minimize the number of messages needed to communicate data. Typically this means that a block for analog values, a block for receipt of operator commands and a block for setpoints and other parameters should be set up. A block for communication to and from other PLC's may need to be separate from the operator station interface blocks in order for fast communications.

Memory Partition Table

Block	Function	Collaborator
I/O Registers		
Analog Input	Process Control	
Analog Output	Process Control	
Digital Input	Process Control	
Digital Output	Process Control	
Control		
Watchdog Timer and Clock	Process Control	
Other Control	Process Control	
Communications		
Alarm Array	Read only	Operator Interface
Event Array	Read only	Operator Interface
Analog Values	Read only	Operator Interface
Operator Commands	Read and Write	Operator Interface
Setpoints and Parameters	Read and Write	Operator Interface
Control	Read and Write	Other PLC's

5.2 Objects

1. Where possible, the program shall make use of standard "objects" or subroutines. Standard objects may come from the standard library of objects or if not available there, then created for the application. Objects created for an application are to be submitted to the Joint Board for consideration as a standard objects.

2. Standard object list:
   a. 2-State Device
   b. 3-State Device
   c. Variable Speed Device
   d. Digital Input
   e. Analog Input
   f. Flow Input
   g. PID Control Station
   h. Timer
   i. Counter

j. Sequencing
k. Scheduling
l. Lead/Lag Control Block
m. Totalizer
n. Averager

5.3 Representation

1. The control logic should present all control actions directly and avoid using the same address or block of addresses for multiple uses.

5.4 Scaling

1. In order to simplify scaling of analog values, the preference is to do scaling only in the field I/O filter.

2. Data manipulations such as summation and subtraction for displays or historical data will be done in the PLC software.

6. Communications

6.1 Addresses

1. Each node on a PLC communications network must have a unique address on that network. Node addresses shall be chosen to integrate into existing networks and conform to the existing Coding System Standard. Nodes shall be assigned in consecutive node addresses. PLC's in hot standby shall have the same node address as their primary PLC.

6.2 Control

1. Control and monitoring should continue without disruption in the event of communication failures. Where control functions rely on information affected by communications failure, a safe mode of control shall be provided.

2. Design of software should seek to reduce the amount of messages transferred between PLC's to the minimum. Store Date and Time for certain alarm points such that upon restoration of communication this information can be relayed to a SCADA computer. Any process control setpoints shall be updated upon restoration of communication.

6.3 Time Synchronization

1. All nodes on a PLC communications network shall have internal clocks synchronized periodically to a master clock. Synchronization shall provide any required time and date stamping accuracy to within one second of the master clock. Master clock and PLC clock shall be accessible from the Operator Workstation. Alarm times will be synchronized, where a time stamp is required for alarms that are recorded during communication failures.

6.4 Exception Reporting

1. Where information is reported over networks on an exception basis, the default exception limits shall be as follows:
   a. Digital values Upon change of state
   b. Analog values flow 1% of range
   c. level 2% of range
   d. pressure 2% of range
   e. temperature 2% of range
   f. quality or analysis 2% of range
   g. other 3% of range

2. If information is communicated on exception as well as on polled or timed basis, the possibility may exist that the most up to date information may not always be received. Control applications should only use unambiguous communications or be able to reduce conflicts to an acceptable level. At a minimum, control communications require one or more of the following:
   a. Repeated messages
   b. Time and date stamping at the point of transmission
   c. Tighter time synchronization

504 Process Displays

1. Standard Requirement

1.1 General

1. This document is a guideline to the structure and documentation of process displays.

2. The purpose of this document is to establish standards for a consistent approach to programming. Consistency will enable:
   a. maximum re-use of programs
   b. reduced time to troubleshoot programs
   c. more confidence and usability of operator workstations.

2. Application

1. This standard applies to all SCADA Server, Terminal Server, Web Server, and the related operator workstation configurations.

3. Versions

1. Each graphic display shall be identified by its version number (Vx.x) and its name. The location of the primary copy of the display shall be recorded.

4. Graphic Colours

1. The SCADA system is detailed on several graphic displays, each representing a distinct part of the process. Each process screen is design to appear as similar to the actual layout of the system or process as possible. Standard ISA symbology is used to represent equipment such as pumps, valves, and transmitters.

2. Colours are used to represent the status(es) of various pieces of equipment or their components on the operator displays and their current use.

3. For the ALARM condition indicators, the background of the indicator (block) must be red and the fonts must be amber, in order to highlight the ALARM condition. The following table lists some standard colour conventions:

Colour	**Object (use)**
Grey- Light	Display background
Green	Equipment is running (or valve open)
Grey-Medium	Equipment is stopped (or valve closed)
Yellow	Equipment is in WARNING condition, including Out of Service
Red	Equipment is in ALARM condition
Yellow, Flashing	Equipment is in WARNING condition, with an unacknowledged alarm
Red, Flashing	Equipment is in ALARM condition, with an unacknowledged alarm

1. Values (and units) appear at various locations on the screen to represent current flows, levels, and pressures. They are to be coloured according to the following table:

Colour	**Status Condition**
Green	Normal Condition
Yellow	Warning Condition, including Out of Service
Red	Alarm Condition
Yellow Flashing	Warning Condition, with an unacknowledged alarm
Red Flashing	Alarm Condition, with an unacknowledged alarm

1. Colours may be used to represent the contents of piping and tankage on the operator displays. The following table lists the standards for colours for contents:

Colour	**Material Carried/Stored**
Blue	Raw Water
Light Blue	Potable Water
Dark Grey	Raw Sewage
Brown	Sludge, Scum or Waste Holding (WTP)
Dark Blue	Effluent
Orange	Chemicals
Yellow	Digester or Natural Gas
Black	General use (borders and outlines) and Text
White	Air

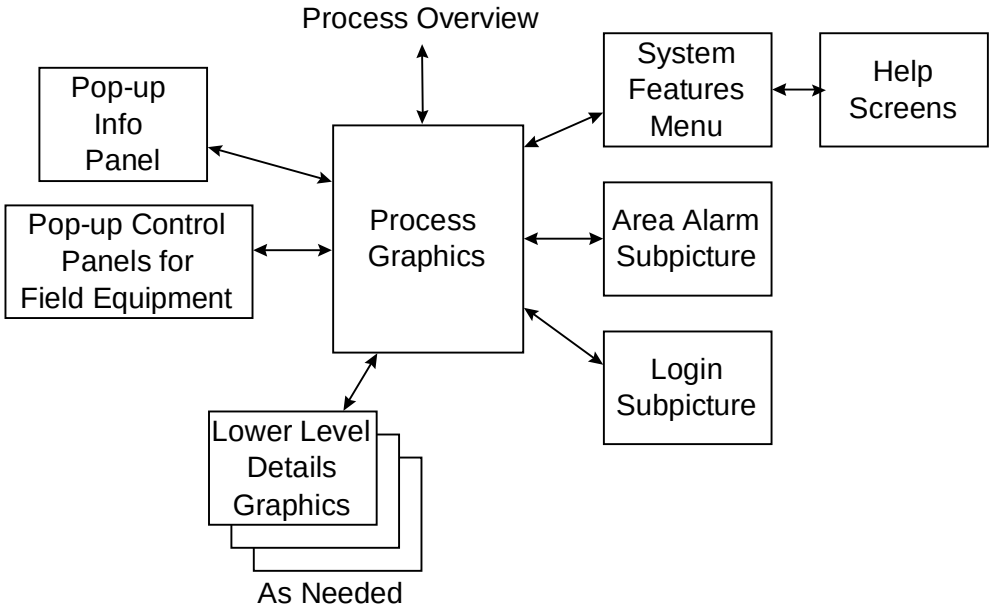
5. Graphic Colour RGB Standards

1. In an effort to ensure colour consistency, the following table defines the colour according to the Microsoft standard.

Colour Name	**Red (R)**	**Green (G)**	**Blue (B)**
Red	255	0	0
Green	0	255	0
Blue- Dark	0	0	190
Blue	0	0	255
Blue-Light	200	225	225
Yellow	255	255	0
Magenta	255	0	255
Grey-Dark	125	125	125
Grey-Medium	190	190	190
Grey-Light	235	235	235
Orange	255	130	0
Black	0	0	0
Brown	150	0	0
Blue-Dark	0	0	150
White	255	255	255

6. Programming

6.1 Displays



6.2 Screen Layout

1. All screens must contain a title bar across the top.

2. The title bar must display:
   a. name and version of the graphic display
   b. date
   c. time
   d. access icons to:
      i. plant overview
      ii. alarm summary
      iii. operator log-in
      iv. system features menu

3. A colour key should be accessible from all screens, providing a quick pop-up reference source.

4. Graphic displays should have minimal information on the left side where pop-up windows initially appear.

6.3 Text

1. Font style and size should be suited to the graphic display. Preferred font styles are plain such as Simplex or Arial with a minimum point size of 10.

6.4 Animation

1. For rotating equipment, animation can be used on some occasions. Generally, animation is distracting and may hinder recognition of other important information such as flashing symbols. Therefore, animation should be used sparingly. Any proposed use of animation to be identified to the Joint Board for their approval.

6.5 Icons

1. Icons should resemble field equipment to make recognition easier. All symbols must be based on the Joint Board library. Label each icon with the equipment number.

2. Icons incorporate the colour and alarm conventions. The colour convention including rules for using flashing to indicate unacknowledged alarms is given in the graphic colours standard.

3. Provide each icon with access to its corresponding pop-up window.

6.6 Pushbuttons

1. Use pushbuttons to call up menus, trends and other displays.

6.7 Pop-up Windows

1. Pop-up windows should initially appear on the left side of the screen, ensuring minimal coverage of the screen. Pop-up windows may be moved and sized by the operator. Pop-up windows will contain:
   a. the name and description of the equipment or item on the top.
   b. current status: e.g. running/off, opened/closed, enabled/disabled, manual/automatic/cascade, alarm/normal
   c. current conditions: e.g. speed, position, electrical current
   d. current alarms and acknowledge function
   e. controls: e.g. start/stop, open/close, setpoint entries
   f. mode selection: manual/automatic/cascade, enable/disable
   g. details button to access data page with detailed information about the equipment or item (future)
   h. Local/Remote handswitch indicator

6.8 Graphic Display Structure

1. The displays will be interconnected in a hierarchy structure. In addition, interconnection will be provided for process streams continued on other process graphics.

6.9 Bar Graphs

1. Use bar graphs to show important measurements such as reservoir levels.

7. Pictures and Sub-Pictures

1. All window control (i.e. task bar) shall be hidden from operator access. When a new picture is launched, the previous picture with all associated sub-pictures shall be closed at the same time. Redundant pictures and sub-pictures shall not be hidden.

8. Documentation

8.1 Screen Print

1. The method of documentation for graphic displays is to print a colour copy of the graphic display and list the display configuration.

8.2 Display Configuration Listings

1. A print of all configuration listings is required for each operator workstation.

505 Alarm Management

1. General

1. This document provides the specification details to be included in all construction contracts that provide control systems or equipment that generate alarms. It should also be used in design as a guideline to what alarms need to be brought into the control system.

2. The purpose of this document is to establish standards that will:
   a. determine information that needs to be alarmed,
   b. prioritize alarm information given to operators.

3. Uniformly applied principles of alarming will help operators respond appropriately to abnormal situations.

2. Alarm Management

1. When a field alarm occurs, the alarm is "latched" in software for safety reasons. The associated device will not be restarted until the alarm is cleared. In order for the alarm to be acknowledged and eliminated, two events must occur. The field condition creating the alarm must be corrected and the alarm must be acknowledged by the operator either at the PLC or SCADA workstation. Power interruptions do not lock out pumps (in software).

3. Communication Alarms

1. Communication links are monitored for failure and when a failure is detected an alarm will appear on the operator workstation. All points associated with stations using the failed communications link will not be alarmed until such time that the communications link is restored. This will result in a lesser level of nuisance alarms. A communication link failure should be addressed immediately and therefore should be configured as a Level 1 alarm.

2. The communication link alarms must include links related to field devices connecting using a fieldbus, Remote I/O racks, PLC, SCADA servers, SCADA workstations, and all other server.

3. Any points associated with a remote station that are deemed to be critical or top level alarms may have local date and time stamping installed. This information can then be fed into the SCADA system for recording. In-plant communication network will be less susceptible to failure, therefore, only very critical points associated with these PLC's to have local date and time stamping for alarming.

4. Communication link failures should not affect the operation of system totalizers such as runtimes and flow totals. All totalized values will be maintained within their associated PLC such that a communication link failure will not adversely affect the accumulated sum. Alarms shall be stored historically for archiving purposes.

4. Alarm Displays and Logs

1. Alarms originating from field contacts or generated by software shall be displayed at the local and main SCADA workstations. Alarms shall have a configurable option to be logged on a printer. The time and date of occurrence shall be displayed and logged (if configured for printing) as well as the time of acknowledgement and return to normal. Alarms should be stored in history files for a minimum time period of one year.

5. Alarm Priorities

1. Level 1 alarms are critical alarms that are paged off the site. In this case, this includes only the man- down alarm.
2. Level 2 alarms require immediate operator attention, caution, and action. Level 2 alarms are defined as those involving personal safety of the operator (fire, gas leak, chlorine leak, etc.) or those involving potential process damage (computer and PLC failures, computer redundancy failures, flooding, etc.). The Operator is to also call the Manager to advise him/her that the alarm occured.
3. Level 3 alarms are MOE adverse event alarms. MOE adverse event alarms require immediate operator attention. The Operator must complete plus the completion of the MOE adverse event form, plus call the Manager. The Operator must enter into the log when the alarm occurred, why, and what actions they took.

This includes loss of communication alarms that exceed the allowable maximum before triggering MOE requirements for collecting the historical data using the backup data collection tool.

4. Level 4 alarms are MOE adverse event warnings. MOE adverse event warnings require immediate operator attention. MOE warning alarms are more strict limits than the MOE, set by Operations, used to warn staff that an adverse event may occur if they don't take action very quickly. The Operator must enter into the log when the alarm occurred, why, and what actions they took.
5. Level 5 alarms require immediate operator attention and are defined as those that cause the immediate shutdown of equipment such as a motor overload condition, hot-backup failure, safety shutdown, high-high level, temperature, flow, etc. This also includes the analog High High and Low Low alarm limits. These alarms indicate the potential for large equipment damage, major cleanup or possible process obstruction.
6. Level 6 alarms are communication failures. These are segregated in a separate group so they are easy to sort when needed.
7. Level 7 alarms include those that require operator attention "as soon as possible" but do not result in the immediate shutdown of equipment. This generally includes the analog High and Low alarm limits. Examples are a high wet well level, impending high temperature condition of a pump motor, failure of auxiliary systems (instrument air, lubrication system, heating, cooling, ventilation system, backup instrument or power) or an instrument failure alarm.
8. Level 8 is for process events, not alarms, to differentiate the events from alarms, and allow filtering and sorting, by staff. For further clarification, an event is defined as a state change of a field DI that has not been previously defined as an alarm. Therefore, an event might be a pump start, pump stop, valve open, valve close, etc.

Alarm conditions from auxiliary systems that are essential to the functioning of the control system or process equipment (instrument air supply systems and equipment lubrication systems for example) should also be monitored for critical alarms.

The Level 1-6 are considered to be "High Priority Alarms" and therefore when they occur, the HMI graphics should indicate this condition using RED. Level 7 is considered to be a WARNING and therefore the HMI graphics should indicate this condition using YELLOW. Level 8 is considered simply a process event and therefore is not highlighted on the graphics.

When Level 6 (Communication Alarms) occurs, the graphics must also indicate that the values displayed are not necessarily accurate because communication has been lost.

6. Alarm Groups

1. All alarms must be organized by alarm groups. Each remote site must be a separate alarm group, and each plant area must be a separate alarm group.

2. In order to also have separate MOE warning and MOE alarm groups, the one field alarm must be configured as two SCADA database points, with one point organized by the area alarm group, and the other point organized as the MOE alarm or warning group.

7. Alarm Matrix

Alarm Level	Operator Workstation Sound	Operator Display Background Colour*
Level 1	Loud	Red
Level 2	High frequency pulse	Red
Level 3	High frequency pulse	Red
Level 4	Low frequency pulse	Yellow

* Alarm characters are black.

506 Historical Operating Data Management

1. Standard Requirement

1.1 General

1. This document provides guidelines on the specification details to be included in all construction contracts that provide SCADA systems with historical storage capability. As well this document covers the generation of reports from within the SCADA system. It should also be used in design as a guideline to what information is historically archived and what information is to be made available for system reports.

1.2 Purpose

1. The purpose of this document is to establish standards that will:
   a. determine information that needs to be archived,
   b. determine the frequency that information will be archived.
   c. determine the reports that will be available on archived information
   d. determine the storage system for information to be archived

2. Uniformly applied principles of archiving and reporting will help management and operators to use information obtained by the SCADA system to more efficiently evaluate system performance.

1.3 Backup Local Data Storage

1. For all remote facilities, provide a local data backup system which can store 7 days of historical operating data.
2. Continuously log, locally, all regulatory parameters plus other values to be specified by the Joint Board.

2. Short Term Data Collection

1. In general, short term data collection includes analog instrument readings and related field device inputs. All of these are continuously monitored by their respective PLC. The following table defines the typical parameters and typical HMI poll times.

In-Plant Parameters

Parameter	Poll Time
General Field DI	10 sec
General Field AI	10 sec

Remote Facility Parameters

Parameter	Poll Time
General Field DI	10 sec
General Field AI	10 sec

2. The selected parameters are to be stored in the SCADA HMI Historical Logging, with the following settings. Discrete values are only “Report by Exception” and time stamped when a change in state occurs.

Analog Parameter	Logger Time Period	Deadband
Level	None	2%
Pressures	None	2%
Flow	None	2%
Other Analogs	None	2%

3. Alarm Logging

1. All alarms are logged separately from process events, in separate alarm log files for review by management.

2. All active alarms are displayed on a separate HMI “Active Alarms” graphic, which can provide sorting by facility.

3. All alarms are displayed on a separate HMI “Alarm Log” graphic, which can be sorted by facility. This includes approximately 7 days of alarm history.

4. Long Term Data Collection/SQL Data Storage

1. All analog and discrete parameters related to regulatory compliance must be collected into the SCADA Historian (RSSql) SQL database.

2. In general, analog parameters are to be stored as per the following.

Parameter	Time Period	Calculation
Facility Flows	5 minutes	Instantaneous value for each period
Chlorine Residual	5 minutes	Instantaneous value for each period
Turbidity	5 minutes	Instantaneous value for each period
Reservoir Levels	5 minutes	Instantaneous value for each period
Equipment Run Times	1 hour	Snapshot at end of each period
Other Flows	5 minutes	Instantaneous value for each period
Pressures	5 minutes	Max. value during period Min. value during period Average value during period

3. All alarm events are also to be logged in RSSql. The information includes.
   a. Alarm Tag
   b. Alarm Description
   c. Time of Alarm

5. Pre-Configured Reports

1. Daily, Monthly, and Annual Reports, per facility, are required for MOE compliance.

2. The daily report data generally includes the following parameters. All revisions/upgrades must be reviewed and accepted by the Joint Board prior to implementation.
   a. Facility Flow – Hourly Average (display as trend)
   b. Facility Flow – Max. Hourly Average
   c. Facility Flow – Min. Hourly Average
   d. Facility Flow – Daily Total
   e. Chlorine Residual – 5 Minute Avgs (display as trend)
   f. Turbidity
   g. Listing of Critical Alarms that occurred

3. The monthly reports data to include all parameters indicated on the daily reports. For all analog values, calculate daily averages, provide the 1 hour maximum and minimum values, and provide the 5-10 minute maximum and minimum values.

4. The annual report data shall be a consolidated report of the 12 monthly reports, including all of the parameters.

6. Data Query Tool Kits

1. Provide pre-configured SQL queries to access the historical analog data and dump it into an Excel spreadsheet. The query to contain the following selectable parameters.
   a. Start Year, Month, Day, Hour, Minute
   b. End Year, Month, Day, Hour, Minute
   c. Parameter 1 Tag name
   d. Parameter 2 Tag name
   e. Parameter 3 Tag name
   f. Parameter 4 Tag name
   g. Parameter 5 Tag name
   h. Parameter 6 Tag name
   i. Parameter 7 Tag name
   j. Parameter 8 Tag name
   k. Parameter 9 Tag name
   l. Parameter 10 Tag name

2. Provide pre-configured SQL queries to access the historical alarm log and dump the data into an Excel spreadsheet. The query to contain the following selectable parameters.
   a. Start Year, Month, Day, Hour, Minute
   b. End Year, Month, Day, Hour, Minute
   c. Alarm Priority
   d. Parameter 1 Tag name
   e. Parameter 2 Tag name
   f. Parameter 3 Tag name
   g. Parameter 4 Tag name
   h. Parameter 5 Tag name
   i. Parameter 6 Tag name
   j. Parameter 7 Tag name
   k. Parameter 8 Tag name
   l. Parameter 9 Tag name
   m. Parameter 10 Tag name

507 Paging Software Configuration

1. General

1. This section is only applicable for the SCADA Systems of St. Thomas, Central Elgin and APAM.

2. This document provides the specification details to be included in all construction contracts that provide control systems or equipment that generate alarms. It should also be used in design as a guideline to what alarms need to be paged.

3. The purpose of this document is to establish standards that will:
   a. Determine information that needs to be paged,
   b. Identify how paging will be programmed.

4. Uniformly applied principles of alarm paging will help operators respond appropriately to abnormal situations.

2. Alarm Priorities vs. Paging

1. All alarms that are priority 1, 2 and 3 must be paged. Refer to the process narratives and software programming requirements documents for the number of alarms to be paged.

3. Paging Algorithm

1. The alarm pages are to be text messages, issued by a dial up telephone connection, that communicate to cellular phones with text messaging.
2. The text messages must be the same messages that are displayed on the SCADA system.
3. The alarm to be unlatched in the WIN911 software, such that acknowledging the alarm in the SCADA software also acknowledges that alarm within the paging software. Therefore, the WIN911 alarms are to be based on the unacknowledged alarm bits.
4. General alarms must be paged to three recipients, with 15 minute delays between escalation of pages.
5. MOE adverse event alarms are to also be paged directly to one selected recipient.

508 Version Control Software Configuration

1. General

1. This document provides the specification details to be included in all construction contracts that provide control systems or equipment that generate alarms.

2. The purpose of this document is to establish standards that will:
   a. Determine what information needs to be stored with version control in the SDMS,

3. Uniformly applied principles of version control software will help operators respond appropriately to abnormal situations.

2. PLC Software Program Version Control

1. All current and previous PLC software programs must be stored on the SDMS server (Asset Centre), for access across the network be maintenance staff.
2. When any programming changes are implemented, the software programmer must place a copy of the most recent version on the SDMS server at the end of each day.
3. The software must be configured to automatically, once per week, search the network and collect the most recent copies of the PLC programs for storage. If any copies are more recent than those previously stored on the SDMS server, then an alarm must be generated and issued to the SCADA Maintenance staff.

3. Facility SCADA Documentation Version Control

1. The Asset Centre software to also be used for storing and managing versions of the SCADA documentation including the following.
   a. Process Narratives & Software Programming Requirements documents
   b. SCADA User Manual
   c. SCADA Maintenance Manual
   d. Excel spreadsheets of panel I/O listings
   e. SCADA ACAD drawings related to control wiring, control panels, plus other components

4. SCADA Domain Controller Configuration

1. The SCADA Domain Controller must be configured to enable the ASSET CENTRE to locate the various components on the network.

509 SCADA Terminal Services Software Configuration

1. General

1. This document provides the specification details to be included in all construction contracts that provide control systems or equipment that generate alarms.

2. Uniformly applied principles of remote monitoring and control will help operators respond appropriately to abnormal situations.

2. Configuration Requirements

1. The intent of the SCADA Terminal Services Server is to enable staff to monitor and control the SCADA system using a web based application.
2. All graphics on the SCADA Servers must be ported over to the SCADA Terminal Services Server, so that operations staff utilizing the portable servers within the plants can monitor and control the process via the wireless LAN (WAN) installed across the facility.
3. Operations staff must also be able to access the server remotely, via the Internet for remote monitoring and control. The Internet link must be via the corporate VPN in order to provide the appropriate level of cyber security.
4. Management staff must be able to access the server, for monitoring only, via the corporate network.
5. Access to the server must include password security
6. The server must be configured for a minimum of three levels of users-
   a. Monitoring Only
   b. Limited Control
   c. Full Control

3. Portable Computer Configuration Requirements

1. The portable computers must be configured for accessing the corporate VPN over the Internet
2. The portable computers must be configured for accessing the SCADA Terminal Services Server via the wireless network within the plants.
3. The portable computers must be configured for accessing the SCADA Terminal Services Server via the corporate network.

510 Regional Water Supply Web Site Software Configuration

1. General

1. This document provides the specification details to be included in all construction contracts that provide control systems or equipment that generate alarms.

2. Uniformly applied principles of a security access, public web site will enable the secondary and tertiary water operators to monitor the Primary Water Supply SCADA system in near- real time.

2. Configuration Requirements

1. The intent of the SCADA Web Site, Terminal Services Server is to enable various external water users to monitor the Lake Huron and Elgin Area SCADA systems using a web based application.
2. All remote facility and plant process area overview graphics on the SCADA Servers must be ported over to the SCADA Web Server.
3. No control functions shall be included on the graphics, to minimize the cyber security issues.
4. The data on the server must be updated every 5 minutes.
5. Access to the server must include VPN password security
6. The server must be configured for a minimum of twenty different user groups.

511 Data Backup Software Configuration

1. General

1. This document provides the specification details to be included in all construction contracts that provide control systems or equipment that generate alarms

2. Uniformly applied principles of a off site data backup will minimize the risk of loss of electronic information.

2. Lake Huron and Elgin Area Primary Water Supply Configuration Requirements

1. The Lake Huron and Elgin Area Primary Water Supply data backup server is located at the London Museum.
2. This server must back up key data on the Lake Huron WTP computers on a nightly basis.
3. This server must back up key data on the Elgin Area WTP computers on a nightly basis.
4. The following plant SCADA Server files are to be backed up-
   a. Historical Trend Files
   b. Historical Alarm Files
5. The following plant SCADA Historian files are to be backed up-
   a. SQL database records
   b. SQL configuration
6. The following SDMS server files are to be backed up-
   a. PLC programs
   b. SCADA Server configurations
   c. Network equipment configurations
7. On a monthly basis, triggered manually by staff, the software must execute a full backup of the following computers at each plant.
   a. SCADA Servers
   b. SCADA Historian
   c. SDMS Server
   d. Terminal Services Server

3. St. Thomas SCADA Configuration Requirements

1. The St. Thomas data backup server is located at the St. Thomas City Hall.
2. This server must back up key data on the St. Thomas SCADA computers on a nightly basis.
3. The back up requirements are equal to those specified for the Primary Water Supply SCADA Systems.

4. APAM SCADA Configuration Requirements

1. The APAM SCADA data backup server is located at the Malahide offices.
2. This server must back up key data on the APAM SCADA computers on a nightly basis.
3. The back up requirements are equal to those specified for the Primary Water Supply SCADA Systems.

5. Central Elgin SCADA Configuration Requirements

4. The Central Elgin SCADA data backup server is located at the 450 Sunset Dr. St. Thomas corporate offices.
5. This server must back up key data on the Central Elgin SCADA computers on a nightly basis.
6. The back up requirements are equal to those specified for the Primary Water Supply SCADA Systems.