Winnipeg

The City of Winnipeg

Water & Waste Department

Automation Master Plan

Document Code:

Revision: 00

Approved By:

Jackie Veilleux
Project Director
Winnipeg Sewage Treatment Program

Nov 27/12
Date

SNC·LAVALIN

City of Winnipeg

Wastewater Treatment Plants Automation Master Plan

PROVINCE OF MANITOBA
C. J.
REIMER
Member
21968
REGISTERED PROFESSIONAL ENGINEER

2012-11-27
Rev 00

APEGM
Certificate of Authorization

SNC-Lavalin Inc.
No. 4489

PREPARED BY : C. Reimer

REVIEWED BY : E. Ryczkowski

APPROVED BY : Curtis Reimer

November 2012
Revision 00

NOTICE

This document contains the expression of the professional opinion of SNC-Lavalin Inc. (SLI) as to the matters set out herein, using its professional judgment and reasonable care. It is to be read in the context of the agreement between SLI and the City of Winnipeg, and the methodology, procedures and techniques used, SLI's assumptions, and the circumstances and constraints under which its mandate was performed. This document is written solely for the purpose stated in the agreement, and for the sole and exclusive benefit of the City of Winnipeg, whose remedies are limited to those set out in the agreement. This document is meant to be read as a whole, and sections or parts thereof should thus not be read or relied upon out of context.

SLI disclaims any liability to the City of Winnipeg and to third parties in respect of the publication, reference, quoting, or distribution of this report or any of its contents to and reliance thereon by any third party.

TABLE OF CONTENTS

Executive Summary **1**

1.0 Introduction **13**

1.1 Overall Project Objectives 13
1.2 Master Plan Scope and Limitations 13
1.3 Definitions 14

2.0 Scope of Automation and Control **17**

2.1 Ancillary Systems 18
2.1.1 Electrical Power System 19
2.1.2 Fire Alarm System 19
2.1.3 HVAC Controls 20
2.1.4 Sampling Systems 20
2.1.5 Lighting Controls 20
2.1.6 Security / Access Controls / Video Monitoring 21

3.0 Reliability Requirements And Analysis **23**

3.1 Reliability Requirements 23
3.1.1 Basic Reliability Analysis 23
3.1.2 Examples - Raw Sewage Pumping 25
3.1.3 Examples – Primary Clarifiers 30
3.1.4 Example - Network Cable 32

4.0 Equipment Control **35**

4.1 Modes of Control 35
4.2 Local Control Requirements 37
4.2.1 General 37
4.2.2 Motor Disconnect Switches 39
4.2.3 General Guidelines 40

5.0 Motor Control **43**

5.1 Motor Control Automation Styles 43
5.2 Reliability Analysis 44
5.3 Recommendations 48

6.0 Instrumentation **49**

6.1 Instrument Selection 49
6.1.1 Classes of Measurement Instruments 49
6.1.2 Discrete vs. Transmitter Selection 50
6.1.3 Use of Networked Instruments 52
6.1.4 Wireless Instruments 53
6.2 Wastewater Instrumentation Guidance 54
6.2.1 Flow Instrumentation 54
6.2.2 Level Instrumentation 54
6.2.3 Temperature Instrumentation 55

6.2.4 Process Analyzers ... 55
6.3 Instrumentation Redundancy ... 56
6.3.1 General Guidelines ... 56
6.3.2 Instrument Redundancy Reliability Calculations ... 57
6.4 Instrument and Signal Application Guidelines ... 59
7.0 Fieldbus Networks ... 61
7.1 Overview ... 61
7.2 Industrial Ethernet Protocols ... 62
7.2.1 Ethernet/IP ... 63
7.2.2 Modbus TCP ... 63
7.2.3 PROFINET ... 64
7.3 Fieldbus Device Networks ... 65
7.3.1 DeviceNet ... 65
7.3.2 PROFIBUS DP ... 65
7.3.3 Modbus ... 66
7.4 Fieldbus Process Networks ... 66
7.4.1 Foundation Fieldbus ... 67
7.4.2 PROFIBUS PA ... 67
7.5 Fieldbus Sensor Networks ... 68
7.5.1 AS-i Bus ... 68
7.6 Other Fieldbus Networks ... 69
7.6.1 HART ... 69
7.6.2 Networks Not Discussed ... 69
7.7 Fieldbus Selection Guidance ... 70
7.8 Fieldbus Application Guidance ... 71
8.0 Environmental and Hazardous Classification ... 73
8.1 Environmental Considerations ... 73
8.1.1 Corrosive Gasses ... 73
8.1.2 General Design Requirements ... 74
8.2 Hazardous Gas Detection ... 75
8.2.1 Combustible Gas Detection ... 75
8.2.2 Hydrogen Sulfide Gas Detection ... 75
8.2.3 Oxygen Gas Detection ... 76
8.2.4 Gas Detector Spacing ... 77
8.2.5 Hazardous Gas Alarm Notification ... 77
8.3 Identification of Hazardous Areas ... 78
8.4 Hazardous Locations – High Level Design Basis ... 80
9.0 Automation Power Supply ... 83
9.1 Electrical Distribution System ... 83
9.2 Uninterruptible Power Supply ... 84
9.2.1 Configuration ... 84
9.2.2 Battery Duration ... 85
9.2.3 UPS Monitoring ... 86
9.3 Load Power Supply Design Criteria ... 86
9.3.1 General Guidelines ... 86

9.3.2 PLC Power Supply 89

10.0 Control System Architecture 91

10.1 General Reference Model Architecture 91

10.2 Existing DCS Architecture 94

10.3 Centralized vs. Distributed 95

10.4 Current DCS Architectures 99

10.5 PLC Based Architectures 100

10.6 Comparison of DCS vs. PLC Architectures 102

10.6.1 City Decision 103

10.7 PLC Architecture 103

10.7.1 Evaluation of Redundancy Requirements 104

10.8 Field Network Architecture 105

10.9 Process Networks 107

10.9.1 General Requirements 107

10.9.2 Facility Process Network 109

10.9.3 Process Area Network 111

10.10 Network Selection Criteria 115

10.11 Master Controllers 115

10.11.1 Potential Configurations 115

10.11.2 Area Control Philosophy 117

10.12 Server Room 118

10.13 Example PLC Architecture 119

10.13.1 Process Requirements 119

10.13.2 Proposed Automation Architecture 121

10.13.3 Failure Analysis 124

10.14 Application Software Logic 126

10.15 Automation System Vendor Selection 127

11.0 Migration Strategy 133

11.1 Existing DCS 133

11.1.1 Existing Installation 133

11.1.2 Manufacturer Support of the Existing DCS 135

11.1.3 Existing DCS HMI 136

11.2 DCS Replacement Schedule 137

11.3 Overall Migration Strategy 137

11.3.1 HMI Lead Migration 138

11.3.2 Parallel Swing-over Migration 139

11.4 DCS Migration Details 140

11.4.1 HMI Migration 140

11.4.2 DCS PCU Migration 140

12.0 HMI and Enterprise Systems 143

12.1 Introduction 143

12.2 System Architecture 143

12.3 HMI Client Configurations 145

12.3.1 Terminal Services ... 145
12.3.2 Desktop Thin Clients ... 146
12.3.3 Touchscreen Thin Clients ... 146
12.3.4 Local Independent Touchscreen ... 147
12.3.5 Local Wireless Operator Device ... 147
12.3.6 Remote Portable Operator Devices ... 148
12.4 Other Considerations ... 149
12.4.1 Server Virtualization ... 149
12.4.2 HMI Network ... 150
12.5 Supporting Infrastructure ... 150
12.6 Graphic Scheme ... 151
12.6.1 Existing ... 151
12.6.2 Current Industry Direction ... 153
12.6.3 Recommendations ... 157
12.7 Alarm Management ... 157
12.8 HMI System Capabilities ... 160
12.9 Control Rooms ... 161
12.9.1 Main Control Room ... 161
12.9.2 Area Control Rooms ... 162
12.10 Central Control and Monitoring ... 162
12.10.1 Location for Centralized Control ... 162
12.10.2 Architecture ... 163
12.10.3 Centralized Control Room ... 165
12.10.4 Contingency Planning ... 166
12.10.5 Implementation Requirements ... 166
12.11 HMI Remote Access Requirements ... 167
12.11.1 Mobile Operator Remote Access – View Only ... 167
12.11.2 Mobile Operator Remote Access – Control Capable ... 168
12.11.3 City Employee Remote Access – View Only ... 169
12.12 Collections System Integration ... 170
12.13 Enterprise System Integration ... 171
12.13.1 Introduction ... 171
12.13.2 Computerized Work Management System ... 171
12.13.3 Laboratory Information Management System ... 172
12.13.4 Process Control Management System ... 172
12.13.5 Implementation Methodologies ... 173
12.13.6 Enterprise System Integration Recommendation ... 174
12.14 Advanced Model Predictive Control ... 174

13.0 Historical Data and Reporting ... 177
13.1 Overview ... 177
13.2 Logging Requirements ... 177
13.3 Reporting Requirements ... 179
13.4 Architecture ... 180
13.5 Backup Requirements ... 182

14.0 Networking ... 183
14.1 Network Requirements ... 183

14.2 Wide Area Network Communications 185
14.3 Demilitarized Zone 187
14.4 Process Area Network Layout 187
14.5 Wireless Integration 188
14.6 Maintenance Responsibility 191
14.7 Design Criteria 192

15.0 Security 195
15.1 Overview 195
15.2 Network Security 195
15.2.1 Two Factor Authentication 197
15.2.2 Connection of Remote Devices 198
15.2.3 Local Portable Operator Devices 198
15.2.4 Remote Portable Operator Devices 199
15.2.5 Wireless Devices and Sensors 199
15.3 Design Criteria 200

16.0 Operations and Maintenance Considerations 203
16.1 Training 203
16.1.1 Automation System General Training – Operations Personnel 203
16.1.2 Automation System Training – Maintenance Personnel 203
16.1.3 Process Operation Training 204
16.2 Testing and Simulation System 205
16.3 Other Operations and Maintenance Considerations 207

17.0 Equipment Standardization 209
17.1 Introduction 209
17.2 Existing Equipment Standards 209
17.3 Potential Equipment Standards 211
17.3.1 Evaluated Equipment 213
17.4 Implementation 218
17.4.1 Duration of the Equipment Standardization 219
17.4.2 Price Evaluation 219

18.0 City Technical Standards 221
18.1 Introduction 221
18.2 Recommended Standards 221
18.3 Identification Standard 222
18.4 Automation Standards 223
18.4.1 Automation Design Guide 223
18.4.2 Tagname Identification Standard 225
18.4.3 HMI Layout and Animation Plan 226
18.4.4 Historical Data Retention Standard 227
18.4.5 Backup and Disaster Recovery Plan 228

19.0 Project Documentation 229
19.1 General Requirements 229
19.2 Documentation Lifecycle Approach 229

19.3 Minimum Documentation Requirements....231
19.3.1 Process and Instrumentation Diagrams....233
19.3.2 System Architecture / Block Diagrams....234
19.3.3 Instrument List....234
19.3.4 Instrument Location Plans....234
19.3.5 Instrument Loop Diagrams....234
19.3.6 Instrument Segment Diagrams....235
19.3.7 Instrument Installation Details....235
19.3.8 Network Overview Diagrams....235
19.3.9 Network Details....236
19.3.10 Process Control Overview....236
19.3.11 Functional Requirements Specification....236
19.3.12 Instrument Datasheets....237
19.3.13 Safety Instrumented Systems Documentation....238
19.3.14 Operations Manual....238
19.3.15 Other Maintenance Documentation....239
19.4 Computerized Work Management System....240
19.4.1 Scope of Equipment to be Entered....240
20.0 Risk Review....243
20.1 Overview....243
20.2 Failure of the Existing DCS HMI....244
20.3 Failure of the Existing DCS Infi90 Hardware....245
20.4 Review of the Design Documents....246
20.5 Cost Overruns....247
20.6 Software Implementation Errors....248
20.7 Unplanned Effect on the Existing Process....249
20.8 Signal Noise and Grounding Issues....250
20.9 Compatibility Issues....251
20.11 Competency of Design Engineer and System Integrator....252
20.12 Automation Maintenance Organization....253
21.0 Implementation Plan....255
21.1 Commissioning....255
21.1.1 CSA Z320....255
21.2 Basis of Schedule....256
21.3 Implementation Responsibility....256
21.4 Associated Project Definition....260
21.4.1 DCS HMI Upgrade....260
21.4.2 Identification Standard Development....261
21.4.3 Critical Electrical and Automation Component Standardization....262
21.4.4 Automation Design Guide and Technical Standards....263
21.4.5 SEWPCC DCS Upgrades....264
21.4.6 WEWPCC DCS Upgrades....264
21.4.7 NEWPCC Central Control and Server Room Upgrades....265
21.4.8 NEWPCC DCS Upgrades....265
21.4.9 Backup and Disaster Recovery Plan....266
21.4.10 CWMS Integration....266
21.4.11 LIMS Integration....266

21.4.12 Collections System Integration 267

This page intentionally left blank.

EXECUTIVE SUMMARY

Introduction

The City of Winnipeg has initiated a program to perform upgrades to the wastewater treatment systems at the NEWPCC, SEWPCC, and WEWPCC facilities. As part of these upgrades, automation systems are required for process control and monitoring. The overall objective for the Automation Master Plan is to plot a course for automation system upgrades at the City of Winnipeg wastewater treatment facilities. This plan is intended to provide guidance regarding the overall control system architecture along with the associated instrumentation and motor control.

Scope of Automation and Control

The automation and control system at the wastewater treatment facilities will monitor and control the wastewater process systems. In addition, the boiler / chiller plant and the HVAC controls will also be fully monitored and controlled by the primary automation and control system. As the automation system Human Machine Interface (HMI) will provide the primary view of the operation of the wastewater treatment facilities, it is appropriate that it also becomes the primary point of integration for most auxiliary systems in the facilities. Detailed monitoring of the electrical power, fire alarm, gas detection, and instrument air systems will be provided. Basic monitoring and alarming of numerous other systems within the wastewater treatment facilities will also be integrated into the automation system.

Reliability Requirements

The wastewater treatment facilities provide a critical service for the City, and thus the automation system must provide a level of reliability that is consistent with the overall process requirements. In some cases, reliability analysis is required to determine if a proposed design solution is adequate to meet the requirements of the process. A method of performing basic reliability analysis is presented in the report, however it should be noted that the method proposed is not suitable for safety systems or other cases where in-depth reliability analysis is appropriate.

Equipment Control

Various modes of equipment control will be provided throughout the wastewater facilities. The most common modes will be the *Hand* mode for local manual control, *Off* mode, *Remote - Manual* for manual control via the HMI, and *Remote – Auto* for normal automatic control via the control system.

The level of local manual control capability provided at the equipment will be minimal, other than a general requirement to provide a means to turn off motorized equipment at a location adjacent to the motor. This could be provided by a stop pushbutton, but in many cases it is proposed to utilize a motor disconnect switch to provide local disconnect functionality along with the required stopping capability.

Motor Control

Intelligent Motor Control Centres (MCCs) utilize digital networks to allow the automation system to directly communicate with individual motor starters, rather than hardwiring individual status and command signals. Utilization of intelligent MCCs is directed for typical new installations due to the advantage of reduced wiring and additional diagnostic information that would be available. It is noted that the installed cost is expected to be comparable to a traditional hardwired MCC.

Instrumentation

The selection of appropriate instrumentation for the process is a critical component of a successful automation system. It is recommended to consider the use of transmitters over discrete switches for essential interlocking and alarming applications, as their benefits include rapid modification of setpoints and continuous basic verification of operation. Networked instruments allow for digital communication of process information, and are appropriate in numerous applications which include those where very high accuracy is required, long cable runs are required, and the additional available diagnostic information is beneficial. Wireless instruments are proposed to be considered only for cases where physical wiring would present challenges due to distance, location and mobility requirements. In addition, wireless instruments have a lower reliability level compared to hardwired instruments and therefore should only be utilized for applications where the level of reliability provided by the wireless instrument is acceptable.

The report also provides high-level guidance regarding selection and application of various instruments types, including requirements for instrument redundancy.

Fieldbus Networks

Fieldbus networks are utilized to connect automation devices within the process areas, and have the potential to provide significant benefits compared to traditional hardwired approaches. There are numerous fieldbus networks available, and current offerings include fieldbus protocols for use over Ethernet networks. It is expected that no single network will be appropriate for all applications, and it is therefore recommended that selection of preferred protocols be included as part of the selection of a control system vendor. Fieldbus network design should also review the reliability impacts of each fieldbus installation, to ensure that the effects of potential failure modes are acceptable.

Environmental and Hazardous Classification

Wastewater treatment facilities have various environmental considerations that must be accounted for in the automation system design. Hydrogen sulphide is a common corrosive gas found in wastewater treatment facilities, and the system design must include provisions for addressing the potential presence of corrosive gases. Gas detection is also required to provide appropriate safety to personnel, and it is expected that hydrogen sulphide, combustible gas, and oxygen deficiency detection systems will be required. Other gas detection systems may be required, dependent upon the processes utilized.

Spaces with potential fire and explosion risks must be evaluated for designation as electrically classified locations. It is expected that NFPA 820 will be utilized as a guide in the identification and mitigation of combustible and flammable risks. In many cases, NFPA 820 presents two or more options regarding electrical classification, dependent upon the level of ventilation provided. It is generally recommended to select a higher level of area ventilation, accompanied with a Class I, Zone 2 electrical classification over a Class I, Zone 1 electrical classification and a lower rate of ventilation. While the installation using a Class I, Zone 1 electrical classification may have a lower net present value, due to the reduced ventilation heating costs, the economic advantages are typically reduced when operational and maintenance considerations are included.

Automation Power Supply

Critical automation systems will be powered from an uninterruptible power supply (UPS). Generally a centralized UPS for each process area is the preferred approach; however, distributed UPS arrangements can be utilized where appropriate.

Motor control power will typically be 120VAC, powered by dedicated local control power transformers associated with each motor starter. Instrumentation and I/O power will typically be 24 VDC for new installations; however, 120VAC may be utilized for existing installations to facilitate the reuse of existing equipment.

Control System Architecture

The City’s wastewater treatment facilities are currently controlled by an ABB/Bailey Infi90 DCS, which has served the City well, but is nearing the end of its effective service life. The current installations typically contain one or more DCS process control units per process area, and remote I/O is only utilized at the NEWPCC UV disinfection facility. All I/O is currently centralized by process area.

As part of the master planning process, the City has made a decision to retire the existing DCS architecture and move towards a PLC-based architecture. The PLC architecture would be based upon small or moderately sized units that are physically distributed and logically associated with specific units or processes, rather than being based upon large centralized units. Where remote I/O is utilized, it will be decentralized to the greatest degree that is practical. HVAC systems will typically be controlled by dedicated PLCs, independent of the process PLCs. It is expected that PLC processor redundancy will be required only for critical systems.

The proposed architecture would include independent field networks, not physically connected to the process networks interconnecting the PLCs, to collect remote I/O and networked instrumentation. Similarly, the process network would be physically isolated from the administration, security and video networks. Various potential configurations for the process network, utilized to interconnect the PLCs, local HMIs, and the HMI servers, are discussed and evaluated based upon the reliability and performance requirements of the treatment facilities.

Installations for the SEWPCC and WEWPCC facilities would include a server room, where the HMI servers, historian, and other servers would be located. It is expected that these installations would be located within the Administration area of the facility, and be adjacent to the main control room. It is proposed that the NEPWCC facility, which is assumed to be the location for centralized monitoring of the entire City treatment systems, would include two server rooms, configured for redundancy.

The selection of a control system vendor is identified as a critical task in the overall design process, and consequently should be completed prior to the initiation of detailed design for the first facility to be upgraded. The selection of the PLC and the HMI systems should be predicated on a two-stage evaluation process, with the second stage evaluation primarily based upon the presentation of a vendor-configured demonstration system.

Migration Strategy

The existing ABB/Bailey Infi90 DCS system will be replaced as part of the proposed control system upgrades. An appropriate migration strategy must be adopted to ensure that the DCS control of the facilities will remain fully functional until and during the conversion. First, the existing DCS system must remain fully functional until replaced, and it is therefore necessary to upgrade critical obsolete components to assure the required service life during the interim period. The existing DCS HMI is obsolete and is not expected to remain in a reliable maintainable state beyond the near term. The replacement of the DCS HMI is required immediately.

The migration from the existing DCS to the new PLC-based control system is to be accomplished with the comprehensive replacement of all DCS equipment in each process area with the corresponding new PLC system. Both the DCS HMI and the new HMI systems would operate in parallel until the transition of all the process areas is complete. The City has indicated that the complete transition, where two HMI systems are utilized in parallel, should not exceed 12 months.

HMI and Enterprise Systems

The Human Machine Interface (HMI) system provides operator monitoring and supervisory control of the wastewater treatment facilities. The architecture proposed for the HMI system is a redundant server configuration with thin HMI clients, based on terminal services. The

HMI clients will include desktop clients in the control room, but also local touchscreens in the process areas and wireless operator devices for mobile access. Server virtualization, which allows multiple logical server computers to operate on a single physical computer, will be utilized where approved by the control system vendor, and the configuration is appropriate.

The existing graphic configuration scheme in use at the wastewater treatment facilities was developed in the late 1980s, while current industry direction utilizes a shades-of-gray style approach. Under this scheme, bright colours are reserved for abnormal situations, and normal operations are de-emphasized utilizing shades of gray and muted colours.

Effective alarm management is critical to successful operation of the wastewater facilities. In addition to providing the appropriate control system alarm capabilities, a formal alarm management program for the new installations is required.

A main control room will be provided for each facility, as the principal control location for the entire facility, and must be configured in a manner to allow for efficient and effective monitoring. In addition, as the SEWPCC and WEWPCC facilities are only staffed during normal working hours, continuous monitoring of all City wastewater facilities from a central location will be required. Since the NEWPCC facility has provided this function to this point, it is assumed that the NEWPCC will continue to be utilized for central monitoring. Based on the proposed HMI architecture, remote thin clients will be utilized to view and control the operation of any facility, simply by connecting to the appropriate HMI server. While the current remote monitoring of the SEWPCC and WEWPCC facilities is very basic, the proposed architecture will allow for comprehensive remote monitoring and control. A sufficient number of operator terminals, and associated networking services will be required at the NEWPCC facility to accommodate the proposed functionality. Since the existing basic monitoring system between the SEWPCC and NEWPCC will be abandoned as part of the impending SEWPCC control system upgrades, upgrades to the NEWPCC control room will be required to support the proposed monitoring system, prior to the completion of the SEWPCC expansion project. It expected that the NEWPCC control room upgrades will be implemented as a separate project from the SEWPCC upgrade; however, the two undertakings will need to be coordinated.

Remote access to the facility control systems is required to allow off-site or on-call operations personnel to support the operation of the facilities. Various potential implementations of view only and control capable mobile and fixed remote access are presented in the report.

Integration of enterprise systems such as the City's Computerized Work Management System (CWMS), Laboratory Information Management System (LIMS), and the proposed Process Control Management System (PCMS) is presented to achieve a fully integrated system and to avoid multiple data entry requirements. While current technologies allow for integration, the efforts required to successfully integrate enterprise systems are not insignificant. In view of this reality, it is expected that the City will perform the required integration as a second phase initiative, after successful deployment of the new control system. In preparation for this implementation, integration features and capabilities must be included as part of the control system specification, and evaluated to ensure that integration capabilities are not overlooked in the selection process of the new control system.

Historical Data and Reporting

Retention of and access to historical data is essential for the operation and maintenance of the wastewater treatment facilities. The automation system must have all the required capabilities to log and retain critical data at the required intervals, as well as report the data in a manner useful to City personnel. It is proposed to install a site historian at each facility to log data, and transfer the data to a Central Historian Server for long term archival. The Central Historian Server should also respond to historical data requests from users outside of the treatment facilities. The architecture would be configured in a manner to allow for local operation, via the site historian, in the event the Central Historian were not available.

Networking

Current automation systems extensively utilize Ethernet based networks for communication between various automation components. It is proposed to physically segregate the automation system Supervisory, Process and Field networks from the Administration and Security networks, to provide a high level of availability and security. Wide-area network communications are also required between the NEWPCC, SEWPCC, and WEWPCC facilities, which may be routed over third party connections. It is expected that Virtual Private Networking (VPN) technology will be utilized to provide the required security for the inter-facility communication. Demilitarized zones (DMZ) will be utilized to segregate network traffic between the enterprise and automation systems, in a manner such that general network traffic does not cross the boundaries between the two systems, but rather terminates in the DMZ.

The automation process networks that serve to connect the process areas will typically be arranged to physically map to the facility process areas. Local wireless access for control will be integrated into the automation system networks, without being routed onto the enterprise system networks.

It will be necessary for the City to formalize the responsibility for maintenance of the automation system Ethernet networking. While City IT personnel are well qualified to service business information systems, they typically are not trained in process automation and control systems, and their specific networking requirements. It is therefore imperative that the complete automation system, including networking, be maintained by dedicated automation maintenance personnel, independent of the City's IT group. However, IT enterprise IT resource involvement will be required for specific initiatives, as discussed in the report.

Security

Security is an extensive subject and the scope of this report is limited to network security within the context of the automation system. Appropriate defence mechanisms are required at the boundary of the automation system, to ensure that the operation of the facilities is not compromised. The use of remote devices will allow for efficiencies in the access of real-time information from the automation system; however, such access must be secured through appropriate security mechanisms. A two-factor authentication should be implemented, where the consequence of unauthorized access is significant, such as for remote control. Specific high-level design criteria are described to guide the automation system designers in the application of acceptable security requirements.

Operations and Maintenance Considerations

Consideration must be given to issues affecting operation and maintenance requirements prior to the selection and installation of the automation equipment at the wastewater treatment facilities. Primarily, appropriate training of operations and maintenance personnel is indicated to be imperative for successful system deployment. In addition, the inclusion of a testing and simulation system is described to facilitate for the testing of system upgrades and new software implementations, as well as training of operations and maintenance personnel.

Equipment Standardization

The potential standardization of automation equipment vendors for the wastewater treatment facilities was reviewed and the following principle benefits were identified:

- Maintenance of compatibility between equipment
- Reduction in training requirements
- Reduction in spare parts
- Reduced engineering requirements for new equipment application
- Reduced maintenance efforts

The benefit of standardizing automation equipment was reviewed in the report, and specific items were identified as candidates for standardization. The standardization of the control system, including PLCs and the HMI system, is deemed to be the highest priority, with Variable Frequency Drives (VFDs) and Intelligent MCCs also prioritized. The implementation of standardization for these and other automation equipment will require specific Bid Opportunity processes to allow for competitive selection.

City Technical Standards

It is required that the City prepare technical automation standards to ensure a consistent high-quality automation installation at the wastewater treatment facilities. Specific standards to be developed include an Identification Standard, Automation Design Guide, Tagname Identification Standard, HMI Layout and Animation Plan, Historical Data Retention Standard, and a Backup and Disaster Recovery Plan.

Project Documentation

Detailed automation documentation is a key requirement to ensure that the automation system design and installation meets the City’s operational needs, as well as facilitation of proper maintenance. The design document preparation should utilize a lifecycle approach, rather than a construction-based approach, to ensure that a complete set of documents detailing the entire plant (new and existing systems) are produced. Minimum documentation requirements are identified in the Master Plan, clarifying the responsibility of the Consultant and the Contractor regarding the level of detail to be provided by each party.

The City's Computerized Work Management System (CWMS) will need to be updated as part of the overall project completion tasks for the work, to ensure that all new and modified plant systems are identified for future ongoing maintenance.

Risk Review

As part of the Master Plan, presently known risk issues were identified along with proposed mitigation strategies. Additional issues may arise and should be assessed in a consistent manner. The issues noted include:

- Potential failure of the existing DCS HMI
- Failure of the existing DCS control hardware prior to system replacement
- Design document quality control due to potentially ineffective review
- Cost overruns
- Software implementation errors
- Unplanned effect on the existing process during the construction work
- Signal noise and grounding issues
- Compatibility issues
- Competency of the design engineer and system integrator
- The organization of the City's automation maintenance group(s)

Implementation Plan

Implementation of the proposed work in the Automation Master Plan will be subject to extensive coordination and will be part of the scope of a variety of project undertakings by the City. While the majority of the work is expected to be addressed under the primary design and construction projects of the specific wastewater treatment plant upgrade projects, a significant amount of supporting work is required before, during, and after the major project design process. Specific automation projects identified for implementation are identified on the following page.

Priority	Project	Recommended Start	Recommended Completion
1	Replacement of the DCS HMI at the wastewater treatment facilities.	ASAP	ASAP
1	The development of an equipment identification standard.	2012 Q2	2012 Q4
1	Standardization of critical electrical and automation components.	ASAP	2013 Q3 (Control System) 2014 Q2 (Overall)
1	Preparation of an automation design guide and other automation technical standards.	2012 Q3	2013 Q3 (Automation Design Guide) 2013 Q4 (Remainder)
2	Review and upgrades of existing DCS hardware at the SEWPCC facility.	2013 Q3	2013 Q3
2	Review and upgrades of existing DCS hardware at the WEWPCC facility.	2013 Q3	2013 Q3
2	Upgrade the NEWPCC Central Control and Server Rooms.	2014 Q1	2016 Q1
3	Review and upgrades of existing DCS hardware at the NEWPCC facility.	2014 Q2	2014 Q4
3	Preparation of a Backup and Disaster Recovery Plan.	2015 Q3	2015 Q4
3	Integration of the Computerized Work Management System with the HMI.	2015 Q4	2016 Q4
3	Integration of the Laboratory Information Management System with the HMI and Historian.	2016 Q4	2017 Q4
3	Provision of interfaces to allow for the automated sharing of operational information between Collections and Wastewater Treatment Systems.	2017 Q1	2017 Q3

1.0 INTRODUCTION

The City of Winnipeg has initiated a program to perform upgrades to the wastewater treatment systems at the NEWPCC, SEWPCC, and WEWPCC facilities. As part of these upgrades, automation systems are required for process control and monitoring. These automation systems must be installed to provide effective monitoring and control of the wastewater treatment processes. There are many methods of implementing an automation system, and the purpose of this document is to provide an overall strategy for automation installations that are consistent with the City's needs. It is expected that this document will form the basis for future design work.

1.1 Overall Project Objectives

The overall objective for the Automation Master Plan is to plot a course for automation system upgrades at the City of Winnipeg wastewater treatment facilities. This will provide guidance regarding the overall control system architecture along with the associated instrumentation and motor control. The control system architecture will also include the required high level integration for HMI and enterprise systems.

1.2 Master Plan Scope and Limitations

As noted, the objective of this document is to provide guidelines and definition for the implementation of automation systems within the wastewater treatment facilities. The City is currently embarking on an extensive program of facility upgrades and it is therefore timely to have a master plan in place to provide designers with the guidance necessary to serve as a basis for the automation designs.

The scope and intent of this document is intended to convey the specific guidance regarding automation systems and is presented at a high level in order that design direction can be established. This document does address specifics related to equipment type, selection, and configuration, however the designs are presented without knowledge of the specific process implementation. It is not within the scope of this report to provide detailed design direction, and it will be the responsibility of the respective system designers to fully develop the automation design details with general conformance to the concepts presented herein.

Verification of the proposed concepts, architectures, and implementation will be required as part of the automation design process for the wastewater treatment facility upgrades. It should also be noted that automation technology has evolved significantly within recent history, and it is expected that this significant pace of development will continue. In some cases the technological developments may present new methods for implementation, or invalidate current acceptable concepts. It is recommended that qualified automation design engineers be utilized for the proposed upgrade projects, who will take ultimate responsibility for the designs. In addition, appropriate review of the designs prepared should be performed by experienced automation professionals on behalf of the City.

1.3 Definitions

AS-I	Actuator Sensor Interface (Industrial fieldbus network)
ASM	Abnormal Situation Management Consortium
ATS	Automatic Transfer Switch
CIP	Common Industrial Protocol
CPT	Control Power Supply
CSA	Canadian Standards Association
CWMS	Computerized Work Management System
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
E&I	Electrical and Instrumentation
FAT	Factory Acceptance Test
FRS	Functional Requirements Specification
FVNR	Full Voltage Non-Reversing (Starter)
H_2S	Hydrogen Sulfide
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
H/O/A	Hand – Off – Auto (switch)
HVAC	Heating Ventilation and Cooling
I/O	Input / Output
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers

IPSec	Internet Protocol Security
ISA	International Society of Automation
LIMS	Laboratory Information Management System
MCC	Motor Control Centre
MTBF	Mean Time Between Failure
NEMA	National Electrical Manufacturers Association
NEWPCC	North End Water Pollution Control Centre
NFPA	National Fire Protection Association
NVRAM	Non-Volatile Random Access Memory
ODVA	Open Device Vendors Association
P&ID	Process and Instrumentation Diagram
PAC	Programmable Automation Controller
PCG	Process Control Group
PCV	Process Control View (Existing HMI software)
PDA	Personal Digital Assistant
PDF	Portable Document Format
PLC	Programmable Logic Controller
POF	Probability of Failure
RAID	Redundant Array of Independent Disks
RFID	Radio Frequency Identification
RGB	Red Green Blue
RSTP	Rapid Spanning Tree Protocol
SCADA	Supervisory Control and Data Acquisition
SCCR	Short Circuit Current Rating
SEWPCC	South End Water Pollution Control Centre
SIS	Safety Instrumented System
TCP	Transport Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VFD	Variable Frequency Drive
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEWPCC	West End Water Pollution Control Centre

WPA2	Wi-Fi Protected Access Version 2 (security protocol)

2.0 SCOPE OF AUTOMATION AND CONTROL

The automation and control systems at the City of Winnipeg Wastewater Treatment Plants will monitor and control the process systems of the facilities. In addition to the process control systems, there are numerous ancillary systems that potentially require monitoring and control. The purpose of this section is to identify the level of integration of the various systems within the wastewater treatment facilities with the automation and control system.

In general, it is expected that the level of integration for the systems can be classified into four categories, as follows:

Full The system will be fully monitored and controlled by the automation system.

Detailed Monitoring The system will be fully monitored by the automation system. This will included multiple detailed alarms, with sufficient information to determine the source of an issue, without looking at an alternate or local control panel.

Basic Monitoring The automation system will have basic monitoring of the system. This could be comprised of one or more general alarms, and in the event of an abnormal situation would generally require personnel to utilize a separate system to fully determine the issue.

None There will be no integration with the automation system.

A summary of various systems, including ancillary systems, within the wastewater treatment plants, and the level of automation system integration is presented in Table 2-1, followed by a discussion for ancillary systems in Section 2.1.

Table 2-1 : Integration of Various Wastewater Treatment Systems

System	Level of Integration	Notes
Process Systems – All	Full	
Electrical Power System	Detailed Monitoring	See Section 2.1.1
Fire Alarm System	Detailed Monitoring	See Section 2.1.2
Gas Detection System	Detailed Monitoring	Associated annunciation and switching of HVAC controls must be via code approved system.
HVAC Controls	Full	See Section 2.1.3
Instrument Air	Detailed Monitoring	Control will be independent.
Potable Water	Basic Monitoring	
Sampling Systems	Application Dependent	See Section 2.1.4
Sump Pumps	Detailed Monitoring	Control will typically be via local ultrasonic or float.
Boiler / Chiller Plant	Full	Individual boilers and chillers will have integral proprietary management systems, however the Automation System will fully integrate the overall system.
Lighting Control	Basic Monitoring	See Section 2.1.5
Security / Access Controls / Video Surveillance	Basic Monitoring	See Section 2.1.6
Communication Systems	Basic Monitoring	

2.1 Ancillary Systems

There is potential for various ancillary systems to be integrated into the automation control system. With currently available technology, almost any ancillary system can technically be integrated; however the benefits of integration do not necessarily outweigh the costs. A brief discussion of selected ancillary systems is presented below to clarify the summary presented in Table 2-1.

2.1.1 Electrical Power System

The electrical power system is critical to the operation of the wastewater treatment facilities. It is proposed that the electrical power system should be monitored by the automation control system to ensure that all information is provided to a central location and appropriate information is logged to the historian. Detailed monitoring of the facility will aid in future energy optimization and control initiatives. A general list of items to be monitored includes the following:

- Power meters
  - Power meters are to be supplied for each significant point in the electrical distribution system. For example, MCCs will typically have power meters installed.
- Generator status and alarms.
- Transfer switch status
- Status of Main and tie breakers
- UPS systems
- Transformer Neutral Grounding Resistors (if present)

2.1.2 Fire Alarm System

A comprehensive fire alarm system is currently installed at the SEWPCC facility. In addition, the NEWPCC facility has local fire alarm systems for selected areas of the facility. The NEWPCC Administration Building, Grit Building, and Digester Building have local fire alarm systems that cover the electrical and control rooms within the given area. The Phosphorus Removal and UV Disinfection facilities have fire alarm systems that generally cover the entire building. The control rooms of other process areas, not covered by a fire alarm system, generally have smoke detectors connected to DCS alarms, with the exception of the Primary Clarifier area.

Since fire alarm systems are critical to life safety and facility protection, appropriate integration with the automation system is recommended. While fire alarm systems must be separate from the automation control system due to specific installation code requirements associated with fire alarm systems, monitoring from the automation control system is recommended to allow for historical logging and annunciation in the control rooms. Modern fire alarm systems have the capability to indicate their status to the control system, and it is proposed that all alarm and trouble status signals should be networked to the control system for display on the HMI and logging in the historian.

2.1.3 HVAC Controls

The existing HVAC controls in the wastewater treatment facilities are controlled by a variety of methods including proprietary electronic controls, pneumatic controls, hardwired interlocking, DCS control, and PLC-based control. The lowest installed cost for HVAC controls would be provided by commercial-grade HVAC controllers, however it is proposed that all HVAC control be integrated with the primary process automation system for the following reasons:

- Commercial-grade HVAC controllers typically have a shorter product lifespan.
- The reliability of commercial-grade HVAC controllers is typically lower.
- Additional training and spare parts inventory would be required for commercial-grade hardware and software maintenance.
- Integration of the commercial-grade systems into the primary automation control system is typically not straight-forward.

2.1.4 Sampling Systems

The level of automation integration of process sampling systems is dependent upon the specific requirements of the application. At minimum, basic monitoring of sampling system failure will be provided. For some systems, the sampling system could potentially be completely controlled by the automation system. Integration may even be required to accomplish scenarios where flow based sampling is required. However, future regulatory requirements may require an independent control system in some applications, and only monitoring may be permissible. Thus, it is recommended to review the level of automation system integration on a case-by-case basis.

2.1.5 Lighting Controls

Lighting controls at the existing wastewater treatment facilities are comprised entirely of manual switches, along with some automatic photo-eye switches and timers for outdoor lighting. Typically, lighting is left on in most areas of the existing facilities, as multiple entry and exit points, large process areas, and high-intensity discharge (HID) lamp warm-up delays do not allow for convenient manual light switching.

More advanced lighting control systems, which can include occupancy sensors, microprocessors and timers, are available and in some cases are integrated with the access control system. While it is expected that there will be some lighting control in the upcoming upgrades, it is assumed that the lighting control will be relatively basic, and will not utilize a sophisticated dedicated microprocessor system or a lighting control system integrated with the security / access controls. As an example, it is expected that some process areas could utilize a master contactor, which turns off the lighting in the majority of a building at 4pm based upon a 24 hour timer, along with some override switches.

In certain process areas, it is expected that the state of the lighting switch could be utilized to indicate occupancy to the control system, to allow for the appropriate level of ventilation during the presence of personnel. Due to Winnipeg's cold climate, a ventilation scheme whereby the ventilation rate is lowered when not occupied allows for significant energy savings. For example, the scheme to utilize a light switch to control the ventilation rate is currently being installed for the SEWPCC wet well ventilation.

Given that the lighting controls are expected to be basic, it is deemed that basic monitoring of the lighting control will be via the automation control system is the appropriate level of integration for this system. Modifications to this level of integration could be considered on an incremental basis where deemed appropriate.

2.1.6 Security / Access Controls / Video Monitoring

Security systems that are expected to be required at the wastewater treatment facilities include the following:

- Access control
- Intrusion Detection
- Video monitoring

The City's existing wastewater treatment facility access control is typically based on keys, although it should be noted that RFID is utilized at the NEWPCC facility for some doors.. The City's existing intrusion detection, where provided, at the wastewater facilities is typically connected directly to DCS inputs. In addition, the City does have some existing video monitoring at the wastewater facilities, which is provided by a dedicated CCTV system independent of the automation system.

For most current construction, the security and access control systems are typically provided by an independent proprietary system. The primary driver of this is cost, and the use of equipment that is designed for the intended purpose. While it is possible for the security system to be tightly integrated into the automation system, it is expected that the cost for a closely integrated system will be significantly higher than for an independent proprietary system. Thus, it is proposed that the security and access control systems be independent of the automation system.

It is recommended that the integration between the automation system and the security and access control system be limited to the following:

- System trouble alarms are to be displayed and logged on the control system.
- Summary security alarms are to be displayed and logged on the control system.

It is proposed that the integration of the security system and access control with the automation system be via a network-based interface, such as OPC, provided by the security system. This will allow for straightforward integration of the required data.

It is expected that video monitoring will be provided by a network of IP based cameras, which communicate via a plant-wide Ethernet network. It is expected that the video monitoring would be independent of the automation system for the same reasons as noted above. If it is deemed necessary to display live video on an HMI screen for operator monitoring of a specific process, this would be integrated via IP routing of the video signal to the HMI system. See Section 14.0 regarding specific networking requirements.

Note: The level of security devices and access controls required to ensure the physical security of the facility is outside of the scope of this report.

3.0 RELIABILITY REQUIREMENTS AND ANALYSIS

3.1 Reliability Requirements

The City of Winnipeg wastewater treatment facilities provide a critical service for the residents of the City. Reliability is a measure of the ability of a system or component to perform its designated function without failure. Reliability assessment can include subjective characterization of the reliability, as well as quantitative values such as probability of failure (POF), mean time between failures (MTBF) and availability. Quantitative analysis of reliability is appropriate in some situations, but can be difficult to perform on larger systems, especially where statistical data is not available. Historically, automation system reliability decisions have often been made based on very subjective opinions of the design team, or in some cases the owner's operations and maintenance personnel. This section describes some basic high-level reliability analysis to allow a regimented and consistent approach to the review of a proposed design's reliability that can be compared to specific process requirements. However, it should be noted that the analysis discussed in this section is very basic, and is not an alternative for in-depth reliability analysis where appropriate.

The methods described below, are only suitable for non-safety systems. Safety systems require more formal methods of analysis, and the ISA-84 series of standards should be referred to as a guide for detailed analysis.

3.1.1 Basic Reliability Analysis

Reliability analysis provides methods to determine if a proposed design solution is adequate to meet the requirements of the process. Ultimately, the goal of reliability is to reduce risk and/or cost. Cost-based reliability analysis is not typically suited to a wastewater treatment facility, and risk analysis is more appropriate. When performing risk analysis, risk is generally defined as *Risk = Probability x Consequence*. Thus, both the probability of the event and the consequence can have a significant impact on risk, and it is vital that reliability analysis include both probability and consequence.

Consequence	Description	Design MTBF
Negligible	The effect of the failure can easily be addressed by facility personnel without any significant affect on the process.	1
Minor	The affect of the failure on the process is limited, and will not significantly affect the long term average of the treatment process quality.	10
Significant	The failure is expected to have a noticeable impact on the effluent quality, potentially result in a relatively small spill to the river, or cause some limited damage to equipment.	100
Major	The failure is expected to have a large impact on the effluent quality, result in a considerable spill to the river, flood basements of residents, or cause significant equipment damage. This is likely an event that would be in the local news.	1000
Catastrophic	Death, or irreparable environmental damage.	See Note
Note: *The analysis described in this section is not suitable for assessing the reliability of catastrophic events.*		

Table 3-1 : Defined Consequence of Failure

The consequence of a potential failure event is subjective, and cannot be easily quantified. Thus, five categories are proposed in Table 3-1, to allow for classification of failure events. It should be noted that catastrophic events are beyond the scope of the reliability analysis presented in this section, and other references such as the ISA-84 standards series should be referred to. Table 3-1 also indicates a design MTBF (Mean Time Between Failure) for each consequence. Essentially, this table is defining a fixed tolerable risk, and as the consequence increases, the probability must decrease. Note that probability is the inverse of MTBF.

Each control system has an overall reliability based upon the details of the design, the reliability of the individual components, and the level of redundancy and self monitoring in the design. Detailed reliability analysis of overall control systems is appropriate for certain critical applications, but is not typically applied to most systems within wastewater treatment. During control system design, decisions regarding architecture and redundancy are often made subjectively. On the other hand, the proposed analysis can facilitate a more structured high level review determine the reliability of the control system. The proposed analysis will compare the expected MTBF of a control system element with the design MTBF from Table 3-1, for the consequence associated with the control system failure. While this method is not necessarily precise, it is at minimum, a good check of a subjective design decision.

Determination of the appropriate design MTBF is not necessarily straightforward as the consequence can change dependent on the failure mode or upon the process requirements, such as incoming flow. It is recommended that each failure mode be assessed separately and that the proposed architecture MTBF exceed the design MTBF for each failure mode. In addition, where process conditions can change the consequence, it is proposed that that the consequence for each process condition be assessed, and a weighted average of the MTBFs and the estimated percent of time that the given process condition is applicable, be utilized to establish the overall MTBF for the design case.

The consequence of failure modes can also vary with time. For example, if a raw sewage pump is interrupted for one minute, the consequence is significantly less than if it is interrupted for a day. For each consequence, a duration (D) is assigned at which time the consequence becomes applicable. If the failure repair time is less than the duration (D), then the consequence is not deemed to be applicable.

It is recommended that the consequence of failure and the associated reliability requirements be reviewed with City operations personnel and process engineers.

3.1.2 Examples - Raw Sewage Pumping

Note: The examples presented below uses estimated values for illustration purposes only. All values require review and confirmation at the time of design.

The proposed basic reliability analysis is illustrated further below using examples. The first example is for the PLC controller configuration of the raw sewage pumping. The process scenario proposed is four raw sewage pumps, with approximately equal flow rates. The analysis shown in Example 1A is based upon a PLC configuration with two PLCs, each controlling two pumps, with no hot standby. The MTBF of a controller is estimated to be 15 years, however during design actual data available for the specific controller should ideally be utilized. The MTBF of two controllers failing simultaneously is 15^2, provided that the time to repair is significantly less than the MTBF. It should also be noted that the proposed control system has manual controls available for the pumps, which limits the consequences of controller failures.

Example 1A assesses two failure modes: failure of all pumps (both PLCs fail) and failure of two pumps (one PLC fails). For the first failure mode, where both PLCs fail, the consequence of failure is *Major*, if the flow is greater than the capacity of two pumps. Note that the duration (D) before the major consequence is deemed to be 0.1 hours, which is much less than the repair time of four hours, and thus the consequence is applicable. The flow rate is estimated to be in this range for approximately 10% of the time, and thus the weighted contribution of this process condition is 10% x 1000 (Major) = 100. Similarly, when the flow rate is less than the capacity of two pumps, which is estimated to be 90% of the time, the consequence of the failure is deemed to be *significant* and the design MTBF contribution is 90% x 100 = 90. The total design MTBF for the failure of all pumps is deemed to be 190 years, and since the MTBF of both PLCs failing is estimated to be 225 years, the architecture appears to be acceptable for this failure mode.

A second failure mode (Failure Mode B) is examined where one of the two PLCs fail, causing two pumps to be taken out of service. In this case, if the flow rate is less than the capacity of two pumps, it is not expected that the consequence will be applicable in less than eight hours, and thus no design MTBF is assigned for this flow scenario. Where the flow rate is above the capacity of two pumps, which is estimated to be 10% of the time, the consequence is deemed to be between *significant* and *major*, and a design MTBF of 500 years is assigned, which results in a weighted design MTBF of 50 years based upon the percent of time in this scenario. As the design MTBF is significantly higher than the actual MTBF of one PLC failure, which is 15 years, the proposed system design would not be acceptable and modification of the design would be in order.

Note that the duration (D) is deemed to be an estimate of time from the initial failure event to when the consequence becomes significant. It is quite typical in wastewater applications that the consequence increases with time. For example, if the raw sewage pumps stop for a few minutes under most flow scenarios, the consequence is negligible, however a long duration outage is significant. The use of the duration (D) parameter is used in comparison with the repair time, and if the repair time is less than the duration, the consequence is not deemed to be significant. This concept was utilized in the second failure mode, where under low flow conditions, it is deemed that local manual control for up to eight hours is acceptable, and repair of the PLC is estimated to take less than eight hours.

Basic Reliability Analysis – Example 1A					
Process	**Raw Sewage Pumping – Four Pumps**				
Proposed System	**Two PLCs – each control 50% of pumps**				
System Analysis	Repair Time	4 hours			
	MTBF – 1 PLC	15 years			
	MTBF – 2 PLCs	225 years			
Notes	Manual control provided, which limits consequence				
Failure Mode A	**Control system failure for all pumps**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two pump capacity	90%	0.5	Significant	100
	Flow > two pump capacity	10%	0.1	Major	1000
	Design MTBF (Weighted Average)				**190**
Notes	System Proposed Acceptable for this Failure Mode				
Failure Mode B	**Control system failure for two pumps**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two pump capacity	90%	8	Minor	-
	Flow > two pump capacity	10%	0.5	Significant - Major	500
	Design MTBF (Weighted Average)				**50**
Notes	System Proposed Not Acceptable for this Failure Mode				

The *Pct* field is utilized to assess the relative probability of each specific case reviewed. Each case is assigned a design MTBF, which is then averaged using a weight based on the *Pct* field. In the example above, it is estimated that the flow only exceeds the capacity of two pumps approximately 10% of the time, and thus the design MTBF associated with this flow scenario is only weighted at 10% in the average. The assignment of the *Pct* field can be estimated, but ideally would be based upon historical process data.

The second example (Example 1B) looked at is the same raw sewage pumping process, but with four PLCs, each controlling one pump. In this case, the probability of simultaneous failure of the four pumps becomes negligible (once in 50,625 years). While there will be common modes of failure, such as power supply, which in practicality will increase the system failure probability, it is proposed that these issues would be assessed independently. The failure modes reviewed are essentially the same as Example 1A, except that the failure mode of one PLC failure affecting only one pump is also reviewed. For each failure mode, the design MTBF is lower than the designed control system architecture MTBF, and thus the design is deemed to be a suitable architecture application.

The third example (Example 1C) also looks at the same raw sewage pumping process, but with a pair of hot standby, redundant PLCs controlling all four pumps. In this case, the failure of a single controller does not affect the process, and analysis is therefore not required. The only case to be analyzed is for failure of all four pumps, when both redundant controllers fail simultaneously, which is estimated to occur every 200 years. The required MTBF for the four pump failure scenario, is the same as the previous examples, 190 years, and thus the proposed design of the control system configuration also appears to have sufficient reliability to meet requirements.

Basic Reliability Analysis – Example 1B					
Process	**Raw Sewage Pumping – Four Pumps**				
Proposed System	**Four PLCs – each control one pump**				
System Analysis	Repair Time	4 hours			
	MTBF – 1 PLC	15 years			
	MTBF – 2 PLCs	225 years			
	MTBF – 3 PLCs	3375 years			
	MTBF – 4 PLCs	50625 years			
Notes	Manual control provided, which limits consequence				
Failure Mode A	**Control system failure for all pumps**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two pump capacity	90%	0.5	Significant	100
	Flow > two pump capacity	10%	0.1	Major	1000
	Design MTBF (Weighted Average)				**190**
Notes	System Proposed Acceptable for this Failure Mode				
Failure Mode B	**Control system failure for two pumps**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two pump capacity	90%	8	Minor	-
	Flow > two pump capacity	10%	0.5	Significant - Major	500
	Design MTBF (Weighted Average)				**50**
Notes	System Proposed Acceptable for this Failure Mode				
Failure Mode C	**Control system failure for one pump**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two pump capacity	90%	8	Negligible	-
	Flow > two pump capacity	10%	3	Minor	10
	Design MTBF (Weighted Average)				**1**
Notes	System Proposed Acceptable for this Failure Mode				

Basic Reliability Analysis – Example 1C					
Process	**Raw Sewage Pumping – Four Pumps**				
Proposed System	**Hot Standby PLC Architecture – One Redundant PLC Pair**				
System Analysis	Repair Time	4 hours			
	MTBF	200 years			
Notes	Manual control provided, which limits consequence. Due to additional complexity, failure rates for primary controller/system will be slightly higher than for a standalone system. Estimated to be 14.1 years MTBF. MTBF does not include I/O.				
Failure Mode A	**Control system failure for all pumps**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design TBF**
	Flow < two pump capacity	90%	0.5	Significant	100
	Flow > two pump capacity	10%	0.1	Major	1000
	Design MTBF (Weighted Average)				**190**
Notes	System Proposed Acceptable for this Failure Mode				

3.1.3 Examples – Primary Clarifiers

Note: The examples presented below uses estimated values for illustration purposes only. All values require review and confirmation at the time of design.

One basic reliability analysis example for a potential primary clarifier sludge pumping process is presented. The proposed process configuration has four tanks, with four independent sludge pumping systems. The proposed control system architecture has two PLCs, each controlling two of the four sludge pumping systems. The MTBF of the PLCs are the same as presented in Example 1.

The process requirements are estimated as shown, however it should be noted that these are not based upon a specific facility or input from process engineers and are shown for illustrative purposes only. When the sludge flow rate is less than the processing capability of two tanks, failure of all sludge pumping systems is deemed to have a *minor* consequence after eight hours. However this is not included in the weighted MTBF contribution, as the repair time is estimated to be four hours which is much less than the eight hours of acceptable duration prior to the consequence. When the flow exceeds the processing capacity of two tanks, the consequence of failure is deemed to be significant after two hours, and thus the weighted contribution to the design MTBF is 40% x 100 = 40. As the MTBF between both PLCs failing is 225 years, the proposed architecture is acceptable for Failure Mode A.

Under Failure Mode B, where one of the PLCs fails and sludge pumping is interrupted for two of the four tanks, the analysis shows that the proposed control system configuration is acceptable as design from a reliability perspective.

Basic Reliability Analysis – Example 2					
Process	**Primary Clarifiers – Sludge Pumping – 4 Tanks**				
Proposed System	Two PLCs – each control 50% of process				
System Analysis	Repair Time	4 hours			
	MTBF – 1 PLC	15 years			
	MTBF – 2 PLCs	225 years			
Notes	Manual control provided, which limits consequence				
Failure Mode A	**Control system failure for all sludge pumping (4 Tanks)**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two tank capacity	60%	8	Minor	-
	Flow > two tank capacity	40%	2	Significant	100
	Design MTBF (Weighted Average)				**40**
Notes	System Proposed Acceptable for this Failure Mode				
Failure Mode B	**Control system failure for sludge pumping for two tanks**				
Failure Analysis	**Case**	**Pct**	**D (h)**	**Consequence of Failure**	**Design MTBF**
	Flow < two pump capacity	60%	24	Negligible	-
	Flow > two pump capacity	40%	3	Minor	10
	Design MTBF (Weighted Average)				**4**
Notes	System Proposed Acceptable for this Failure Mode				

3.1.4 Example - Network Cable

Note: The examples presented below uses estimated values for illustration purposes only. All values require review and confirmation at the time of design.

This final example reviews the reliability requirements for communication network cabling that connects the Headworks Process Area PLCs with the server room where the HMI servers are located. Upon failure of this network link, all HMI monitoring and control capability for the Headworks area would be lost (other than any local monitoring capability provided). In addition, it is expected that other process areas would require the incoming flow rate as part of their control strategy, and when this is not available, there would be a slow degradation of treatment due to less than optimal control.

The estimated reliability for various cable configurations is presented below. The failure mode investigated is the potential for network failure of both cables. In this case, only the cables are assessed as they will have a long replacement time. Separate analysis should be performed for the network switches, or the system as a whole.

The consequence of network failure causing loss of monitoring and control of the *Headworks* process area is deemed to have a *minor* consequence if the failure duration for less than four hours. On the other hand, the consequences would be *significant* if the failure duration exceeded eight hours. As the repair time is estimated to be 40 hours, the overall consequence is *significant*, and a design MTBF of 100 years is assigned. Only a network design configuration where two independent cables are installed via separate routes provides the required level of reliability, and thus is the minimum configuration that should be utilized.

<table>
<tr><th colspan="6">Basic Reliability Analysis – Example 3</th></tr>
<tr><td><b>Process</b></td><td colspan="5"><b>Headworks Process Area</b></td></tr>
<tr><td><b>Proposed System</b></td><td colspan="5">Network connection to server room – redundant, not looped</td></tr>
<tr><td rowspan="4">System Analysis</td><td>Repair Time</td><td colspan="4">40 hours</td></tr>
<tr><td>MTBF – 1 cable</td><td colspan="4">50 years (no effect)</td></tr>
<tr><td>MTBF – 2 cables (not independent routes)</td><td colspan="4">75 years</td></tr>
<tr><td>MTBF – 2 cables (independent routes)</td><td colspan="4">2500 years</td></tr>
<tr><td>Notes</td><td colspan="5">With network fibres out of service, HMI monitoring and control completely out of service. Other processes that are based upon incoming flow rates would not operate well.</td></tr>
<tr><td><b>Failure Mode A</b></td><td colspan="5"><b>Network failure of both cables</b></td></tr>
<tr><td rowspan="4">Failure Analysis</td><td><b>Case</b></td><td><b>Pct</b></td><td><b>D (h)</b></td><td><b>Consequence of Failure</b></td><td><b>Design TBF</b></td></tr>
<tr><td>Any Flow</td><td>100%</td><td>4</td><td>Minor</td><td>10</td></tr>
<tr><td>Any Flow</td><td>100%</td><td>8</td><td>Significant</td><td>100</td></tr>
<tr><td colspan="4">Design MTBF (Weighted Average)</td><td><b>100</b></td></tr>
<tr><td>Notes</td><td colspan="5">System Proposed Acceptable for this Failure Mode</td></tr>
</table>

4.0 EQUIPMENT CONTROL

4.1 Modes of Control

Various modes of equipment control will be provided throughout wastewater facilities. It is expected that all controlled equipment will utilize one of the four following sets of control modes, depending on the specific control and associated process requirements.

- **PLC Only** – The equipment is always controlled via the PLC, although may be switched between *Manual* and *Auto* modes via the HMI.
- **Local / Remote** – A *Local/Remote* switch will be provided, and in *Remote* mode the equipment is controlled via the PLC, but in *Local* mode, local manual control is provided to override PLC control.
- **Hand/Off/Remote** - A *Hand/Off/Remote* switch will be provided. In *Remote* mode the equipment is controlled via the PLC system. In *Hand* mode, the PLC control will be disabled and the equipment will run continuously.
- **Hand/Off/Auto -** A *Hand/Off/Auto* switch will be provided, with the *Auto* mode providing automatic equipment control via a controller other than the overall plant PLC system.

The characteristics associated with each set of control modes is described in detail in the following tables. It should be noted that while the use of *Hand/Off/Auto* and *Computer/Off/Hand* switches have in the past been utilized to switch between PLC and local control, these control mode designations are not recommended as they can conflict between the software *Auto/Manual* modes typically provided on PLC/HMI systems. It is therefore proposed that the *Remote* designation should be utilized to indicate that the control is via the PLC control system, but not necessarily automatic control. It should be noted that the location of the local controls may be at the equipment itself, the Motor Control Center, or another local control panel.

Table 4-1 : Modes of Control – PLC Only

Field Mode	HMI Mode	Description	Notes
N/A	Manual	Equipment is controlled by the PLC as manually directed by the operator via the HMI.	
	Auto	Equipment is controlled by the PLC in an automatic mode of operation.	

Table 4-2 : Modes of Control – Local / Remote

Field Mode	HMI Mode	Description	Notes
Local	N/A	Equipment is being controlled locally via the local controls. Typically implemented via a Local/Remote or Hand/Off/Auto switch. Local controls could include Start/Stop or Open/Close, etc.	
Remote	Manual	Equipment is controlled by the PLC as manually directed by the operator via the HMI.	
	Auto	Equipment is controlled by the PLC in an automatic mode of operation.	

Note: Where required for clarification, the Manual mode and Auto mode may be referred to as Remote-Manual and Remote-Auto.

Table 4-3 : Modes of Control – Hand / Off / Remote

Field Mode	HMI Mode	Description	Notes
Hand	N/A	Equipment is locally forced to run manual Typically implemented via a Hand/Off/Remote switch.	
Off	N/A	Equipment is locally forced off.	
Remote	Manual	Equipment is controlled by the PLC as manually directed by the operator via the HMI.	
	Auto	Equipment is controlled by the PLC in an automatic mode of operation.	

Note: *Where required for clarification, the Manual mode and Auto mode may be referred to as Remote-Manual and Remote-Auto.*

Table 4-4 : Modes of Control – Hand/Off/Auto

Field Mode	HMI Mode	Description	Notes
Hand	N/A	Equipment is locally forced to run manually.	Equipment may be monitored, but not controlled by the PLC.
Off		Equipment is locally forced to be off.	
Auto		Equipment is controlled by a local (non-PLC) controller, such as an ultrasonic level controller.	

4.2 Local Control Requirements

4.2.1 General

Local control is required for certain equipment to facilitate one of the following functions:

- Allow for operation of the process in the event of failure of the automatic control system.
- Allow for maintenance of the equipment.
- Safety

A typical minimum requirement for local manual control is to provide the ability to start the equipment without the PLC. However, this is not an absolute requirement and would not be provided in instances where a complex piece of equipment requires significant control logic for safe operation. For example, it is expected that operation of a centrifuge would only be permitted with the PLC controlling the equipment and monitoring the appropriate interlocks.

The level of local control and local indication provided is to be the minimum required for basic operation of the equipment. Local equipment monitoring such as pilot lights, would be limited. For example, equipment failed pilot lights will typically not be provided. In addition, equipment interlocking would not be provided, whether by relay logic or other backup systems, except for safety interlocks and other critical interlocks that are required to protect against significant equipment damage.

The appropriate location for installation of local controls is open to some debate. At the time of the existing DCS installation at the three wastewater facilities, it was common to install local controls at a Field Device Panel in the area control room, and a lock-off-stop (LOS) pushbutton at the equipment. Additional local controls were installed adjacent to the equipment in some special cases. Electrical motor disconnect switches located adjacent to the motor were not typically provided.

The primary issue with the existing local control installation approach is the expense of installing and wiring of the Field Device panels. In addition, the installation of lock-off-stop switches is no longer recommended, as part of good practice, as they can imply equipment lock-off capability. Equipment lockout may only be performed by interrupting the source of power, not the control circuit, and thus locking off a LOS switch is not acceptable by current codes.

A proposed requirement is to generally provide, at minimum, a method for personnel to turn off motorized equipment from a location near to the motor. In the past, this was provided through the use of a Lock-Off-Stop pushbutton adjacent to the equipment, however this could be provided by a local disconnect switch, a H/O/R switch, or an *Off* pushbutton. Where a control panel is within the vicinity of the equipment (typically line-of-sight), the control panel may be utilized for containing the local controls.

Area control panels, known currently as Field Device Panels, with local controls and hardwired interlocking will no longer be installed as a general standard.

4.2.2 Motor Disconnect Switches

Motor disconnect switches provide for electrical disconnection of power to the motor. They can either be integrated as part of the motor control center starter or be a local switch at the motor. Certain types of equipment, such as air conditioning equipment, require the use of a local disconnect to meet code requirements. While motor disconnect switches are technically part of the electrical discipline, rather than the automation discipline, the presence of local disconnect switches closely relates to control system requirements.

As discussed in Section 4.2.1, it is proposed to provide a means to stop all motors locally at the motor. The potential application of local motor disconnect switches as an alternate to controls located near the equipment, has numerous related issues to consider. The primary motivation to utilizing local disconnect switches is that it allows maintenance personnel to isolate equipment for maintenance without walking to the electrical room and performing the associated checks to ensure that the correct piece of equipment is isolated. It is typical that local motor disconnects are provided in industrial facilities where operations and mechanical maintenance personnel are not permitted access to the electrical room. Historically, it was the practice within the wastewater treatment facilities that operations and maintenance personnel were allowed to lock-out equipment within the electrical rooms, however electricians must now lock out MCC starters where the switching arc flash hazard is not low (above Category 0). If the local disconnect switches would have a lower switching arc flash rating, which can be switched by non electrical personnel, this would be beneficial to maintenance personnel. While it would typically be expected that arc flash switches associated with smaller motors would have low arc flash ratings, this cannot be assured without performing a full arc flash hazard analysis.

The principle disadvantages of local disconnect switches are that they have an additional cost, which can be significant for larger sizes, require special precautions with VFDs, may have issues associated with the SCCR, and may not be suitable for a corrosive environment. An additional issue that must be considered is appropriate HMI indication of the motor state when the disconnect is pulled. Appropriate indication can be provided by an auxiliary contact, wired to I/O, however this will require additional control wiring. An alternative that is presented with intelligent MCCs is to utilize logic based upon motor current monitoring, to determine appropriate motor run status. This is deemed to be a viable solution, with the caveat that the position of the disconnect switch cannot be detected with the contactor disengaged. In summary, motor disconnects are deemed to be an appropriate solution for certain cases.

An area of caution is that non-fused disconnect switches must not be applied above their rated short-circuit current withstand rating. Disconnect switches have ratings as low as 5kA, although 10kA rated switches are available. To achieve higher short-circuit current ratings, the installation of fuses is required to reduce the potential energy associated with a short circuit. As the City's standard is to utilize circuit breakers throughout the facility, installation of fuses into the circuit is not desirable.

For small motors, in many cases the length of motor cables will often reduce short circuit currents below 10 kA. For example, 10m of 12 AWG cable will reduce a short circuit current of 50kA at the source to below 10 kA at the load. Thus, it is expected that the short circuit current for small motor disconnects will typically be within the 10 kA ratings, however this must be verified at design time.

4.2.3 General Guidelines

General guidelines for the location of local controls are as follows:

- Motor Drive Equipment – Single Speed
  - Small motors (< 50 HP), continuous operation
    - Install a Hand-Off-Remote (H/O/R) switch at the MCC/Starter
    - Install a local disconnect switch at the motor, but ensure the disconnect SCCR is appropriate.
  - Small motors (< 50 HP), standby operation
    - Install a Hand-Off-Remote (H/O/R) switch at the MCC/Starter
    - Install a local disconnect switch at the motor with auxiliary contact wired to provide indication if the motor is not ready. Ensure the disconnect SCCR is appropriate.
  - Small motors (< 50 HP) with frequent disconnect maintenance requirements (weekly or more).
    - Install a local disconnect switch with an auxiliary contact interlocked to the control circuit. Ensure the disconnect SCCR is appropriate.
    - Install local controls (L/R or H/O/R) adjacent to the equipment to allow personnel to stop and start the motor.

  - Medium size and larger motors (>= 50 HP)
    - Install a Local/Remote (L/R) and Start/Stop station at the equipment.
- Motor Driven Equipment - VFD Drive
  - If the VFD is located in the electrical room and the equipment has normal maintenance requirements:
    - Install a H/O/R switch at the equipment.
  - If the VFD is located in the electrical room, and the equipment has frequent disconnect maintenance requirements (weekly or more) and is < 50 HP and SCCR < 10kA and is not in a corrosive location.
    - Install a local disconnect switch with an auxiliary contact interlocked to the VFD control circuit.
    - Install local controls (L/R with Start/Stop or H/O/R) adjacent to the equipment. (See Note 1)
  - If the VFD is located near to the equipment
    - Install a local disconnect switch for the VFD.
    - Local / Remote and Start / Stop or H/O/R switches at the VFD.
- Valve Actuators – Large, Electric
  - Provide *Local / Remote* switch and local controls integrated as part of the actuator.
- Valve Actuators – Large, Pneumatic, On/Off
  - If the fail-safe state is not acceptable for temporary plant operation:
    - Provide local controls consisting of a *Local / Remote* switch and *Open / Close* pushbuttons. These could be next to the valve or at the PLC panel.
  - If the fail-safe state is acceptable for temporary plant operation, then no local controls are required.
  - Note that the capability to utilize and monitor local controls may be limited in some cases if the valve is controlled from certain fieldbus networks.
  - Provide valve actuators with a mechanical position indication for all valves.
- Valve Actuators – Pneumatic, Modulating
  - If the fail-safe state is not acceptable for temporary plant operation:
    - Provide a handwheel for local manual operation, unless process hazard analysis dictates additional requirements.
- Additional Guidelines
  - If the equipment is subject to potential flooding and must remain operational

    - Consider eliminating the local controls at the motor or relocating to a higher elevation.

- For equipment with significant local operational requirements (e.g. bar screens):

    - Provide a *Local / Remote* switch located at the equipment along with other associated controls as required.

- For equipment with moderate safety hazards

    - Prove an *Emergency Stop* Switch adjacent to the equipment. Provide a *Local / Remote* switch and *Start / Stop* pushbuttons at the MCC or adjacent to the equipment. See Notes 3 & 4

Notes:

1. *For motors > 50 HP, momentary Start / Stop provided to ensure motor does not restart after brief power interruption, as is possible if a Hand position is provided.*
2. *Use of Lock-Off-Stop switches will not be permitted as they imply lock-off capability for the equipment, but are not suitable for use as a disconnecting means. Existing Lock-Off-Stop switches can be maintained, provided that no significant modifications are made to the motor control circuit.*
3. *Additional safety controls may be required for equipment with safety requirements. An emergency-stop switch is considered to be a minimum.*
4. *Where an Emergency Stop pushbutton is provided together with local control, the equipment shall utilize a Local / Remote set of control modes, with separate Start and Stop pushbuttons. Equipment shall not restart automatically upon the Emergency Stop pushbutton being released, but rather require a separate restart action from either a local Start pushbutton or a start or reset action from the HMI.*

5.0 MOTOR CONTROL

5.1 Motor Control Automation Styles

Three configuration categories of Motor Control Center (MCC) automation are available. The first is traditional control, where the motor starters are hard wired to the control system. This is typical of existing MCCs at the City of Winnipeg wastewater treatment facilities. The advantage of this configuration is that it is well proven and understood by City electricians and instrumentation personnel. It also has the lowest cost of components, but not necessarily the lowest installed cost. The primary disadvantage of the traditional MCC is the extent of individual control wires required for full control and PLC monitoring.

The second category of MCC automation configuration is integrated control, where either PLC or PLC/DCS remote I/O is integrated into MCC cabinets. The motor starter buckets are typically pre-wired at the factory with pluggable connectors or loose leads, to minimize on-site wiring time. This configuration is usually has a reasonable installed cost, and well understood by City electricians and instrumentation personnel, as it functionally is very similar to a traditional hardwired MCC. However, it has a few potential disadvantages. The first is that pluggable connectors can be a potential source of failures and maintenance headaches. This can be overcome by wiring leads to terminals, at the expense of a slightly higher site installation cost. The second disadvantage is that space is required in the MCC for control components such as a PLC or remote I/O.

The third category of MCC automation is intelligent MCCs. Intelligent MCCs utilize “smart” controls within the motor starter bucket and network wiring between motor starters and the overall control system. There are numerous networks being offered by the various MCC manufacturers, but the four most common networks are Modbus TCP over Ethernet, Ethernet/IP, PROFIBUS and DeviceNet. The primary advantage of this system is the elimination of most field device control wiring, which can significantly reduce installation time, and potentially simplify maintenance. In addition, additional diagnostic information is available remotely over the network, which can aid in motor monitoring and maintenance. For example, intelligent MCCs can typically provide an ammeter reading without an electrician opening the MCC bucket door. The cost of intelligent MCC components is higher, but prices have been dropping. Given current trends, it is expected that the installed cost of an intelligent MCC will be equal to or less than a traditional MCC in 2013. While, a disadvantage is that many City electrical and instrumentation personnel are not familiar with the technology, the City's first intelligent MCC will be installed as part of the MacLean Water Pumping Station Electrical Upgrades project in the winter of 2012 and the City has decided to install an intelligent MCC, with networked control, in the NEWPCC Main Building as part of the Raw Sewage Pump Upgrade project. Thus, it is expected that the City maintenance personnel will become more familiar with the technology in the near future.

A fourth category of MCC automation is a combination of an intelligent MCC with traditional hardwired control. Under this hybrid approach, the intelligent MCC network is utilized to communicate motor starter status, diagnostics and alarm feedback to the control system while the control of the motor is via hardwired control. It is deemed that this type of control is appropriate for certain simple application, which may not be controlled by a PLC, such as a sump pump. However, hardwired control from a PLC with networked monitoring is not typically recommended as it is very difficult to make appropriate control logic decisions on control, if no monitoring inputs are active in the event of network failure. Thus, it would not be uncommon to have inadvertent results due to a network failure, eliminating the benefit of the PLC-based hardwired control.

5.2 Reliability Analysis

The reliability of intelligent MCCs compared with hardwired MCCs is not well documented. MCC vendors are advertizing that intelligent MCCs promote plant reliability, however in many cases the vendors are referring to the benefits of additional diagnostic information, which can aid in plant pre-emptive maintenance. Existing, unbiased, documentation on the subject of intelligent MCC reliability is minimal. To bring some clarity to this issue, the reliability was calculated for two simple MCCs, one networked and the other hardwired, using analysis based upon IEEE 493. An overview of the analysis, including the assumed failures per year, and associated downtime are presented in Table 5-1 and Table 5-2.

The analysis is based upon numerous assumptions regarding the number of failures per year, and the hours of downtime per failure. The values utilized are shown in Table 5-1 and Table 5-2. While any inaccuracies in the values will affect the final results, it is fairly typical in this type of analysis that individual value differences of plus or minus 100% in many cases make only minor differences on the final result. For example, if the MCC network switch is assumed to fail at a rate of 0.04 (1 in 25 years) rather than 0.02 (1 in 50 years), the final downtime per year is only increased from 1.8398 to 1.9198 hours per year (4.8 minutes per year).

Table 5-1 : Calculated Reliability Motor Starter with Hardwired Control

Component	Failures / year	Hours of downtime per failure	Downtime / year	Notes
MCC Power Supply	3.6000	0.3	1.0800	
Main Breaker	0.0035	8	0.0280	
Bus	0.0003	40	0.0136	
Motor Circuit Protector	0.0050	8	0.0400	IEEE 493-1997 App A, Table 2
Contactor	0.0139	8	0.1112	IEEE 493-1997 App A, Table 2
Electronic Overload	0.0300	8	0.2400	
Wiring to MCC Terminals	0.0010	4	0.0040	
Wiring to Control Panel Terminals	0.0010	10	0.0100	Assume 30m
Wiring to PLC	0.0010	4	0.0040	
PLC I/O Module	0.0400	4	0.1600	At minimum 1 DI + 1 DO module
PLC Processor	0.0300	4	0.1200	
Total	**3.7257**	**0.49**	**1.8108**	

Table 5-2 : Calculated Reliability of a Motor Starter with Intelligent Control

Component	Failures / year	Hours of downtime per failure	Downtime / year	Notes
MCC Power Supply	3.6000	0.3	1.0800	
Main Breaker	0.0035	8	0.0280	
Bus	0.0003	40	0.0136	
Motor Circuit Protector	0.0050	8	0.0400	IEEE 493-1997 App A, Table 2
Contactor	0.0139	8	0.1112	IEEE 493-1997 App A, Table 2
Intelligent Overload	0.0300	8	0.2400	
Network Wiring to Switch	0.0010	12	0.0120	
MCC Network Switch	0.0200	4	0.0800	Assume industrial-grade
Network Switch Power Supply	0.0100	4	0.0400	assume redundant
Networking Maintenance Error	0.0500	0.5	0.0250	
Network Wiring to PLC	0.0010	10	0.0100	
PLC Comm. Module	0.0100	4	0.0400	
PLC Processor	0.0300	4	0.1200	
Total	**3.7747**	**0.49**	**1.8398**	

It can be seen from the analysis that the total downtime per year for a motor starter is 1.8108 hours for the hardwired starter compared to 1.8398 for the intelligent motor starter. This difference is insignificant, and it should be noted that the other factors, such as the electrical power supply, have a much greater factor on the motor availability than the control interface. However, the analysis presented in the two previous tables only compares one starter on each MCC. For certain failure modes with the intelligent MCC, the entire MCC could potentially be out of service. A calculation of the additional common downtime for all motors on an intelligent MCC is presented in Table 5-3. On average, approximately 20 minutes of additional total MCC downtime per year, can be expected to be attributed to common networking failures, with an average downtime of 2.14 hours. This can be mitigated to an extent by splitting the wiring of multiple motors on the same process between two intelligent MCC systems to improve the available of the motors to the overall process.

Table 5-3 : Calculated Additional Common Downtime of Intelligent MCC

Component	Failures / year	Hours of downtime per failure	Downtime / year	Notes
MCC Network Switch	0.0200	4	0.0800	Assume industrial-grade
Network Switch Power Supply	0.0100	4	0.0400	assume redundant
Networking Maintenance Error	0.0500	0.5	0.0250	
Network Wiring to PLC	0.0010	10	0.0100	
PLC Comm. Module	0.0100	4	0.0400	
Total	**0.0910**	**2.14**	**0.1950**	

While the intelligent MCC has slightly lower reliability scores, the calculated additional downtime is relatively insignificant in the overall system, provided that the process configuration and motor power supply is set up in a manner that a single overall MCC failure can be managed and is acceptable for short term emergency operations.

5.3 Recommendations

It is recommended that intelligent MCCs be generally utilized for new MCCs due the reduced wiring and additional diagnostic information available. It is expected that the total installed cost of an intelligent MCC will not be higher than a hardwired MCC. For specific applications where small MCCs are utilized in non-critical applications, the use of a non-intelligent MCC may be acceptable. It should also be noted that for certain applications, with very high reliability requirements, the overall reliability of a networked installation may not be sufficient to meet the specified reliability requirements, and in this case, the use of a hardwired MCC would be appropriate. The use of non-intelligent MCCs must be by City approval.

Specific guidelines for ensuring a reliable intelligent MCC installation are as follows:

- Utilize Ethernet-based networking for intelligent MCCs.
- Utilize reliable-industrial grade network switches and other networking components.
- Provide a redundant power supply to all networking switches.
- Review the network reliability between the MCC and the PLC and provide redundancy if required.
- For each motor, ensure that the fallback setting for motor operation on a network failure is correct. Typically, each motor can be configured to continue running on a network failure, or to stop. During network failure fallback, any local controls would remain active.
- Ensure that the process equipment power supply is configured in a manner to fail acceptably in the event of a MCC communication failure. If upon review, it is determined that the common failure of the MCC upon network failure is unacceptable, separate the motor starter communications into physical groups with separate switches in a manner to provide the required availability. Detailed reliability analysis may be required for some cases.

6.0 INSTRUMENTATION

6.1 Instrument Selection

Instrumentation consists of the devices that measure and monitor the process variables, as well as devices that control the process, such as valves. The selection of appropriate instrumentation for the process is a critical component of a successful automation system. Instrumentation should be selected with the following criteria in mind:

- Accuracy – The accuracy of the transmitter should be better than the application requirements.
- Reliability – The failure rate of the instruments should be very low, or set up in a manner to avoid a significant effect on the process upon failure.
- Environmental considerations – The instruments must be suitable for the installed environment, which in some cases could be corrosive or hazardous.
- Training – Training for instruments must be considered, and the number of instrument manufacturers should be minimized to reduce training requirements.
- Maintenance Requirements – The maintenance requirements of instruments must be considered, and instruments with reduced maintenance requirements are preferable. Spare parts and replacement instruments should also be considered.

6.1.1 Classes of Measurement Instruments

For the purpose of this document, instruments are divided into four major classes:

1. *Discrete Hardwired Switches*, which include on-off devices such as level switches, pressure switches etc.
2. *Analog Transmitters*, which may have analog or digital internals, but output an analog output signal such as 4-20mA. A common example is a temperature transmitter.
3. *Discrete Networked Switches*, which are basic on-off devices, but communicate over a network such as AS-i, rather than dedicated hardwiring.
4. *Smart Networked Transmitters*, which measure a process variable and transmit a signal over a fieldbus network, such as Modbus, PROFIBUS, or DeviceNet.

6.1.2 Discrete vs. Transmitter Selection

The selection of discrete instruments compared with transmitters (either networked or not) should be considered in all cases. There are many cases where historically a switch was selected to provide alarming or interlock functionality, based upon process requirements. The primary advantages of switches compared to transmitters are simplicity and cost. In some cases transmitters are required as part of the automation scheme, such as PID control. However, transmitters with logical setpoints can have the following advantages compared to switches for basic interlocking and alarming functionality, as described below:

- The alarm or interlock setpoint can easily be modified or changed without recalibration of the instrument.
- The deadband and hysteresis of the setpoint can be defined in logic, rather than being limited to the capability of the switch.
- The transmitter provides a signal that can be monitored, and thus basic verification of operation is continuous. The functionality of a hardwired switch can only be verified with testing.
- In some cases, setting up a test of a switch can be an onerous scenario, and longer transmitter calibration intervals may be preferable to shorter switch proof intervals.

Given the advantages of transmitters, it is recommended that they be considered for essential interlocking and alarming applications, but with some sensitivity to the additional costs. General application guidelines are shown in Table 6-1.

Table 6-1 : Guidelines for Selection of Switches vs. Transmitters

Application	Instrument	Notes
Critical and safety applications	Consider Transmitter	Careful review is required. Codes may apply.
HVAC low temperature (Freeze-stat)	switch	Simple cost effective solution requiring hard-wired interlock.
Wet Well Low Level	Transmitter	Redundancy should be provided for control.
Room High Temperature	Transmitter	Can be utilized in control strategy as well.
Pump Low Flow Detection	Switch	Partial testing with pump on/off cycling provided.
	Transmitter	Where there is use as part of process measurement.
Ventilation Low Airflow Detection	Switch	On/off fans Partial testing with fan on/off cycling provided.
	Transmitter	Variable speed fans.
Instrument Air Low Pressure	Transmitter	Continuous indication of operation.

6.1.3 Use of Networked Instruments

Networked instruments are those connected to a fieldbus network to allow for digital communication of process information. While connection to a fieldbus network, such as PROFIBUS or Foundation Fieldbus, is the most common case, the use of Ethernet networks to connect instruments is becoming increasingly common, and is also applicable in the below discussion.

Instruments connected to a fieldbus provide potential savings on installation costs, while allowing for an increased amount of operational and maintenance data to be presented to the automation system. However, hardwired instrumentation is a more straightforward installation, and is well understood by maintenance personnel. Use of a fieldbus connected instrument should generally be utilized in the following scenarios:

- Very high accuracy is needed.
- Instruments are mounted outdoors, where temperature may affect equipment accuracy.
- Instruments are connected to long cable runs
- Where the additional maintenance diagnostic information available will provide significant operational benefit.
- Where more than two variables are transmitted to/from the automation system.
- Where the use of the fieldbus eliminates the use of pulsed output totalizers.
- Where access to the instrument is difficult. In this case, regular maintenance would be more difficult and additional benefit from the maintenance data provided by fieldbus connected smart instruments would be useful.

Despite the above rationale, it is typical that there will be cases and scenarios where the previous rationale is not adequate and a decision must be made based upon other system design characteristics. Other criteria which may need to be considered on a case-by-case basis include:

- Cost and availability of the fieldbus instrument vs. the traditional hardwired instrument,
- Whether or not a fieldbus is already deployed within the process area,
- Reliability analysis, including the availability of parallel processes due to failure of a common fieldbus, and

- Economic evaluation of the fieldbus installation compared to the hardwired installation from an overall installation and maintenance perspective.

6.1.4 Wireless Instruments

Wireless industrial field devices are relatively new, and have not previously been applied within the City's wastewater treatment facilities. The current wireless field devices typically are based upon either the ISA-100 or WirelessHART standard.

The primary motivation for wireless field devices over wired instrumentation is to reduce wiring costs. Given the limited distances within a wastewater treatment application, it is expected that most field devices can be hard-wired with reasonable costs. It should also be noted that wireless communication cannot yet be considered reliable, and thus should not be utilized for control purposes. At this time, it is proposed that wireless devices only be considered in the following applications:

- Instrument wiring would be of significant distance (>100m) or wiring would be difficult due to location or mobility issues, and
- The reliability requirements for the instrument are such that failure of the device communication for a period of a day will not impact the process or operations.

It should be noted that wireless technology will continue to evolve, and a future review of wireless applications and potential reliability improvements would be appropriate.

6.2 Wastewater Instrumentation Guidance

6.2.1 Flow Instrumentation

Proper design of flow instrumentation is required to ensure a reliable flow signal is provided to the control system. Flow instrumentation must be mounted with appropriate upstream and downstream straight length runs to ensure uniform flow at the instrument. Magnetic flowmeters are the instrument of choice for most liquid flows in wastewater treatment plants, however consideration should be given to alternate technologies where requirements dictate. For airflows, preference is given to thermal dispersion based flowmeters due to their reliability and limited maintenance requirements.

Consideration must be given to regulatory or license requirements when selecting flow instrumentation. For example, raw influent and final effluent flow metering are expected to have license requirements regarding accuracy.

For open channel flow, selection of appropriate flow measurement is not necessarily straightforward, but it is recommended that consideration be given to ultrasonic, and area velocity flow meters. It should be noted that the accuracy of open channel flowmeters is typically limited.

Consideration should be given to designing a system with means to verify critical flowmeter measurements. This could be accomplished via redundancy, an alternate flow measurement technology, or periodic draw/fill tests of a given volume. While it is acknowledged that in some cases verification of flow measurement may be cost prohibitive, it should be considered for all critical flow measurements.

6.2.2 Level Instrumentation

Level instruments are required in the wastewater treatment facilities for numerous control, monitoring, and alarming functions.

Where a level instrument is utilized for control, it must, at minimum, be backed up by a secondary high and/or low level switch for alarming and interlocking. Where level control is critical, such as in raw sewage pumping, use of redundant level sensors is recommended.

Ultrasonic level transmitters are typically the instrument of choice in wastewater applications, as they have no physical contact with the medium being measured. Their accuracy is typically better than 2%, however they may have issues in the event that foam is present. In addition, careful consideration should be given to good installation design practice and manufacturer instructions as most issues with ultrasonic installations are due to false echoes from obstructions within the tank or tank walls. The design engineer must include consideration of vessel configuration and transmitter mounting for each design application.

Submersible pressure based level sensors can be considered in certain applications and are a potential instrument to back up an ultrasonic level transmitters. Care must be taken to ensure the sensor is not subjected to turbulence, and a stilling well may be required. In addition, the end of the pressure compensation tube must be kept dry and clean, and at a similar atmospheric pressure as the vessel being measured to avoid error. Alternately, in lieu of pressure compensation tubes, absolute pressure transmitters may be utilized for atmospheric pressure compensation, and may be appropriate in locations where the pressure compensation tube is subject to fouling, or maintenance of desiccants is not desired.

Level switches for water application can either be conductivity based or float switches, such as the Flygt ENM-10, which are commonly utilized for high and low level applications.

6.2.3 Temperature Instrumentation

Temperature transmitters are required for various process monitoring, as well has HVAC applications. Resistance Temperature Detectors (RTDs) are the sensor of choice for most applications as they have a high accuracy, and excellent stability and repeatability. In addition, RTDs are generally not very susceptible to electrical noise.

Temperature elements such as RTDs, must interface with a local transmitter (or signal conditioner) or a local input module that is specific to the specific type of temperature element in use. The transmission of RTD or other low level sensor signals over long distances is not recommended.

6.2.4 Process Analyzers

There are numerous types of process analyzers that can potentially be utilized within a wastewater treatment process. They can include, but are not limited to, suspended solids, turbidity, sludge density, chlorine residual and dissolved oxygen. The application of process analyzers is beyond the scope of this report, however it is recommended that the sensor integration include appropriate failure indication, to avoid erroneous data from being recorded and to advise personnel of service requirements.

6.3 Instrumentation Redundancy

6.3.1 General Guidelines

Where failure of a single instrument has unacceptable consequences, redundancy of the instrumentation may be required. Instrumentation redundancy could be provided by either an identical instrument, or by an alternative instrument technology that provides an acceptable response. For example, it is common to have a level transmitter backed up by a high-level float switch to turn on an alarm.

Guidelines for evaluation when instrumentation redundancy may be required are provided in Table 6-2.

Table 6-2 : General Guideline for Instrumentation Redundancy Requirement

Criteria	Yes	No
Is a six hour unplanned shutdown of the instrument signal, approximately every 10 years acceptable?	Instrument redundancy not necessarily required.	Instrument redundancy or redesign required.
Will failure of the instrument result in unacceptable consequences and is failure difficult to detect	Instrument redundancy or redesign required.	Instrument redundancy not necessarily required.

6.3.2 Instrument Redundancy Reliability Calculations

The reliability of redundant instrumentation can be calculated to provide a quantitative assessment whether the instrumentation system is suitable for to process requirements. The reliability calculations presented in this section are based upon IEEE 493.

Note that for critical and safety systems, the guidelines below are inadequate and a more formal analysis of the complete automation or safety system is required. It is recommended that analysis regarding the reliability of the overall safety system follow the requirements of ISA 84.00.01-2004.

The calculations below can be utilized to calculate the frequency of failures and expected downtime for redundant systems. Note that these calculations only include the instrument reliability, and not that of the cabling, I/O module, or controllers used to process the logic. When assessing redundancy, consideration must also be given to the final control device, which may be less reliable than the measurement instrument. The subsequent calculations utilized the following definitions:

$$MTBF = \text{ Mean Time Between Failures (years)}$$

$$f = \frac{1}{MTBF} = \text{frequency of failures (per year)}$$

$$r = \text{ average downtime per failure (hours)}$$

$$fr = \text{average downtime per year (hours)}$$

Given the MTBF of a single instrument, and the downtime per failure r, which includes the detection, response and repair time, the average downtime per year fr would be equal to:

$$fr = \frac{r}{MTBF}$$

For redundant instrumentation, the combined probability of failure and average downtime are calculated as follows:

$$f_p = \frac{f_1 f_2 (r_1 + r_2)}{8760}$$

$$r_p = \frac{r_1 r_2}{(r_1 + r_2)}$$

Where the redundant instrumentation has equal probabilities of failure and downtime, the equations can be simplified to:

$$f_p = \frac{2{f_1}^2 r_1}{8760}$$

$$r_p = \frac{r_1}{2}$$

It should be noted that the above equations only hold if the failure of one of the two instruments will have no affect on the process and/or the control system can automatically immediately detect the failure of an instrument and switch over to the redundant instrument. If the failure of an instrument requires operator intervention to switch over, then the equations are as follows (assuming identical instruments), assuming that the downtime (time to repair) is much shorter than the *MTBF*:

$$r_o = \text{Time for operator to identify problem \& switch over (hours)}$$

$$f_p = f_1 + \frac{2{f_1}^2 r_1}{8760}$$

$$r_p = \frac{f_1 r_o + \frac{f_1^2 r_1^2}{8760}}{f_1 + \frac{2{f_1}^2 r_1}{8760}} = \frac{8760 r_o + \ f_1 r_1^2}{8760 + 2\, f_1 r_1}$$

$$f_p r_p = \left(f_1 r_o + \frac{f_1^2 r_1^2}{8760} \right)$$

However, typically the downtime (time to repair) is much shorter than the *MTBF*, and thus the equations can be simplified to:

$$f_p \approx f_1$$

$$r_p \approx r_o$$

$$f_p r_p \approx f_1 r_o$$

For example, if we have a redundant wet well level transmitter with a *MTBF* of 20 years, eight hours of downtime to repair, and it takes half an hour to diagnose a problem and switch over to the alternate level transmitter, the average downtime can be calculated as follows:

$$f_1 = \frac{1}{20} = 0.05$$

$$f_p \approx 0.05$$

$$r_p \approx 0.5$$

$$f_p r_p \approx 0.025$$

That is, the combined system would have an average downtime of 0.025 hours (1.5 minutes) per year, but the average downtime of a failure event would be 0.5 hours.

For a triple redundant scheme, where three identical instruments are installed for ultimate redundancy, a voting scheme can be utilized to immediately disable a defective instrument. In this type of scheme, the probability of failure is approximately calculated as follows, provided the repair time is much shorter than the MTBF:

$$f_r \approx f_1^3$$

With triple redundant systems, the average downtime is typically reduced to extremely low levels. Note that the use of triple redundant systems is not expected to be common in a wastewater treatment facility, and would only be applied for safety systems where the consequences of failure are extremely high.

While the above calculations are useful to perform a quantitative assessment of some more complex cases, it is not expected that calculations will be performed for every instrument. The guidelines presented in Table 6-2 can generally be utilized as an informal assessment if redundancy should be considered for an instrument.

6.4 Instrument and Signal Application Guidelines

General guidelines for the application of instrument and associated monitoring are as follows:

- Electric Motors
  - All motors shall generally be monitored for:
    - Motor Running
    - Overload Status
    - Out of Service Status (May be communication failure for intelligent starters)

  - Motors with disconnect switches shall utilize motor current together with the auxiliary contact status to determine running, if not provided with an auxiliary contact input to the PLC.
  - Provide the following for motors over 100 HP:
    - Bearing temperature
    - Winding Temperature
    - Vibration sensor with 4-20 mA output.
    - Current monitoring (May be via intelligent overload)
- Pumps
  - On larger pumps (> 100HP) consider the following (use engineering judgement)
    - Bearing temperature
    - Case temperature (very large pumps)
- Sluice Gates
  - All sluice gates should be monitored with a minimum of open and closed limit switches.
  - Motor actuated large or critical sluice gates should have full diagnostic monitoring, including full position monitoring.
  - Connect motorized actuators via fieldbus network connections.
- Valves
  - Automatic Valves
    - All automatic valves require monitoring of closed and open position.
    - Modulating valves typically require position feedback, except in the case of non-critical valves where the operation can be verified through another process variable.
  - Manual Valves
    - Manual valves utilized for process isolation bypass of significant process equipment and trains should have at minimum a single limit switch for the normal operating state.
    - Valves used for equipment maintenance isolation of a single piece of equipment do not typically need monitoring.

7.0 FIELDBUS NETWORKS

7.1 Overview

Fieldbus is a general term utilized to describe a network that connects devices in the field. There are a significant number of potential fieldbus offerings, and their capabilities vary significantly. While it is expected that some level of standardization on fieldbus networks is appropriate, it is not practical to expect that only a single network will be utilized in a facility. For example, a network that is appropriate for valve and limit switch communication will not be appropriate for communication between remote I/O and PLCs. Fieldbus networks can generally be classified as follows, however there can be significant overlaps between these classifications.

- Ethernet networks (e.g. Ethernet/IP, Modbus TCP, PROFINET)
- Fieldbus Device networks (e.g. DeviceNet, PROFIBUS DP)
- Fieldbus Process networks (e.g. Foundation Fieldbus, PROFIBUS PA)
- Fieldbus Sensor networks (e.g. AS-i)

Note that Ethernet networks have not been traditionally classified as a fieldbus, however current practice is that Ethernet can compete directly with traditional fieldbuses in many applications. Table 7-1 presents typical classifications of fieldbus application for various types of devices and communication. As the applications will not be consistent with a single fieldbus network, it is expected that multiple fieldbus network protocols will be utilized. Still, it would be useful to minimize the number of fieldbus protocols utilized within each classification, ideally to a single protocol.

Table 7-1 : Typical Fieldbus Application Classification

Type of Device	Ethernet	Fieldbus Device Networks	Fieldbus Process Networks	Fieldbus Sensor Networks
Remote I/O	Y	Y		
Motor Control Center	Y	Y		
VFD	Y	Y		
Process Analyzer	Y	Y		
Encoder		Y		
Gas Detection Controllers		Y		
Large Electric Valve Actuator		Y		
Flowmeter		Y	Y	
Modulating Control Valve			Y	
Pressure Transmitter			Y	
Temperature Transmitter			Y	
Level Switch				Y
Limit Switch				Y
On/Off Valve				Y
Pressure Switch				Y
Pushbutton / switch				Y

7.2 Industrial Ethernet Protocols

Industrial Ethernet protocols have traditionally been utilized for communication requiring significant throughput, and are increasingly being applied in many other applications due to the pervasiveness of Ethernet installations, availability of technical personnel who are competent in the design and troubleshooting, and due to the ease of integration with other networks. Ethernet installations are also very cost competitive with other fieldbus networks.

The current Ethernet based networks that would be potential candidates for use at the wastewater facilities are described in the following sections.

7.2.1 Ethernet/IP

Ethernet/IP is a common industrial Ethernet protocol originally developed by Rockwell Automation, and is currently managed by the Open DeviceNet Vendors Association (ODVA). Ethernet/IP is based upon the Common Industrial Protocol (CIP), and treats data and devices as a series of objects.

The largest advantage of Ethernet/IP compared to other industrial Ethernet protocols is also its largest disadvantage. Ethernet/IP uses multicasting UDP packets rather than only point-to-point TCP/IP packets. This allows a single producer of information to send a message once, which can be received by multiple consumers, rather than resending the message to each consumer. However, the network management required to manage Ethernet/IP based systems is typically more complex than for other industrial Ethernet protocols, and can be a significant undertaking for very large Ethernet/IP based networks.

Ethernet/IP has an extensive set of features and capabilities, which are beyond the scope of this document. Selection of Ethernet/IP as a preferred Industrial Ethernet Protocol is dependent upon the selection of the control system vendor. Rockwell Automation is the leader in Ethernet/IP utilization, with support also provided by Omron and Schneider Electric.

7.2.2 Modbus TCP

Modbus TCP is primarily an Ethernet-based implementation of the Modbus protocol. It has essentially the same capabilities as Modbus, except for no logical limitation on the number of devices per network, and higher data transfer rates. Modbus TCP is implemented on top of the TCP/IP protocol, and thus can be routed over enterprise networks. It should also be noted that devices can theoretically be accessed from anywhere, simply by utilizing the IP address of the device, however this is practically limited by the extent of integration of the process network with the enterprise network, and associated security policies that are in place.

The primary advantages of Modbus TCP are that the protocol is well documented, open, and easy to implement, which leads to high levels of adoption by equipment manufacturers. However, the most significant disadvantage is that it is a very simple protocol, and does not have many of the advanced features of Ethernet/IP and PROFINET.

7.2.3 PROFINET

PROFINET is essentially the Ethernet successor to PROFIBUS. It is functionally divided into two perspectives, PROFINET CBA and PROFINET IO. PROFINET CBA is suitable for component based real-time machine-to-machine communication via TCP/IP networks. PROFINET IO is more similar to PROFIBUS DP, and is typically utilized to collect distributed I/O. However, these are not necessarily separate physical networks, but rather an integrated system where a PROFINET IO node can appear as a component within a PROFIBUS CBA system. PROFINET IO communication is configured with the assistance of GSD or General Station Description files, which are provided by instrument and equipment vendors.

PROFINET is unique in that it does not always utilize the TCP/UDP/IP network stack for all traffic. The TCP/IP stack is utilized for “standard data” such as configuration, parameter assignment, and reading diagnostic data. However, real-time data bypasses the TCP/IP stack and is sent over base Ethernet according to the IEEE 802 series of standards. Standard Ethernet switches may be utilized except in isochronous real-time applications such as motion control, where specific PROFINET functionality must be provided by the switch.

PROFINET has an extensive set of features and capabilities, which are beyond the scope of this document. Selection of PROFINET as a preferred Industrial Ethernet Protocol is dependent upon the selection of the control system vendor. Siemens is the leader in PROFINET utilization, with support also provided by ABB and GE. Some other vendors provide some level of PROFINET support, but it is typically limited.

7.3 Fieldbus Device Networks

Fieldbus Device networks are designed to meet the communication needs of higher level devices. They are well suited to collecting I/O and passing on the data to controllers, and communicating to intelligent devices. They are typically not as well suited to connection of process instruments, especially in hazardous locations. In this document, fieldbus I/O networks are differentiated from Ethernet networks, however Ethernet networks are expected to continue to advance into the domain of the non-Ethernet Fieldbus I/O networks.

7.3.1 DeviceNet

DeviceNet is based upon a 4-wire network topology that can be daisy-chained or branched. Branches are permitted to a maximum of 6m, with power included in the network. Up to 62 devices are permitted on a network, which is based upon the CAN (Controller Area Network) technology. DeviceNet is well suited to discrete networks, although it has been applied successfully to modulating control applications as well. The most common application of DeviceNet is MCC and VFD integration. It should be noted that the DeviceNet is not typically rated for hazardous locations.

While some users’ overall experience with DeviceNet has been positive, two items should be noted. The primary disadvantage of DeviceNet is that a new device cannot be configured without taking the whole network out of service. Secondly, it should be noted that while DeviceNet communications are typically advertised as “plug-and-play”, most users experience significant time troubleshooting and configuring the network.

7.3.2 PROFIBUS DP

PROFIBUS DP is based upon a 2-wire RS-485 network with a separate power supply. Up to 126 devices can be connected in one PROFIBUS DP network, however each segment is limited to a maximum of 32 devices. The DP network must be laid out as a daisy-chain linear bus, and bus spurs are not typically allowed. Network communication speeds are dependent upon the length of the installation, and can range from 9.6 kbit/s to 12 mbit/s.

PROFIBUS communication is configured with the assistance of GSD or General Station Description files, which are provided by instrument and equipment vendors. It should be noted that some PROFIBUS DP benefits are negated if the PROFIBUS DP networks are not integrated directly into the control system. For example, use of network gateways negates some of the advantages of the PROFIBUS DP Network.

While historically PROFIBUS adoption has been faster in Europe than in North America, the availability of PROFIBUS devices in North America is increasing.

7.3.3 Modbus

Modbus is a serial communication protocol which typically communicates over an RS-232 or RS-485 physical medium. It was originally developed in 1979 and is the most common protocol in use to connect industrial devices. While an ASCII version is available, the Modbus RTU version is typically utilized, where communication is based upon binary data transmission.

A Modbus RTU network is typically based upon a 2-wire RS-485 network with a separate power supply. Up to 127 devices can be connected in one Modbus network, however RS-485 limitations limit each segment to a maximum of 32 devices. The RS-485 network must be laid out as a daisy-chain linear bus, and bus spurs are not typically allowed. Network communication speeds are dependent upon the length of the installation, and typically range from 2.4 kbit/s to 56 kbit/s.

The Modbus communication protocol has been widely utilized due to its simplicity. It is master-slave based, and simply polls registers and bits from the slaves.

7.4 Fieldbus Process Networks

Fieldbus process networks are designed to integrate process instrumentation such as pressure and level transmitters, as well as control valves. They are well suited to control loops and can typically be utilized in hazardous locations. Fieldbus process networks also typically allow for spurs off trunk lines, rather than daisy-chain style installation, which aids in physical deployment and maintenance.

7.4.1 Foundation Fieldbus

Foundation Fieldbus is a process fieldbus network that is typically utilized to integrate instrumentation and valves on a single network. Foundation Fieldbus segments are limited to 16 devices per segment. Base field segments are typically based upon the H1 specification, which allows for 31.25 kbit/s communication with a maximum range of 1900m. However, it should be noted that while spurs are allowed, the length of the spurs can be significantly limited with multiple devices on the network. Higher level H2 and H3 segments can be utilized to collect multiple H1 segments, and have 1.0 Mbps and 2.5 Mbps communication respectively. It should also be noted that Foundation Fieldbus does support installations in hazardous rated locations.

Foundation Fieldbus communication is configured with the assistance of DD or Device Description files, which are provided by instrument and equipment vendors. It should be noted that some Foundation Fieldbus’ benefits are negated if the Foundation Fieldbus networks are not integrated directly into the control system. For example, use of network gateways negates some of the advantages of the Foundation Fieldbus Network.

It should be noted that from a physical wiring perspective, Foundation Fieldbus is identical to PROFIBUS PA, however Foundation Fieldbus uses cyclic data transmission rather than polling as utilized in PROFIBUS.

7.4.2 PROFIBUS PA

PROFIBUS PA is based upon a Manchester Bus Powered physical network to ease installation requirements. Other network layers are the same as PROFIBUS DP, and thus PROFIBUS masters do not differentiate between PROFIBUS DP and PROFIBUS PA communications in terms of functionality. The network communicates at a fixed speed of 31.25 kbit/s. Typically a PROFIBUS PA segment is branched from a PROFIBUS DP segment via a DP/PA Coupler, and the PA network is more flexible than the DP network in that tees and spurs are allowed. It is also possible to install a PROFIBUS PA system in a hazardous rated location.

PROFIBUS communication is configured with the assistance of GSD or General Station Description files, which are provided by instrument and equipment vendors. It should be noted that some PROFIBUS benefits are negated if the PROFIBUS networks are not integrated directly into the control system. For example, use of network gateways requires the additional configuration of the network gateway, often by a separate software package.

7.5 Fieldbus Sensor Networks

Fieldbus sensor networks are typically utilized to transmit small bits of information between sensors and controllers, typically at a high data rate. The networks are typically designed to be simple, such that the communication interface can be integrated into small sensors and switches. The only sensor fieldbus that has significant industrial adoption in North America, which would be appropriate in a wastewater application, is AS-i bus.

7.5.1 AS-i Bus

AS-i bus is a simple bus utilized for sensor, actuators, and simple human interface devices such as switches and indicator lights. It does not directly compare to most other fieldbuses in that it is intentionally a simple architecture, and does not support more advanced general communications and diagnostic capabilities provided by other fieldbuses. AS-i is not targeted at integration of more complex field devices such as a VFDs, or analog type instruments, but rather simple devices with discrete signals of up to four inputs and four outputs. For example, a valve with open/close control and open/close status monitoring would be ideal for AS-i integration. The advantage of AS-i over more complex fieldbuses is that it is significantly simpler and less expensive to implement, and has a high performance within its discrete domain. AS-i is quite popular in Europe and is increasing in popularity in North America.

AS-i utilizes unshielded 2-wire cable to communicate with a maximum of 63 slave nodes. Power is delivered to the end device over the 2-wire network, which can extend up to 100m without repeaters and 300m with repeaters.

7.6 Other Fieldbus Networks

7.6.1 HART

HART is a field communication protocol, where digital communication is superimposed over an industry standard 4-20 mA analog signal. While not strictly a fieldbus network, it provides some of the maintenance benefits associated with diagnostic information, while retaining the traditional physical wiring interface. The advantages of HART include familiarity on the part of maintenance personnel, interoperability with legacy 4-20mA equipment, and digital communication of various instrument configuration parameters and diagnostic data. As it is not a bus technology, it is typically wired with dedicated wires to each instrument rather than as a bus or network. There is also a multi-drop version of HART, where it can act like a bus with sensors, but this configuration is not as well supported or utilized.

7.6.2 Networks Not Discussed

There are also many other fieldbus networks, which are deemed not suitable for potential use at the wastewater treatment facilities. A list of some of these networks, and primary motivation for not including them in the discussion is presented in Table 7-2.

Table 7-2 : Other Fieldbus Networks Not Discussed

Fieldbus Network	Classification	Primary Disadvantage
CANOpen	Fieldbus Device	Not typically applied within industrial process industries. Note that DeviceNet and Ethernet/IP are based upon CAN models.
CompoNET	Fieldbus Sensor	Specialized bit-level high-speed network that is not commonly utilized in industrial environments.
ControlNET	Fieldbus Device	Utilizes coax cables and is generally viewed as nearing obsolescence.
EtherCAT	Ethernet	Currently poor adoption in North America.
Foundation Fieldbus-HSE	Ethernet	An Ethernet version of Foundation Fieldbus, typically only applicable within Emerson systems.
Interbus	Fieldbus Device	Poor adoption in North America.
Lonworks	Fieldbus Device	Primary utilized for building automation.

Note: The above table is not exhaustive, as many other fieldbus protocols have been developed.

7.7 Fieldbus Selection Guidance

The selection of appropriate fieldbus networks will be a significant contributor to the overall success of the automation system. However, it is expected that more than one fieldbus network will be utilized as part of the future automation systems. As discussed in Section 7.1, it is expected that various fieldbus networks will be required to meet the needs of the instrumentation requirements within the facility. Specific guidance for each application is summarized below.

For Ethernet networks, it is recommended that selection of a preferred protocol be made as part of the selection of a control system vendor. However, it is recommended that support for integration of Modbus TCP networks should be included, due to the general support for Modbus TCP by many vendors.

It is recommended that the use of non-Ethernet Fieldbus Device networks be minimized during the plant design process, where the application can be served by an Ethernet network. It is believed that Ethernet based networks will provide a longer useful life than other Fieldbus networks, and in the event of a protocol change, physical wiring would not typically require replacement. Where a Fieldbus I/O network such as DeviceNet or PROFIBUS DP is required, integration would be on a case-by-case basis.

The selection and use of Fieldbus Process Networks is highly dependent upon the selection of the control system vendor, and the type and layout of the required equipment. It is recommended to utilize a Fieldbus Process network, such as Foundation Fieldbus or PROFIBUS PA, where the use of smart instruments is required, or the fieldbus provides significant cable installation savings. Refer to Section 6.1.3 for further discussion.

The requirement for Fieldbus Sensor Networks, such as AS-i, is not currently clear. A review of the existing City facilities would be unlikely to yield many applications with significant benefit for the use of a sensor interface. In many cases, use of remote I/O nodes located close to the installation would be expected to provide the most cost effective installation. However, if there is an installation proposed where there are a concentrated number of discrete sensors and on/off valves, it is recommended that a Fieldbus Sensor Network be considered for potential cost savings.

7.8 Fieldbus Application Guidance

Where fieldbuses are utilized, it is recommended that a reliability review be performed to ensure that a single bus failure cannot cause the performance of the plant to degrade to an unacceptable level. For critical processes, it is expected that a separate fieldbus segment will be required for each process train. For some processes with a more moderate reliability requirement, a dedicated fieldbus for each process train may not be required, but a reduction in the number of nodes on each bus may be required to reduce the extent of a failure to an acceptable level. It is recommended that the reliability of each fieldbus segment be reviewed at design time, to ensure that failure modes are such that the extent of impact on the process is kept at acceptable levels.

8.0 ENVIRONMENTAL AND HAZARDOUS CLASSIFICATION

8.1 Environmental Considerations

8.1.1 Corrosive Gasses

Wastewater treatment facilities have various environmental considerations that must be accounted for in the automation system design. The first is the presence of corrosive gasses including hydrogen sulphide (H_2S), which are corrosive to electrical and automation equipment.

It is recommended that ISA 71.04-1985, *Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants*, be referenced as a guide regarding corrosion level classification. There are four corrosion levels identified in the ISA standard and the specific level for an area is typically assigned based upon the corrosion rate of a sample copper coupon. The classification levels are presented in Table 8-1.

Table 8-1 : Corrosion Classification Levels

Level	Description	Recommended Guideline
G1 Mild	The environment is sufficiently well controlled that corrosion is not a factor in determining equipment reliability.	No restriction regarding installation of controls.
G2 Moderate	The effects of corrosion are measurable and may be a factor in determining equipment reliability.	NEMA 4 or 4X enclosures are required to minimize the effect of corrosive gases.
G3 Harsh	There is a high probability that a corrosive attack will occur.	NEMA 4X enclosures are required for non-critical controls. Avoid critical controls in this area, but if deemed to be required, utilize special precautions. See note.
GX Severe	The corrosion in this area will be severe and it is expected that only specifically designed equipment will survive.	Installation of controls not permitted unless mandatory. If required, special precautions must be taken. See note.

Note: *The design of special precautions to protect control equipment in highly corrosive locations is beyond the scope of this document, but an example would be the utilization of an enclosure pressurization system equipped with a media filter.*

As a reference, corrosion monitoring coupons were installed in the NEWPCC Main Building between May and June of 2010 as part of the Raw Sewage Pump Upgrades project. The coupons in numerous areas indicated a G3 environment, and the coupon installed on the main floor in the drywell area indicated a GX environment. Thus, there is significant corrosion potential at the NEWPCC facility. It should be noted that the NEWPCC Main Building is located just east of the open primary clarifier tanks, and it is believed that these primary clarifiers are a significant source of the corrosive gasses that were observed.

For new and significantly upgraded process areas, it may not always be possible to utilize testing to classify corrosion levels. In these cases, appropriate estimates based upon similar installations must be utilized. These estimates must look at the potential sources for corrosive gases, levels of ventilation, and the quality of the ventilation supply air.

It is recommended that the electrical rooms and control rooms be provided with appropriate ventilation and media filtration to achieve a G1 corrosion classification. It is also recommended that sufficient ventilation be provided to process areas to minimize corrosion potential. However, it is expected that some control system equipment will be located in areas with corrosion levels higher than G1, and appropriate design precautions will therefore need to be implemented as part of the system design.

Acceptance testing of the completed electrical room installations should utilize corrosion coupon testing, to ensure that the environment meets the specified G1 corrosion classification.

8.1.2 General Design Requirements

Automation equipment must be suitable for the location within which it is installed. Specific requirements include:

- Where mounted outdoors, equipment must be rated to withstand temperatures within the range of -40℃ to 40℃.
- Minimum enclosure requirement for electrical rooms – NEMA 1.
- Minimum enclosure requirement for mechanical rooms and light process areas – NEMA 12.
- Minimum enclosure requirement for general process areas – NEMA 4.
- Avoid locating instruments and automation equipment in areas of potential submergence.
- Equipment mounted in field process areas where corrosive gases are present must be selected to resist corrosion. Where available, stainless steel NEMA 4X enclosures should be selected. Copper-free aluminum enclosures are also appropriate.

- It is preferred if control panels containing PLCs and I/O are located outside of the corrosive process locations. However, if the reduced wiring associated with a local control panel in the corrosive location provides significant potential cost savings, it is recommended that enclosure pressurization with clean air be considered as an option. The pressurization system could potentially utilize a local media filter pressurization system for the enclosure.

8.2 Hazardous Gas Detection

8.2.1 Combustible Gas Detection

Combustible gas detection is recommended to ensure that personnel are warned of any combustible atmospheres which may exist. The most common combustible gas risk is associated with the generation of methane gas by sewage decomposition. However, there is also a risk of combustible liquids entering wastewater facilities via sewage influent due to external spills or dumping. The vapours generated by these liquids present a risk of fire and explosion to the facility. Early warning is critical, to ensure that operations personnel are aware of the situation, and can take appropriate mitigation measures.

Methane gas is lighter than air, and has a density of 0.68 g/L, while air has a density of 1.19 g/L. Thus, it is typically appropriate to place methane detection sensors near the ceiling of an enclosed space, where the methane would tend to accumulate.

However, certain combustible liquid vapours are heavier than air. For example, if gasoline were to enter the facility, the vapours would generally accumulate at lower elevations. It is recommended, at minimum, to install combustible gas detection at a low elevation to detect these heavier vapours, at the point of sewage entry into the facility. Additional sensors may be required near the wet well ceiling, to detect potential methane accumulations.

It is recommended that NFPA 820 be utilized as a reference document for the application of combustible gas detection sensors.

8.2.2 Hydrogen Sulfide Gas Detection

Hydrogen sulphide (H_2S) is a toxic gas, which is harmful even in low concentrations. Some H_2S concentrations and their effect on humans are as follows:

- 0.0047 ppm is the typical human recognition threshold.
- 10-20 ppm is the concentration for eye irritation.

- 50-100 ppm leads to eye damage.
- 150-250 ppm paralyzes the olfactory nerve after a few inhalations, and the sense of smell disappears.
- 320-530 ppm leads to pulmonary edema with the possibility of death.
- > 800 ppm is the lethal concentration for 50% of humans for 5 minutes exposure.
- >1000 ppm can cause immediate loss of breathing.

H_2S gas is slightly heavier than air with a density of 1.363 g/L, while air has a density of 1.19 g/L. While H_2S gas may settle in lower spaces, it can easily be circulated into other spaces by dispersion and air currents, as it is not that much heavier than air. Thus, it is generally recommended that H_2S sensors be placed between knee height and normal breathing height.

A standard that provides detailed recommendations regarding application of H_2S sensors in wastewater treatment facilities is not available. Thus, the application of H_2S sensors must be based upon good engineering design practice, and experience. As a general guideline, H_2S sensors should be installed in all areas where there is a potential for H_2S to accumulate, with the ventilation for that area not active.

It should also be noted that the acceptable levels for H_2S exposure have been reduced in 2010 by the American Conference of Governmental Industrial Hygienists (ACGIH) to a 1 PPM limit for an eight hour Time Weighted Average (TWA) and 5 ppm for Short Term Exposure Limit (STEL). However, most available sensors are not currently capable of measuring low concentrations of H_2S exposure. This is an issue that the industry is just beginning to address. Further review of sensor capabilities and industry practices are recommended during implementation.

8.2.3 Oxygen Gas Detection

Oxygen (O_2) is necessary for human life. The normal concentration of oxygen in the air is 20.9%, and concentrations below 16% are considered unsafe for humans. One of the more likely causes of oxygen depletion is the potential displacement of air by other gases. It is possible that certain liquids, which could be spilled into the sewer system, could produce vapours that displace air, and reduce the oxygen concentration to an unsafe level.

O_2 gas is slightly heavier than the general air composition. Oxygen has a density of 1.43 g/L, while atmospheric air has a density of 1.19 g/L. Since the density is similar enough that oxygen will be dispersed in the air, it is generally recommended that the O_2 deficiency sensors are placed close to breathing level at a mounting height of 1.5m above the floor.

It is recommended that oxygen deficiency sensors be installed in low areas of the facility where there is a possibility of oxygen displacement. An example would be the raw sewage pumping drywell. It should also be noted that excess oxygen in the air is also dangerous, and can cause spontaneous combustion of certain materials. If there are areas where oxygen generation or use exists within the plant, consideration should be given to the installation of O_2 sensors.

8.2.4 Gas Detector Spacing

There are no known published standards that clearly specify detector spacing requirements for gas detectors. While some manufacturers publish a detection radius of 15m, this is not deemed to be universal or appropriate for all applications. Items that must be considered in the selection of gas detection sensors and their installed location include:

- Density of the gas to be detected.
- Potential source of the gas.
- Dispersion of the gas source.
- Ventilation patterns created by the space ventilation system.
- Gas migration patterns during a potential power failure, where ventilation would not be operable.
- Whether redundancy is required to address potential sensor/detector failure.

8.2.5 Hazardous Gas Alarm Notification

It is recommended that the combustible gas, H_2S, and oxygen deficiency detectors all utilize common alarm notification devices. In addition, ventilation failure detection, based upon PLC logic, would signal the same warning devices if the space is potentially occupied. Coordination of signals from the fire alarm system and other audible devices must be provided to allow personnel to differentiate between the alarm signals. The City has standardized on the use of red strobe lights for gas alarms and white strobes for fire alarms.

In areas in which combustible gas detection is required, NFPA 820 section 7.5.3 recommends both visual and audible alarm notification within the protected area, and at the entrances to each area. In spaces where a higher level of ventilation is provided during occupancy, it is proposed that the warning at the primary entrance to areas would consist of a small panel with a red “Do Not Enter” and green “Enter” light. The status of these lights would be based upon both the gas levels, and the ventilation rates.

All gas alarms should be transmitted to the control system for display and logging. In addition, all gas levels should be logged to the historian in the units of display available on the gas controller.

8.3 Identification of Hazardous Areas

There are fire and explosion risks within wastewater treatment facilities that require the designation of electrically classified locations. The risks can be associated with biogas production via the decomposition of sewage, the inflow of a flammable or combustible liquid, or the use of certain chemicals or products on site, such as methanol. The code requirements for electrical classification of hazardous areas are contained within the Canadian Electrical Code (with local amendments), however the specific code guidance regarding electrical hazardous classification of most wastewater facility areas is limited. The primary standard utilized as a guide in the identification and mitigation of combustible and flammable risks in wastewater facilities is NFPA 820.

In areas where there is a potential source of combustible gases, the level of electrical classification required is typically related to the level of ventilation provided. The primary purpose of ventilation is to remove any potential hazardous gases (either combustible or toxic) to ensure a safe working environment for personnel. The secondary purpose of ventilation is to remove any potential combustible gas from the space, to ensure that an explosion does not occur. The third purpose of ventilation is to reduce corrosive gases and moisture to prevent degradation of the facility infrastructure. Where ventilation is inadequate to prevent an explosive concentration of gases from forming, hazardous classification of electrical equipment can be utilized to ensure that the operation of electrical equipment will not ignite a potentially combustible atmosphere.

The proposed ventilation and electrical classification includes analysis based primarily on NFPA 820, the Ontario Ministry of Environment (MOE) Design Guidelines, and the 2012 Canadian Electrical Code.

In areas where there is a direct potential source of combustible gases, such as the primary clarifiers, there are typically two major choices in the ventilation rate and electrical classification. One choice is to electrically classify the space as a Class I, Zone 1 location, and provide a limited amount of ventilation (< 12 ACH). While this reduced ventilation rate can reduce heating requirements and together with the electrical classification eliminate explosion hazards, it does not address the removal of potential hazardous gases, and a higher ventilation rate would be required when the space is occupied.

The second choice is to provide a higher rate of ventilation, which is typically comprised of 12 ACH of ventilation in the summer, when occupied, and when combustible gas is detected, and a reduced ventilation rate of 6 ACH during winter weather. This approach is accepted by current standards, provided a Class I, Zone 2 electrical classification installation is provided.

Significant analysis of the proposed ventilation rate and electrical classification of the existing SEWPCC and NEWPCC facilities was performed under the Reliability Upgrades project. While there can be a net present value economic benefit associated with reduced ventilation rates in a Class I, Zone 1 electrical classification, the economic benefits are typically discounted when operational and maintenance considerations are included. It should also be noted that utilization of the Class I, Zone 1 electrical classification typically increases the total electrically classified area, as it is common for the incorporation of buffer zones with Class 1, Zone 2 classification to be provided between the Zone 1 and the unclassified areas.

Maintenance of electrical and automation equipment must also be considered when electrically classifying areas. In a Class I, Zone 1 location, it is not acceptable to work on energized equipment, except if the equipment is intrinsically safe. In addition, tools used in a Class I, Zone 1 location must be electrically classified for the location. While the general rule for a Class 1, Zone 2 location also requires appropriately rated tools, there is an industry accepted exception that proves to be very useful. ISA-TR12.13.03-2009 presents a method, called a Gas Free Work Permit system, whereby portable combustible gas detection is utilized to allow “hot” work in a Class I, Zone 2 location.

The electrical classification of each area within the wastewater treatment facilities must be performed by a qualified professional engineer. When a choice is provided between Class I, Zone 1 electrical classification and Zone 2 classification, based upon ventilation, it is recommended that in most cases that preference be given to Zone 2 electrical classification, especially if the space is routinely occupied. However, it should be noted that this must be reviewed on a case by case basis, with review of the specific hazards associated with each area of the facility with respect to current codes and standards.

8.4 Hazardous Locations – High Level Design Basis

The general proposed solution to hazardous classification of various automation components in electrically classified locations is shown below.

PLCs

It is recommended to avoid installation of PLCs in classified locations. While Class I, Zone 2 rated PLCs are available, the hazardous locations typically also have other hazards, such as corrosive gases, which could affect the maintenance or life of the equipment in the location.

Enclosures

The preferred solution is to utilize NEMA 4/4X enclosures in Class 1, Zone 2 locations, provided appropriately rated components are utilized internally, or intrinsically safe circuit design is employed. The alternate solution is to utilize an explosion-proof NEMA 7/7X enclosure if the components contained within cannot be appropriately rated for the location.

In Class 1, Zone 1 locations, the preferred solution is to utilize NEMA 4/4X enclosures provided intrinsically safe circuit design is employed. Alternately, explosion-proof NEMA 7/7X enclosures are required.

Switches and Pilot Lights

In Class 1, Zone 2 locations, switches and pilot lights can either be appropriately rated for the location (sealed variants), or designed as part of intrinsically safe circuits.

In Class 1, Zone 1 locations, switches and pilot lights can either be appropriately rated for the location, within the appropriate enclosure, or designed as part of intrinsically safe circuits.

Instruments

It is typically relatively straightforward to procure instruments rated for Class I, Zone 2 locations, which can be wired via conduit or TECK-style hazardous rated cable, and this is deemed to be the preferred installation. The use of intrinsically safe circuits is acceptable, and may be required for certain instrumentation, but is not preferred due to the costs and space required for the installation of barrier devices.

In Class 1, Zone 1 locations, the case for explosion-proof vs. intrinsically-safe equipment must be made on a case-by-case basis, but the use of intrinsically-safe instruments is preferred. Intrinsically-safe systems allow for live maintenance of instruments and also are less likely to cause a hazard due to potential damage of the enclosure.

Control Valves

Typical choices for control valves are either electric or pneumatic actuation. Where instrument air is available, consideration should be given to pneumatic control valves, which can allow for a straightforward installation in a Class I, Zone 1 or Class I, Zone 2 application. In Class I, Zone 1 locations, the solenoids or positioner to actuate the valve can typically be obtained in intrinsically safe versions. If instrument air is not available, electric actuation can be utilized, but will typically require an explosion-proof actuator enclosure.

9.0 AUTOMATION POWER SUPPLY

9.1 Electrical Distribution System

Basic discussion of the electrical distribution system is required to identify the proposed sources of electrical power for the automation systems. Based upon the configuration of the existing electrical distribution systems at the City of Winnipeg wastewater treatment facilities, it is assumed that the electrical distribution systems will generally be set up as a secondary selective system, where the 600V distribution system is set up with two points of distribution, fed via separate transformers and utility supplies, and connected with a tie breaker. A typical secondary selective system is shown in Figure 9-1.

.

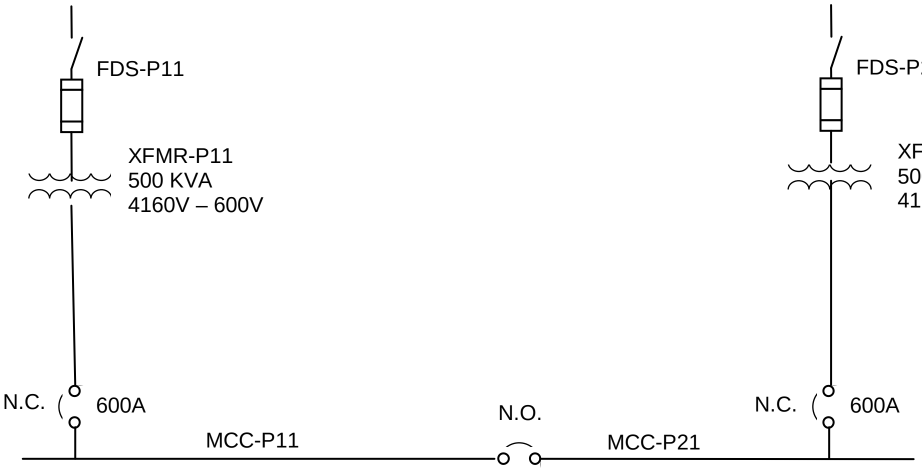


Figure 9-1: Secondary Selective Electrical Distribution System

It is expected that parallel process equipment installations will typically be powered from alternate banks of the electrical distribution system to ensure a high level of process power availability. For example, process trains 1 and 3 may be fed from MCC-P11 while process trains 2 and 4 may be fed from MCC-P21. Also, primary and secondary pumps and meters could be fed from alternate banks in critical applications to increase probability of power availability.

9.2 Uninterruptible Power Supply

9.2.1 Configuration

Critical automation systems will be powered from an uninterruptible power supply (UPS). UPS units may either be centralized or distributed. Generally, a centralized approach is recommended where there are a significant number of UPS powered loads, as this reduces the maintenance requirements associated with UPSs and their battery systems. Centralized systems are typically 120/208V, 3ph, with a capacity greater than 5 kVA. However, the centralized system should at most extend over the area of a single building, and the length of the UPS distribution wiring should be limited. There are two primary purposes for the utilization of UPS power. The first is to provide uninterruptible power, and the second is to provide clean, filtered power at the nominal output voltage. If a UPS distribution system is extended over too wide an area, the UPS power distribution system can suffer from induced noise, voltage drop, and grounding potential issues. As a rough guideline, an individual UPS distribution should be limited to a maximum of 100m from the source, however this value is highly dependent upon the nature of the installation and surrounding electrical installation. Consideration should be given to reducing the total number of UPS units to limit the production of harmonics on the upstream power distribution system, and reduce the number of battery locations for maintenance. The maintenance of the battery installations is an important factor in the UPS system design.

Smaller, individual distributed UPS units are appropriate where the number of UPS loads within a given physical area is limited and/or widely distributed. For example, at a remote outfall sampling building, if UPS power is required, it would be more appropriate to install a small distributed UPS than to extend UPS power from a centralized UPS system. For smaller distributed applications, such as a single panel installation, an industrial-grade 24 VDC UPS system should be considered over a commercial-grade 120VAC UPS unit with receptacles. Distributed UPS units should be located within a control panel enclosure and be ventilated to avoid hydrogen gas build-up from the batteries. Alternately, the batteries can be located external to the panel in a separate module.

For the most critical systems, consideration should be given to utilization of two UPS systems, with separate power supplies, and separate distributions, feeding loads that are essentially dual sourced. For example, computer servers can be purchased with dual power supplies and power supply cords. Some UPS manufacturers will promote redundant UPS units with a common UPS power distribution, however in many cases these may not provide the expected reliability as a fault within the UPS distribution system could potentially disrupt power to all UPS loads.

9.2.2 Battery Duration

The required design battery duration rating of UPS units is dependent upon the criticality of the load and the level of backup within the power supply system. The suggested battery design rating for various scenarios is provided in Table 9-1.

Table 9-1 : UPS Design Battery Life

UPS Type	Power Supply Configuration	Time	
		Low / Medium Reliability Requirements	High Reliability Requirement
Centralized	Single Source	60 minutes	120 minutes
	Transfer Switch Between 2 Sources	45 minutes	90 minutes
	Single Generator backed	30 minutes	60 minutes
	Multiple Generator backed	15 minutes	30 minutes
Distributed	Single Source	45 minutes	120 minutes
	Transfer Switch Between 2 Sources	30 minutes	90 minutes
	Single Generator backed	20 minutes	60 minutes
	Multiple Generator backed	10 minutes	30 minutes

In addition, manufacturer rated battery capacity is typically based upon ideal operating conditions when the battery is new and operating at ideal temperatures, and de-rating based on the expected battery life and actual operating temperatures is required at design time to ensure that the design capacity will be provided throughout the battery life.

Finally, it should also be noted that UPS battery life is limited, and can be as low as five years in some cases. UPS design planning should consider maintenance requirements associated with the batteries, and means for end-of-life detection.

9.2.3 UPS Monitoring

Interface of the UPS systems to the automation system is required to allow for remote monitoring and alarming. At minimum, alarms for large UPS units are to include UPS OK/fault status, battery low, utility status, and bypass status. Small, panel based UPS units should have at minimum have a battery low alarm and a fault alarm via a remote interface. A UPS overload alarm would also be useful. The UPS interface may be via relay interface or communication.

9.3 Load Power Supply Design Criteria

9.3.1 General Guidelines

General design guidelines regarding the power supply of automation systems are as follows:

- Motor controls will be powered by dedicated local 120VAC control power transformers associated with each motor starter. Ensure that manual control capability, where provided, is not compromised due to the loss of any other power source, including the loss of UPS power.
- The preferred voltage for instrumentation and I/O is 24VDC. The primary rationale is for safety and arc flash rationale. It is expected that most or all new PLC I/O will be 24 VDC, although 120VAC I/O will be utilized to interface with existing equipment.
- Where redundant power supplies are provided, they must be monitored, to ensure that failure of a single power supply is alarmed to the HMI.

The design criteria for the power supply to various automation loads are summarized in Table 9-2. Note that the reliability requirements are a general assessment, and it is recommended that a reliability assessment be utilized for specific applications, as discussed Section 3.0.

Table 9-2 : Automation Power Supply Design Criteria

Item	Reliability Requirement (See Note 1)	Power Supply	Notes
Motor Controls	-	Dedicated Local Control Power Transformer – 1 per starter	
120 VAC Powered Instrumentation	Low	120 VAC Process Panelboard	See Note 2
	Medium	120 VAC UPS	
	High	120 VAC UPS	
24 VDC Instrumentation & I/O	Low	24 VDC Power Supply fed from Process Panelboard	See Note 2
	Medium	Redundant paralleled 24 VDC Power Supplies fed from UPS	
	High	Redundant 24 VDC Power Supplies, paralleled output A - UPS Power B - Filtered Non-Essential Power	
PLC Power Supply	Low	UPS Power – Single Feed	
	Medium	If Power Supply Dedicated to PLC – Single Power Supply, UPS fed.	See Note 3
		If shared with I/O or other purposes, dual power supplies A - UPS Power B – Filtered Non-Essential Power	
	High	Dual Power Supplies A - UPS Power B - Filtered Non-Essential Power	See Figure 9-2
Ethernet Network Switches	Low	UPS Power – Single Feed	
	Medium	Dual Power Supplies A - UPS Power B - Filtered Non-Essential Power	
	High	Dual Power Supplies A - UPS Power B - Filtered Non-Essential Power or redundant UPS	
Electric Valve and Damper Actuators (Small)	Low	120 VAC Process Panelboard Optionally 24VAC via CPT	
	Medium	UPS Power – Single Feed	
	High	UPS Power – Single Feed	

Notes for Table 9-2:

1. *The Reliability Requirement is a general assessment of the reliability associated with the individual automation device, not necessarily the system as a whole.*
2. *Associate the instrument power supply with the same bank as the equipment is powered from. For example, if a pump is powered from Bank 2, power the associated flowmeter from a Bank 2 120 VAC panelboard.*
3. *The use of a common 15A breaker and supply wire is not considered shared provided the loading is less than 20% of the max 12A loading and appropriate fusing with selective coordination is provided to avoid tripping the circuit breaker on a fault associated with the alternate load. The use of a common 24VDC power supply is considered shared under any circumstance.*

9.3.2 PLC Power Supply

The proposed PLC power supply configuration for all but the simplest PLC applications is shown in Figure 9-2.

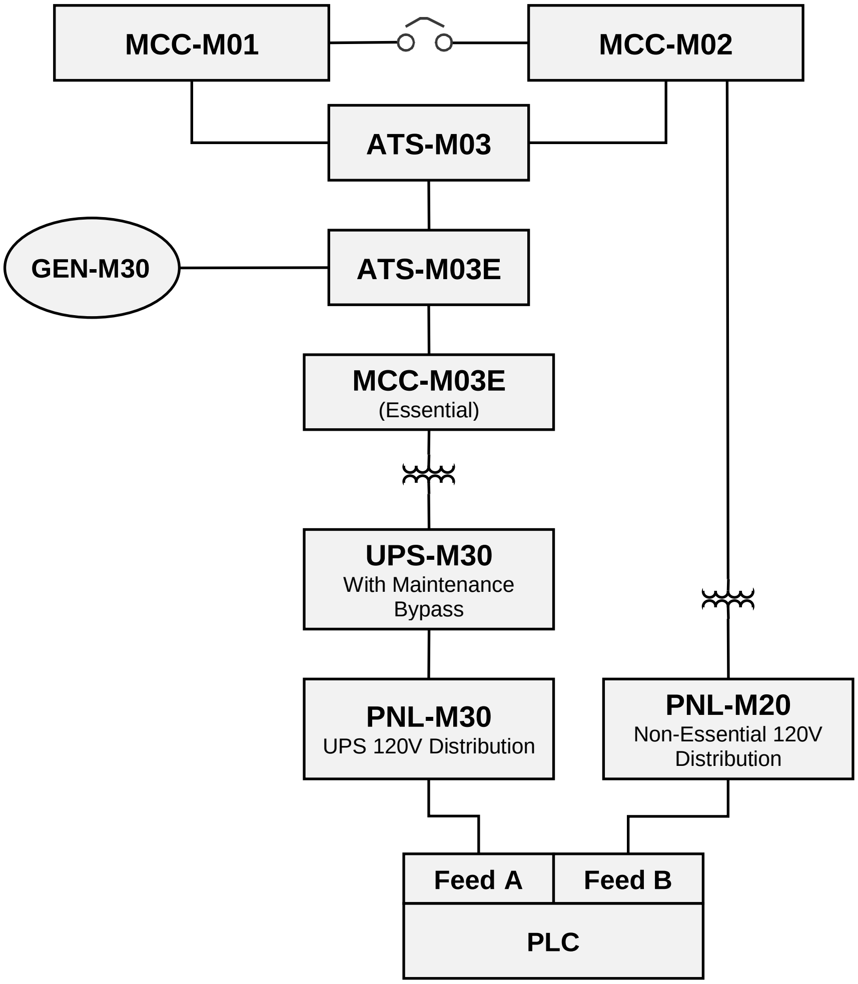


Figure 9-2 : PLC Power Supply Block Diagram – Medium & High Reliability Requirement

10.0 CONTROL SYSTEM ARCHITECTURE

10.1 General Reference Model Architecture

The current and future control system architecture at the wastewater treatment facilities is comprised of numerous hardware and software components working together to monitor and control the process and ancillary systems. Prior to detailed discussions regarding control system architecture, it is beneficial to utilize a common reference model that is well understood in industry practice. The Purdue Model for Control Hierarchy was developed to document manufacturing, operations, and management relationships, and has been referenced by many groups. This model is probably the most widely understood reference model for describing the relationship between various levels of the control system. The control system hierarchy, based upon the Purdue Model, is depicted in Figure 10-1. The reference model contains six levels, where a specific functionality is provided at each level.

Level 0 is the Process level, which contains the automation components which directly measure or control the process. This includes sensors, motors, drives, and other components at the field level within the process. It typically would also contain local push-button stations and local control panels.

Level 1 is the Basic Control level where the automation system directly monitors and controls the process. PLC (or DCS) based control is typically at this level, along with I/O devices, single loop controllers, and traditional relay based interlock systems. Local operator stations, such as a small touchscreen that controls a specific piece of equipment, could potentially be considered as Level 1 devices, although there is potential for them to be considered as Level 2 in some cases. The interface from Level 1 to Level 0 will typically be via fieldbus or via direct connection to input and output modules.

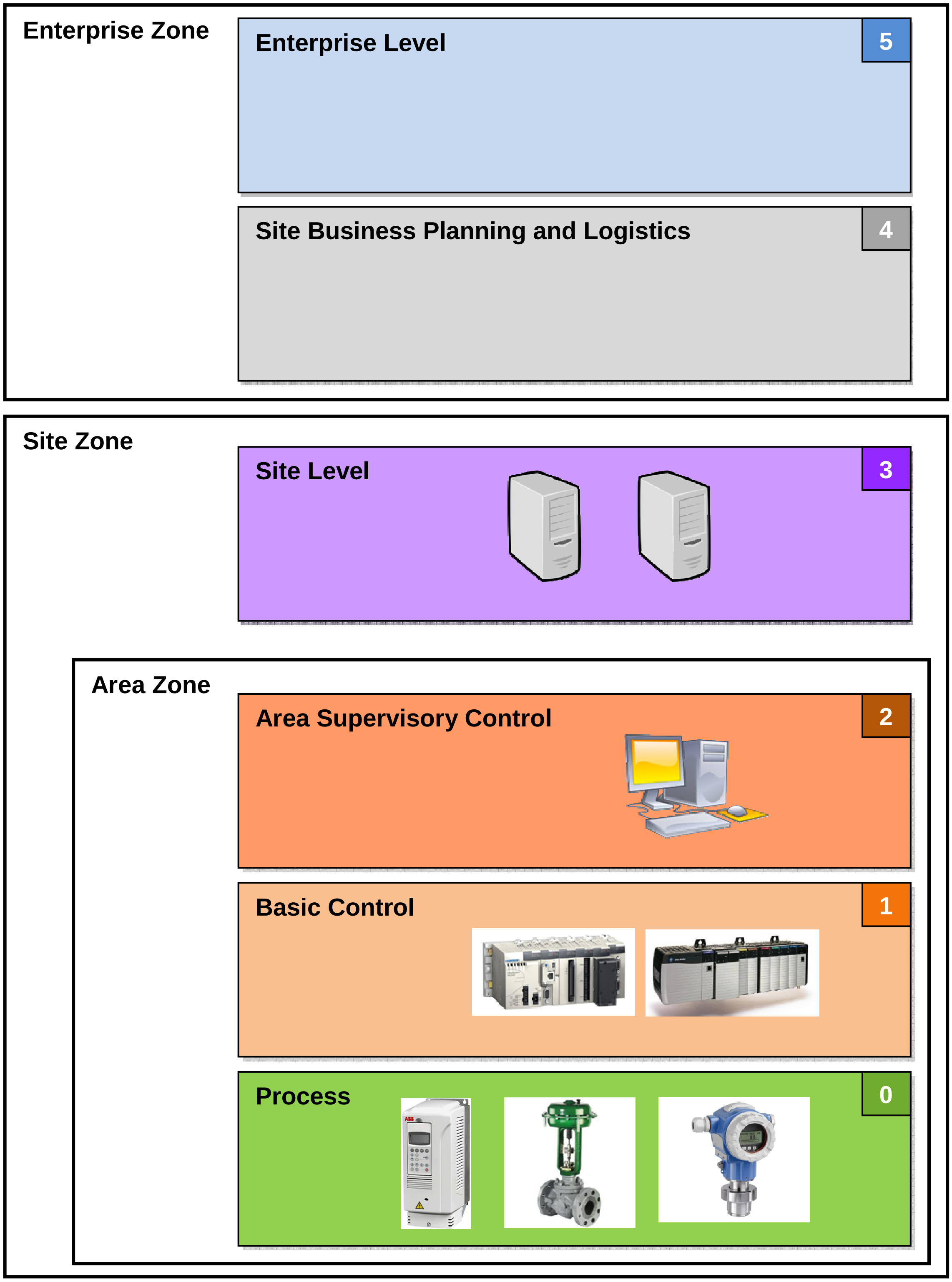


Figure 10-1 : Control System Heirarchy

Level 2 is the Area Supervisory Control level, where operations personnel monitor and control the overall process for an area. Typically this would be an HMI interface, which communicates to the Level 1 control system via a network interface. The original intent of the Purdue Model appears to be that Level 2 is for supervisory control of an area only, but this is not clearly applied when most modern HMIs are able to access and control then entire facility from anywhere. For the purpose of this document, the HMI's intended primarily to control a specific area are considered to be Level 2.

Level 3 is the Site Level, and is typically viewed as the highest level of industrial automation and control systems. There is significant variability as to the industrial automation components that are installed at this level, and can include: production reporting, the plant historian, site-level operations management, asset and material management, patch launch server, file server, and other servers such as domain servers, active directory, and terminal services.

The levels 0 – 3 are typically reasonably well understood, although in some cases the boundaries between the levels can be blurred. For example, some may classify the HMI Servers as Level 3, while others may classify them as Level 2, together with the HMI clients. The boundary between Level 3 and 4 is typically well understood, but traditionally the interfaces across these levels have been the subject of limited automation. The interface between IT responsibility and automation responsibility has typically been applied at the Level 3 / 4 boundary. The level of IT involvement at the levels 0 – 3 must be clarified prior to implementation.

Level 4 is typically referred to the Site Business Planning and Logistics level, and is where the overall operations of the facilities are managed. Typically, for other industries, this level contains the Manufacturing Execution Systems; however this is not directly applicable to a wastewater treatment application. Applications and tasks that would be typically associated with this level are: internet access, e-mail, non-critical production systems such as overall plant reporting, Computerized Work Management System, and LIMS (Laboratory Information Management System).

Level 5 is the Enterprise level, and consists of the corporate network and overall business management systems.

While detailed classification of every component into this six level reference model is not required, an understanding of this reference model is very useful for the development of the automation system architecture, network planning, security planning, and development of interfaces to enterprise systems. This reference model will therefore be subsequently referenced to facilitate further discussion and analysis.

10.2 Existing DCS Architecture

The existing DCS architecture at the three wastewater treatment facilities is generally comprised of one or more DCS Process Control Units (PCUs) per process area. Each DCS PCU has redundant processors and centralized local I/O, with the PCUs typically located in a conditioned control room, with media filtration for corrosive gasses. The DCS PCU's are connected together on a dual ring proprietary network. Remote DCS I/O is typically not utilized, except at the NEWPCC UV disinfection facility. A typical configuration of the existing DCS is shown in Figure 10-2. This DCS architecture has served the City well, however the DCS, in its current state, is nearing the end of its effective service life. Significant upgrades to or a replacement of the DCS will be required to support the planned wastewater treatment plant upgrades.

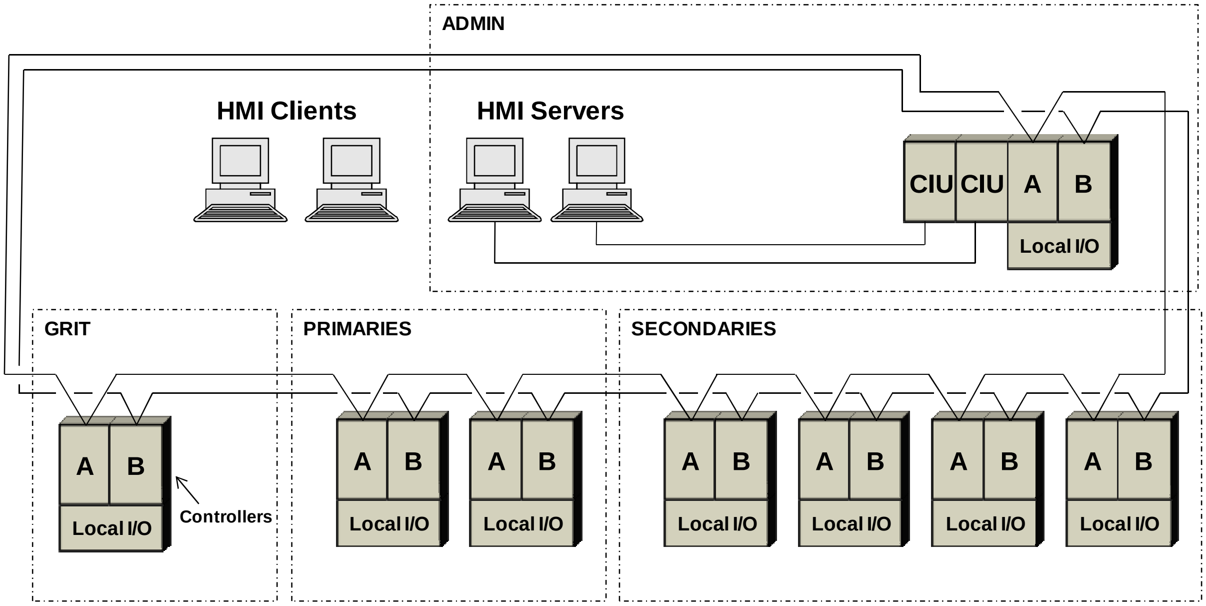


Figure 10-2 : Typical Existing DCS Architecture

10.3 Centralized vs. Distributed

The existing DCS architecture is centralized by process area. All I/O and control is almost exclusively located within the dedicated control room for each process area. This centralized control concept has served the City quite well; however, there can be significant advantages to distributing the control logic and I/O to the field. In reality, the concepts of centralized vs. distributed control can be blurred, as the control could potentially be centralized with the I/O set up as distributed remote I/O.

A comparison between a centralized and distributed architecture is presented in Table 10-1. Centralized and distributed architectures are presented, along with a combined architecture where the control is centralized, but the I/O is distributed.

As can be seen, in Table 10-1, while each architecture concept has some benefits, there are deemed to be more advantages with a distributed architecture. The distributed architecture must however not be taken to the extreme, or new disadvantages will become apparent. For example, it would be possible to implement a local control loop with a valve, flowmeter, and local single-loop DIN-style controller, connected to a larger network for overall integration. While this example would be very distributed, the additional complexity of integration and training of maintenance personnel on the single-loop controllers are an obvious disadvantage.

Table 10-1 : Centralized / Distributed Comparison

Item	Centralized	Centralized Control / Distributed I/O	Fully Distributed	Notes
Reduced Wiring		✓	✓	Distributed control has reduced wiring costs, but it is noted that centralized control can utilized remote I/O.
Expansion and Modifications			✓	Centralized control system modifications can be more difficult as control system interruptions can affect the entire process.
Provision of Local Touchscreen HMIs			✓	Local touchscreen HMIs are typically easier to implement with distributed control.
Speed			✓ ✓	Most distributed control is significantly faster than centralized control.
Project Delivery			✓	People working on centralized control system architectures must have a reasonable understanding of the entire system.
Troubleshooting			✓	Distributed systems are typically simpler.
Reduced Redundancy Requirements			✓	Failure of a single distributed controller will typically affect only a limited system within the process.
Environmental Considerations	✓ ✓	✓		It is easier to provide a conditioned environment for centralized control.
Vendor Homogeneity	✓	✓		Vendor homogeneity is almost mandatory with centralized systems, but can be optional for distributed systems. This can affect training requirements and spare parts.
Control Logic Application Management	✓	✓		Centralized systems consolidate the control logic application, providing easier management compared to multiple distributed applications.

In the context of the wastewater treatment facilities it is recommended that the following guidelines are applied regarding distributed control concepts:

- I/O should be decentralized as much as practical. Utilize networked equipment or I/O that is closer to the processor.
- Allocate controllers to smaller systems rather than complete process areas, to limit the effect of a single controller failure. Consideration should be given to utilizing separate controllers for parallel process trains, such that failure of a single controller will not affect all process trains.
- Set up the control system architecture in a manner that is consistent with the process configuration layout. As the process configuration is not within the scope of this report, only general guidelines regarding layout can be provided.
- Limit control systems to a single vendor to avoid issues associated with distributed systems from multiple vendors. This is discussed further in Section 17.0.
- Be aware of environmental considerations associated with the area. Generally installation of controls should be avoided in corrosive and electrically classified locations. In a wastewater context, this typically means that controls such as PLCs and I/O should be avoided in areas with direct exposure to wastewater (e.g. Primary Clarifier process area). Also avoid outdoor installations if other alternatives are practical.

An example of proposed distributed control concepts is presented in the following two figures. Figure 10-3 indicates the relative location of the I/O in plan view for the SEWPCC primary clarifiers. For a potential future configuration with up to six secondary clarifiers, it is proposed that additional I/O (and possibly control) locations would be installed closer to the process, as shown in Figure 10-4. Note that the elevation of the I/O is not indicated in both figures, and the existing I/O in Figure 10-3 is actually on the lower level of the facility.

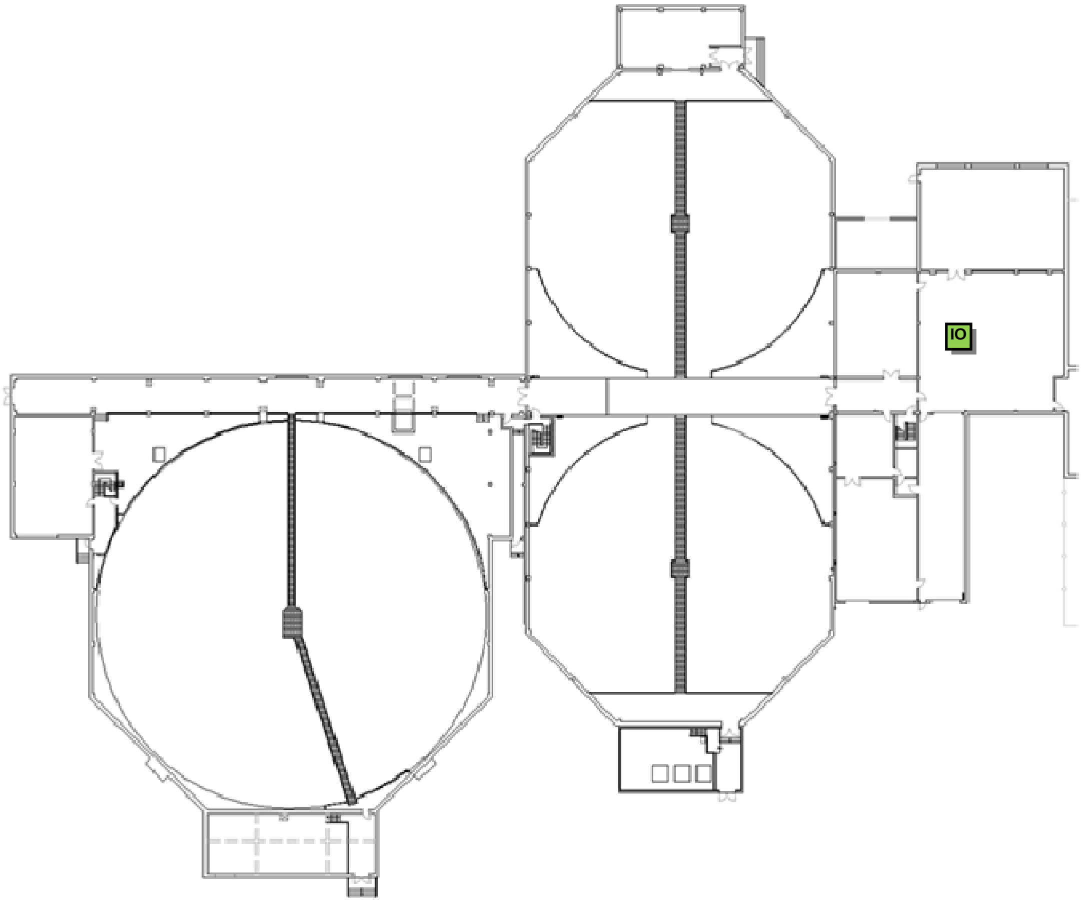


Figure 10-3 : Existing Area Centralized I/O

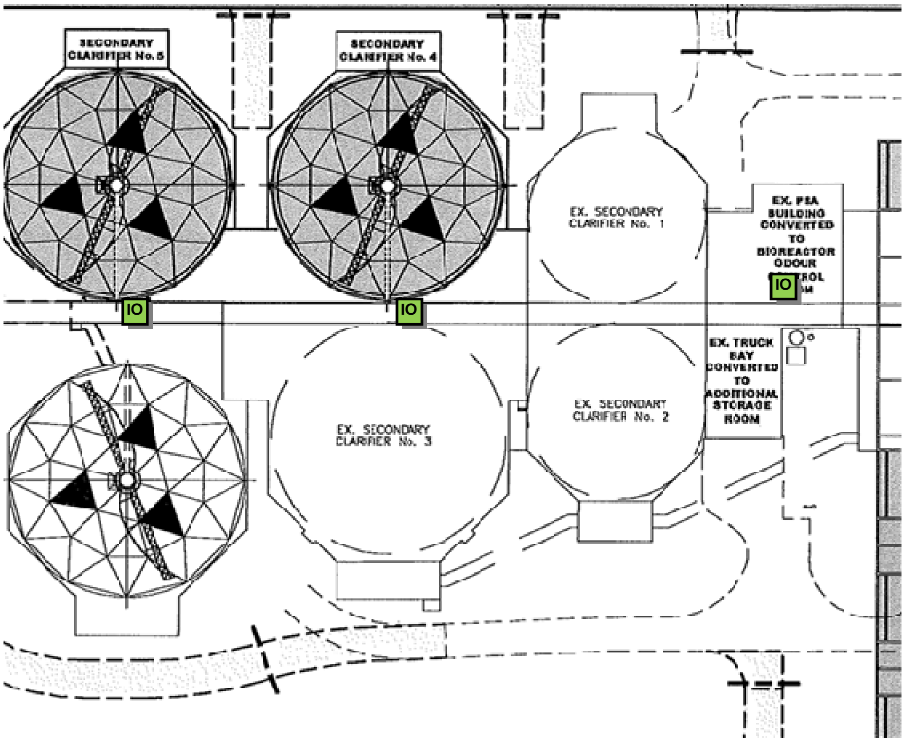

SECONDARY CLARIFIER No. 5
SECONDARY CLARIFIER No. 4
EX. SECONDARY CLARIFIER No. 1
EX. PEA BUILDING CONVERTED TO BIOREACTOR ODOUR CONTROL ROOM
IO
IO
IO
EX. TRUCK BAY CONVERTED TO ADDITIONAL STORAGE ROOM
EX. SECONDARY CLARIFIER No. 2
EX. SECONDARY CLARIFIER No. 3

Figure 10-4 : Potential Distributed I/O

10.4 Current DCS Architectures

There are quite a few DCS vendors on the market, and most current DCS architectures are very similar when viewed from a high-level perspective. It is typical for redundant HMI servers to connect to redundant process controllers in the field. These controllers are typically quite powerful and have advanced features. The DCS controllers are typically expensive, however given their processing capability, can service a substantial amount of I/O and serve a large process area. Thus, in a typical wastewater treatment plant, it would be typical to have a process area served by a single DCS controller pair, and in some cases multiple process areas could potentially be served by a single controller pair. Many DCS systems have limitations on the number of controller pairs; for example, the ABB 800xA system is limited to a maximum of 75 controllers on a system. Remote I/O, which may or may not be distributed, would be utilized for integrating equipment. In addition, fieldbuses may be utilized to integrate equipment, and DCS support for fieldbus technologies is typically quite good.

Figure 10-5 provides a high-level representation of a typical DCS architecture, where there are a limited number of redundant controller pairs servicing remote I/O. It is typical, although not necessarily required, that remote I/O communications are redundant.

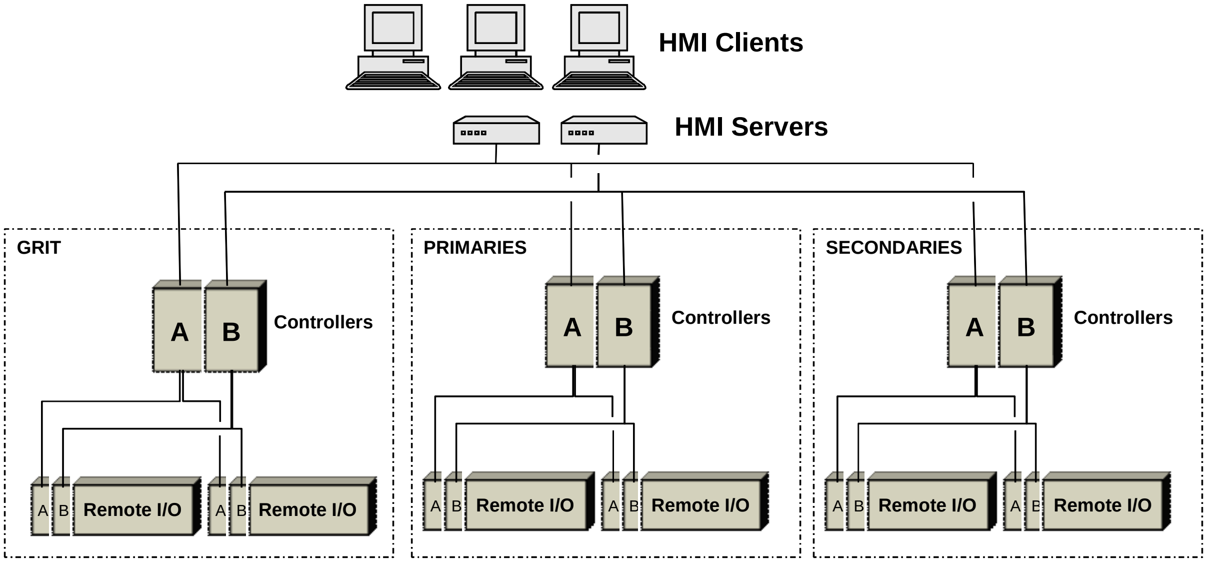


Figure 10-5 : Typical Wastewater Industry DCS Architecture

10.5 PLC Based Architectures

In this document, the term PLC (Programmable Logic Controller) is utilized to encompass both traditional PLCs and Programmable Automation Controllers (PACs). Historically, PLCs were better suited to discrete logic and their capabilities for complex control loops and advanced automation functions were limited. However, most PLC vendors now produce PLCs with advanced automation features that can compare with DCS controller capabilities. Some vendors have replaced the term PLC and are now calling their products PACs, to represent the advanced features available within the systems. However, it is still typical in industry to refer to all of these systems as PLCs, and they will be referenced as such in this document.

PLC architectures can be similar or quite different than DCS style architectures. It is possible to construct a PLC architecture that physically appears to be identical to the typical DCS architecture presented in Figure 10-5, with redundant PLC controllers (or alternately called processors), and remote I/O. Note that while the architecture can appear physically similar, there can be significant differences relating to control logic implementation and overall system integration.

PLC systems are not always as tightly integrated as DCS systems, however they provide significantly more flexibility than DCS systems. It is easier to implement a true distributed architecture, where more PLC nodes are utilized and situated adjacent to process equipment. An example of a PLC distributed architecture is presented in Figure 10-6.

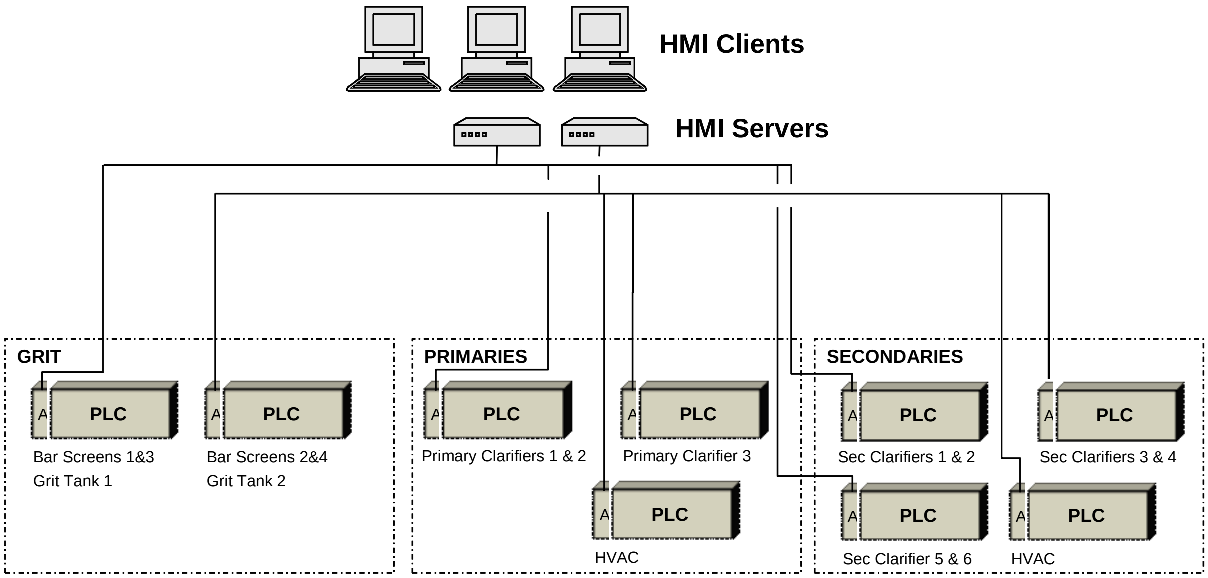


Figure 10-6 : Typical PLC Distributed Architecture

It should also be noted that the vendors for PLC based systems have a different business approach compared to DCS vendors. DCS vendors prefer to sell complete systems with hardware and logic configuration fully integrated as part of the package. It is strongly encouraged in the business model to return to the vendor for all parts, service, and upgrades, as they best understand the product. However, the PLC businesses typically are more flexible and are receptive to the sale of individual components and thereby allow local systems integrators to perform the overall system integration. PLC vendors often do have a system integration team, however this service is usually only practical on large initial installations.

10.6 Comparison of DCS vs. PLC Architectures

A comparison of current DCS technologies vs. PLC systems is presented in Table 10-2. Note that this comparison is high level, and attempts to avoid specifics associated with a single vendor.

Table 10-2 : DCS / PLC Comparison

Item	DCS	PLC
Typical Architecture	Large redundant DCS controllers with remote I/O and fieldbuses.	More distributed PLC controllers.
Up-front Cost	$$$ to $$$$	$ to $$$
Redundancy	Typically provided at almost all levels.	Redundancy is provide where required.
Project Delivery	Vendor will provide single-source solution.	Typically via systems integrator. Vendor may integrate large projects.
Vendor Supplied Programming Libraries	Moderate to high	Few to moderate
Ability to customize	Low to moderate	Moderate to high
HMI / PLC Development Software Integration	Typically well integrated.	Less integrated than DCS.
Fieldbus Support	Good	Moderate to good
Open vs. Proprietary Development	More proprietary	More open
Major Vendors	ABB Emerson Honeywell Invensys Siemens Yokogowa	GE Omron Rockwell Schneider Siemens

10.6.1 City Decision

As part of the master planning process, the City has made a decision to retire the existing DCS architecture and move towards a PLC-based architecture. Some of the rational for this decision include:

- Spare parts and minor upgrades for the existing DCS have within recent history, proven to be quite costly.
- Existing DCS programming capability is limited to internal City forces and ABB. As part of the upgrade projects where the programming requirements exceed the City’s internal capabilities, there is no competition available and the prices received from ABB have been significantly higher than for comparable PLC based systems.
- The capability of the existing DCS in many cases is at its limit. While ABB does offer upgrade paths and options that could extend the DCS capabilities, based upon experience to date it is believed that these upgrades will be more expensive than migrating to a PLC based system.
- The City’s method of competitive procurement does not align with the DCS strategy to develop long term relationships between clients and the vendors. The PLC vendor strategy of utilizing system integrators allows for competitive bidding of automation work.
- Current PLC platforms can provide functionality that is very similar to DCS capability.

10.7 PLC Architecture

Guidelines to be utilized for the PLC architecture design are as follows:

- It is preferred that PLCs be smaller or moderately sized and tied to a specific unit or process rather than large PLCs that control a large number of systems. By using more, distributed PLCs, the reliability can be increased in a cost effective manner. In addition, start-up and maintenance of the smaller PLCs is more straightforward than for large centralized PLCs.
- Auxiliary systems, such as HVAC, will typically be controlled by dedicated PLCs independent of the process PLCs.
- Redundancy of PLC processors will only be utilized for critical automation systems with a high reliability requirement. Reliability assessment, as discussed in Section 3.0 should be utilized as a guide, and Section 10.7.1 provides some basic guidelines.
- Where multiple process streams are present with a high reliability requirement, multiple PLCs are to be employed such that, at minimum, at least half of the process streams remain fully functional in the event of a controller failure. Additional PLC redundancy may be required, and as should be assessed utilizing Section 3.0 as a guide.

- The networks utilized to integrate PLC controllers with field devices (Level 0) must provide sufficient availability to not impede the reliability of the overall automation system. Further discussion is provided in 10.8.

10.7.1 Evaluation of Redundancy Requirements

The requirement for redundancy in automation systems is not always clear. It has been quite common for engineers to specify redundant DCS or PLC controllers with the intent of achieving a higher level of reliability, but rarely are the I/O or field instruments redundant in an application comparable to wastewater treatment. However, when reviewing the reliability of current automation components, the controllers typically have a lower failure rate than many other automation system components. Providing redundancy to the more reliable component within an automation system does little to improve overall system reliability. However, there are a caveats for continuous 24/7 processes, such as wastewater treatment, in that the consequences of taking a controller out of service for maintenance or upgrade must also be reviewed. With redundant controllers, a single controller may be replaced, or downloaded with a new program while the other controller maintains operation of the process.

As a general rule of thumb, the criteria identified in Table 10-3 are a basic guideline for determining controller redundancy requirements, however it is recommended that further reliability analysis be performed for critical processes, as discussed in Section 3.0.

Table 10-3 : Conservative Guidelines for Controller Redundancy

Criteria	Yes	No
Is a 15 minute planned shutdown of the PLC, with 30 minutes notice, on an annual basis acceptable?	Controller redundancy not necessarily required.	Controller redundancy or redesign required.
Is a 120 minute unplanned shutdown of the PLC, approximately every 10 years acceptable?	Controller redundancy not necessarily required.	Controller redundancy or redesign required.

Note: *The above guidelines assumes that PLC controller spares will be maintained on site. If this is not the case, additional evaluation regarding controller redundancy is required.*

For applications with the highest level of criticality, instrument and I/O redundancy could be required. In some cases, redundancy of individual instruments may be required, which is discussed further in Section 6.3, and where instrument redundancy is provided, care should be taken to separate the redundant instruments onto separate I/O modules or fieldbuses. It is noted that the need for I/O redundancy in a wastewater treatment application is not very common.

10.8 Field Network Architecture

The architecture of the network to connect PLC controllers (Level 1) with field devices (Level 0) must ensure reliable communications to ensure continuity for process monitoring and control.

It has been traditional to provide segregation between field networks which integrate field devices and the controller process networks which integrate PLCs for peer level communication, and communication with the HMI systems (Level 2 and 3). An example of an acceptable PROFIBUS field network is shown in Figure 10-7.

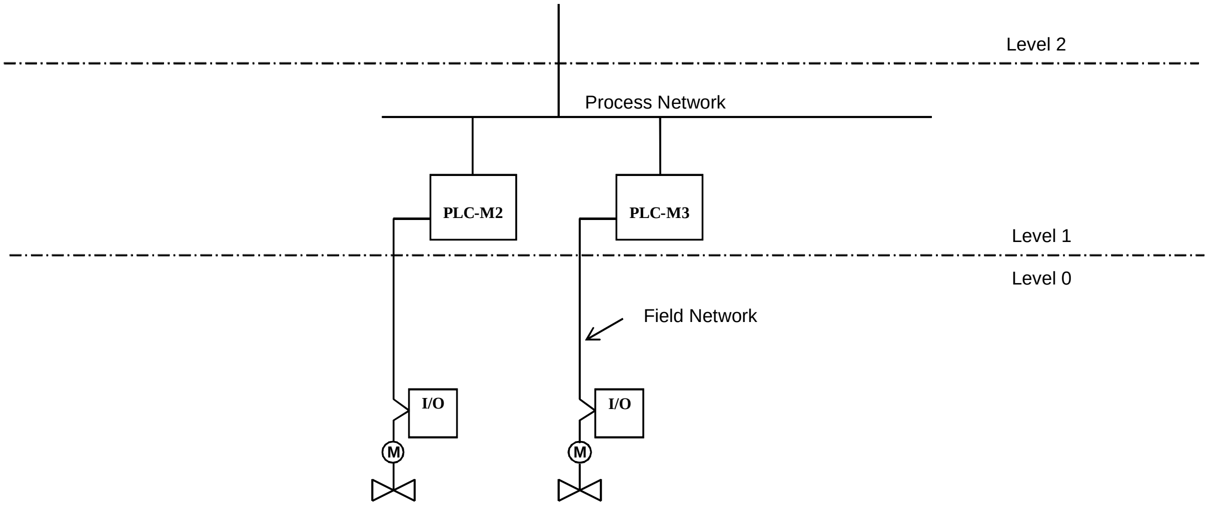


Figure 10-7 : Segregation of Field and Process Networks – PROFIBUS Field Network

However, it is becoming more common for the use of Ethernet communications at the field network level. Figure 10-8 depicts the use of an Ethernet field network to collect remote I/O, where the field network is segregated from the process network. The advantage of this approach is that the field network and process network will not interfere with each other. This is also a more secure approach as advanced network security features are not required to protect the field network. However, the disadvantage of this approach is that the field networks are local islands, and communication to the field network is dependent on the controller's ability to bridge the communications between the field and process networks. If this bridging is not available, personnel must physically connect to the field network.

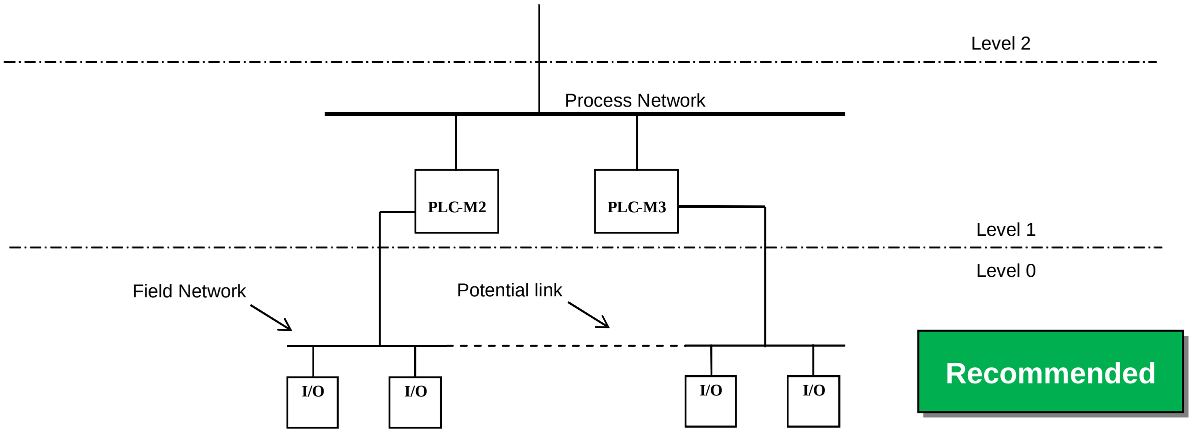


Figure 10-8 : Segregation of Field and Process Networks – Ethernet Field Network

Alternately, given the ability to easily connect Ethernet networks, it is quite common that the Level 0 field devices can be directly connected to the process network. The primary advantages to this approach are fewer networking switches and ease of routing directly to the I/O for maintenance, or direct access from the HMI, if desired. However, the integration of the process and field networks must be set up to avoid impacting either network's traffic. In the past, when network bandwidth was limited, this would never have been a viable approach, however with 100 Mbps, and gigabit Ethernet capability easily attainable, it is possible to share the physical process network with the field network, as shown in Figure 10-9.

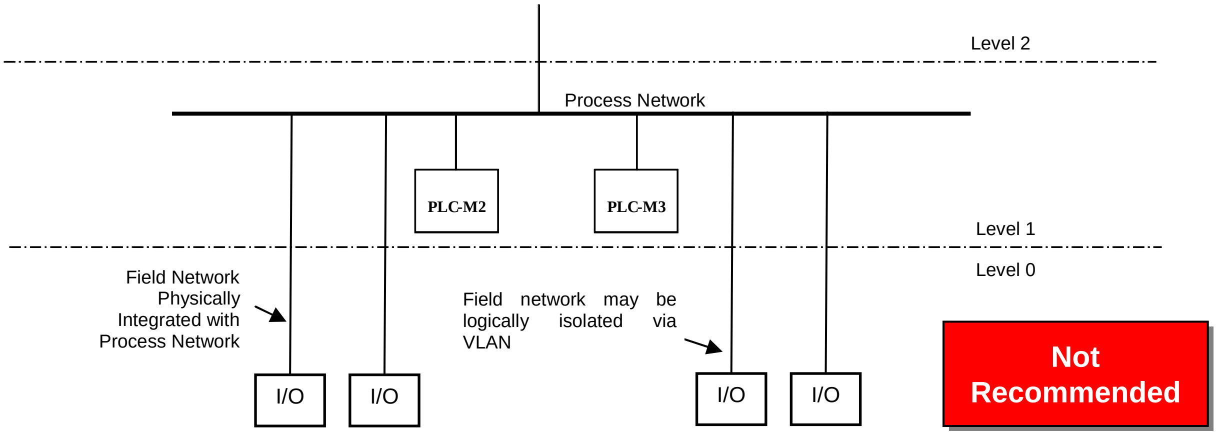

Level 2
Process Network
PLC-M2
PLC-M3
Level 1
Level 0
Field Network Physically Integrated with Process Network
Field network may be logically isolated via VLAN
I/O
I/O
I/O
I/O
Not Recommended

Figure 10-9 : Potential Integration of Field and Process Ethernet Networks

If an architecture such as Figure 10-9 is utilized, it is best if the field (Level 0) and process (Level 1/2) networks are separated with a VLAN. A VLAN is a logical separation of a physical network using managed switches, such that the logical networks cannot communicate without a router or layer 3 switching. This segregation may not be optional in certain large or Ethernet/IP installations, where the VLAN may be required to manage the network bandwidth and prioritize traffic.

However, an issue with the approach identified in Figure 10-9 is effective management and support of the network. Network segregation using VLANs is not necessarily straightforward, especially for control system support personnel with minimal networking experience. Some organizations have utilized corporate IT teams to supplement the automation support weaknesses with Ethernet networking. The success of this has been questionable due to the fact that IT personnel do not have a thorough understanding of control systems or industrial protocols such as Ethernet/IP. As the extensive use of Ethernet will be new for City maintenance personnel, it is recommended that for the near term, the field networks (Level 0) be effectively isolated as much as possible. This will provide a significant increase in the reliability of these networks, which are critical to the control of the process. This will significantly reduce the probability of an error in switch configuration affecting the real-time control of the equipment by the PLCs.

10.9 Process Networks

10.9.1 General Requirements

Process networks are primarily utilized to interconnect PLCs and the HMI Servers, and will be based on Ethernet technology. The reliability requirements for this network will be significant as it will be utilized for inter-PLC communication and operator interface interaction. The process network will also be utilized to connect HMI clients to the HMI servers, however it is expected that VLAN segregation will be utilized to segregate HMI client communications from inter-PLC communications.

The proposed layout of the process network is highly subject to the configuration of the physical facility, conduit and wiring paths, and distances between nodes. In some cases a star approach might be appropriate, while in other cases a ring approach will be more cost effective. General design requirements are summarized as follows:

- General
  - Administration, security, or video network traffic is not permitted to be on the same physical network as the process network. Complete physical segregation is required.
  - HMI client computers are permitted to be located on the process network, with appropriate VLAN segregation.
- Communication Between Process Areas or Buildings
  - Network connections between significant process areas will be gigabit based (minimum).
  - Connections between physically separate buildings will be fibre-based.
  - Connections between process areas within a common building will be fibre based, except if the distance between process areas is < 90m, the electrical power system is closely coupled, and equipotential grounding is provided between the areas.
  - Communication between buildings and process areas should be redundant. An exemption would be considered for non-critical processes where a long duration outage would be acceptable.
  - Failure of any inter-area redundant cable should not interrupt any communication between any two nodes on the network.
- Communication within Process Areas / Buildings.
  - The requirement for redundancy within each process area is highly dependent upon the specific configuration and availability requirements. Each case must be reviewed and designed appropriately.
  - Failure of any network switch should not cause complete control failure or loss of the HMI view of any major process. For example, a single switch failure should not cause the operator to lose monitoring and control of all raw sewage pumps.
  - In most cases one Ethernet connection to the process will be made per PLC controller. However, Ethernet switching may be utilized local to the PLC to provide additional redundant paths.
  - Traffic between nodes within a single process area should be switched such that it remains within the process area. Avoid switching / routing the inter-process area traffic in other process areas or in a centralized location.
  - Where multicast traffic is utilized, ensure that sufficient physical and logical network segregation is provided in the design to prevent network overload.

10.9.2 Facility Process Network

The facility process network is deemed to be comprised of the network connections that link the process areas and the main server room(s). The server rooms are expected to house the facility HMI servers and would typically be adjacent to the main facility control room. The proposed general layout for the facility process network is shown in Figure 10-10.

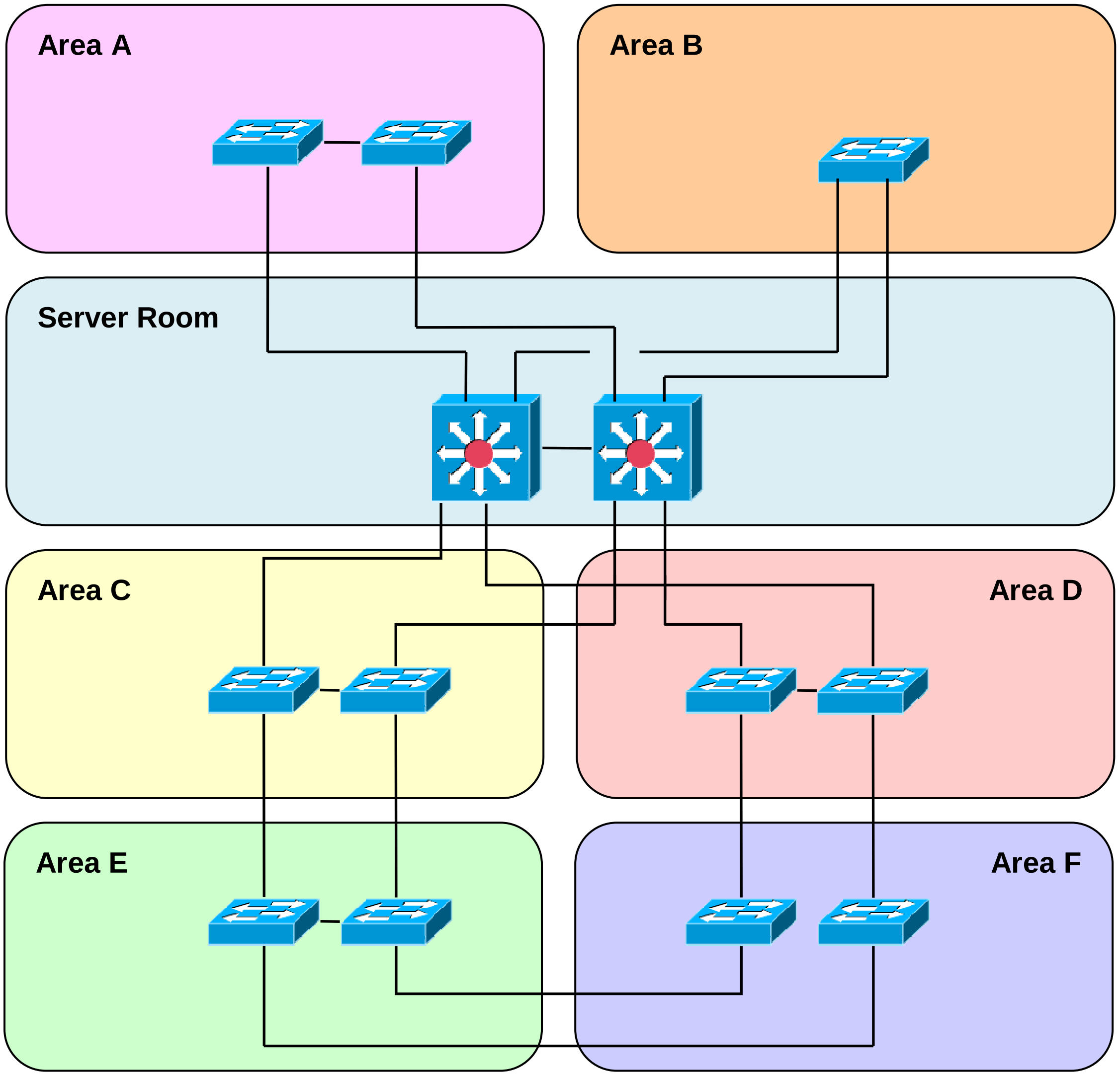


Figure 10-10 : Facility Process Network Overview

Note that there are a few different topologies shown. The server room would contain Layer 3 switches to allow for routing between the LANs and VLANs. The network for Areas C through F is shown as a dual-ring architecture, for ultimate availability. Typically two links could be out of service without affecting the ability to communicate to any node. For some process areas close to the server room, or with a high bandwidth requirement, the architecture shown for Area A would be utilized. Area A utilizes redundant connections dedicated to the process area. While it may appear that the configuration for process Area A is a loop, the link between the Layer 3 switches would be a routed link, and thus it would not be a typical Layer 2 loop. For process areas with limited bandwidth and redundancy requirements, the architecture shown in Area B could be utilized, where a single managed switch is connected to the server room.

Referencing, Figure 10-10, it should be noted that Areas C, D, and E have a link shown between the two switches on the facility network. These links actually turn the dual-link network into a mesh network, but are recommended in any process area where inter-area nodes that need to communicate to each other are connected to different switches. As discussed previously, it is recommended that all inter-process area communications stay within the process area, and don’t travel through other process areas. This reduces bandwidth requirements on the facility network links. While the links between the switches turn the network into a mesh, a single non-looped network would be created by the Rapid Spanning Tree Protocol (RSTP). Typically, one of the loops would be blocked until the other loop failed. However, with the use of VLANs, the links that are blocked can be different for each VLAN, and thus a VLAN for inter-PLC communication could use one ring, and the VLAN for HMI client communication can utilize the other ring, both with failover capability in case of ring failure.

It should also be noted that the use of mesh network configurations require that the Rapid Spanning Tree Protocol (RSTP) is utilized for redundancy switching, rather than proprietary fast ring network failover mechanisms. The advantage of proprietary systems are that some of them can reconfigure the network very quickly (< 100ms), where RSTP can take up to a second to reconfigure. For field networks with I/O, the loss of the network for a second could be an issue, but for the process network, the interruption of the network for a second is not expected to be an issue, and the RSTP will provide appropriate flexibility and adequate recovery times in the event of a failure.

10.9.3 Process Area Network

Within each process area, the configuration of the process network will be highly dependent upon the area's specific requirements, including the number and location of the nodes, and reliability requirements of the nodes. Some potential architectures are shown in Figure 10-11, Figure 10-12, Figure 10-13, and Figure 10-14. Note that the segregated field networks are not shown.

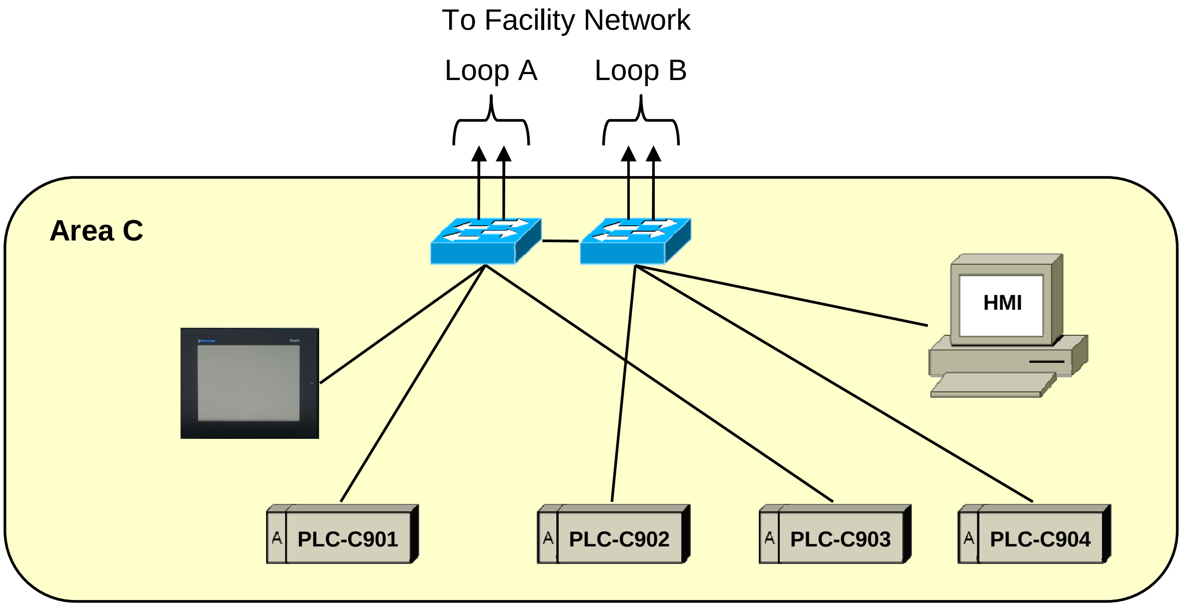


Figure 10-11 : Area Network Example Configuration A

Figure 10-11 shows a potential architecture where single ported devices are connected directly to the main process area switches in a manner that roughly half of the communication would be on each switch. Communication between any area device would be possible via the connection between the two switches. In the event of an area switch failure, approximately half of the nodes would be inaccessible from the network. In the case of PLCs, the control would continue through the segregated field network, but all monitoring and control from the HMI would be interrupted until the switch was repaired. This architecture would be appropriate when:

- The nodes are relatively close to the main area switches, and a temporary cable could be installed within a short period of time in the event of a cable fault.
- The effect of approximately half of the nodes being temporarily out of service is acceptable.

Some specific recommendations regarding use of this configuration are as follows:

- Provide spare ports on each switch, ideally 50% spare capacity at initial construction.
- It is deemed to be acceptable to locate both switches in a common enclosure, provided that the risk of a fire is deemed to be low.

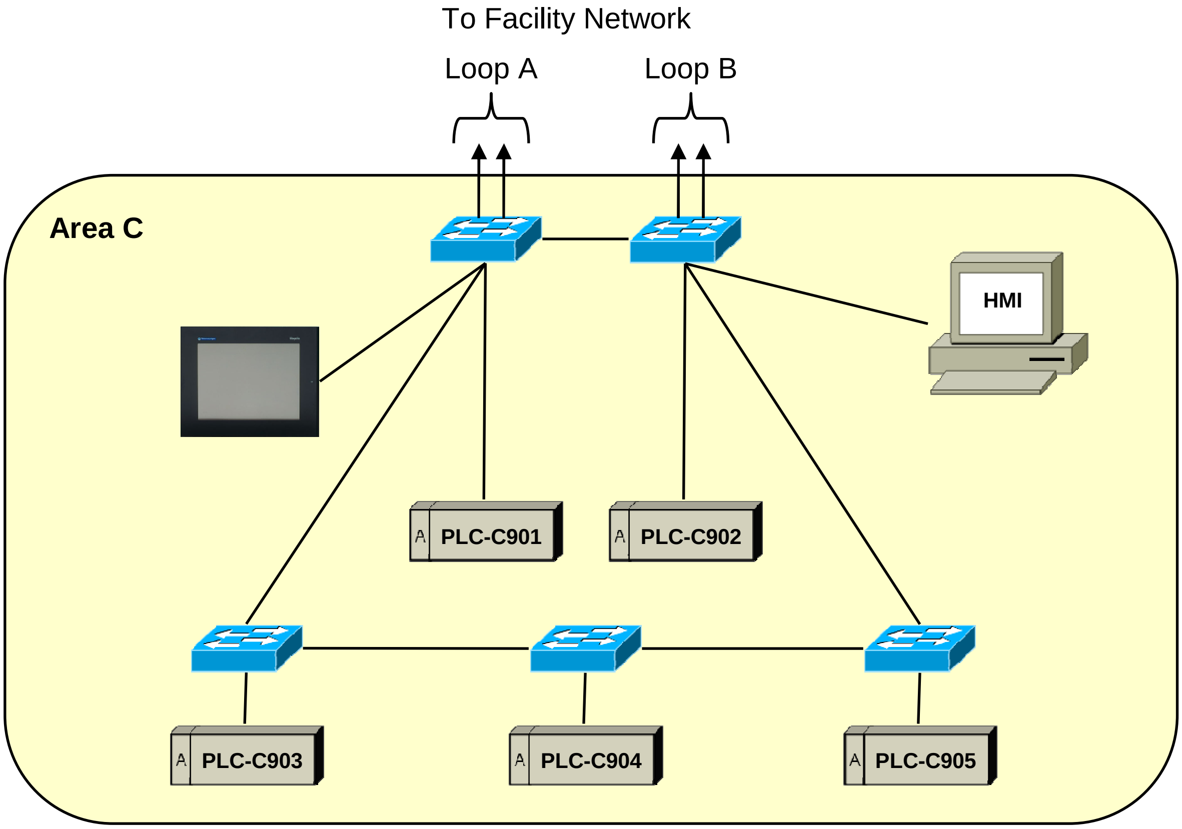


Figure 10-12 : Area Network Example Configuration B

Figure 10-12 shows a potential architecture where some single ported devices are connected directly to the main process area switches in a manner similar to Configuration A, but others are connected in a ring topology, to allow for fault-tolerance of a single network segment failure. The topology is configured in a manner such that communication between the area devices would be possible within the area, without network traffic leaving the area. This architecture would be appropriate when some of the networked nodes require a level of network fault tolerance.

Some specific recommendations for regarding use of this configuration are as follows:

- Provide spare ports on the main switch, ideally 40-50% spare capacity at initial construction.
- Review the installation of the ring to ensure that the location of parts of the ring within corrosive process areas do not significantly reduce the overall ring reliability.

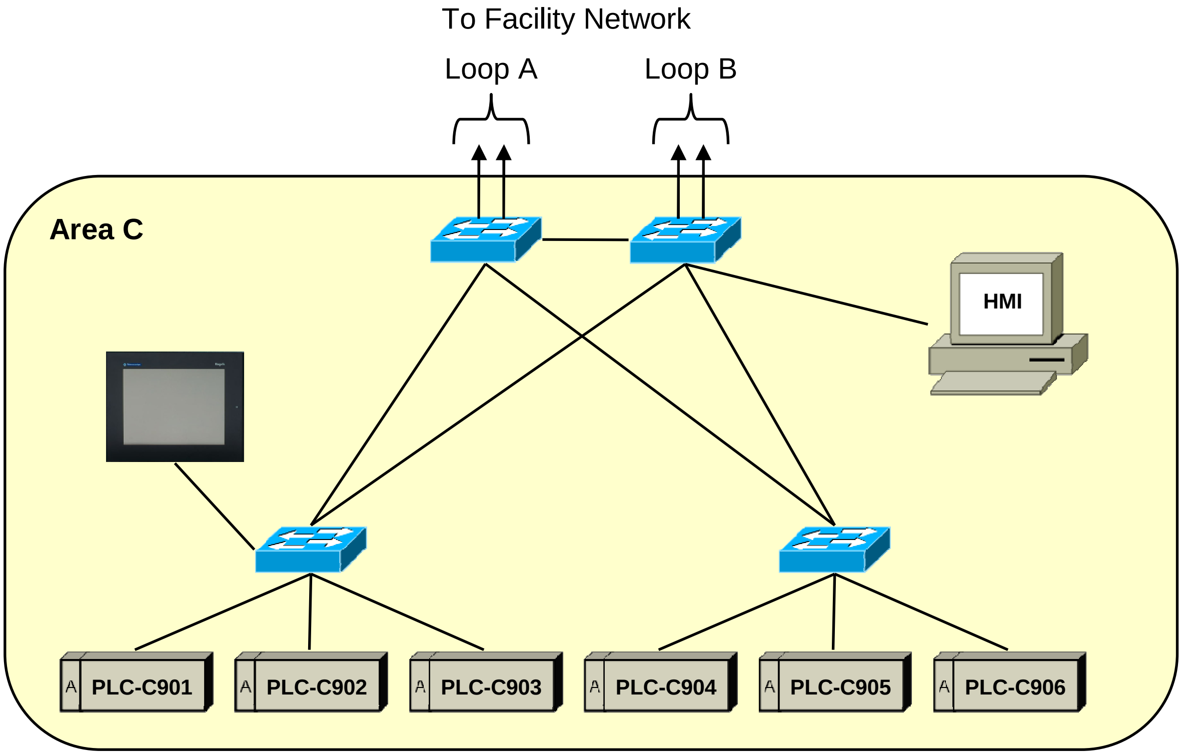


Figure 10-13 : Area Network Example Configuration C

Figure 10-13 shows a potential architecture where small groups of PLCs are connected to a common switch, which is them redundantly connected to both primary process switches in the area. Any failure of the primary process switches does not impact the PLC communications, however failure of one of the lower PLC switches would interrupt communication to three PLCs. This architecture would be appropriate when multiple small PLCs are within close proximity, and the probability of failure of the PLC to switch links is very low.

Some specific recommendations regarding use of the configuration shown in Figure 10-13 are as follows:

- Provide spare ports on the main switch, ideally 25% spare capacity at initial construction.
- Ensure that the failure of the switch connecting the three PLCs results in an acceptable process condition.

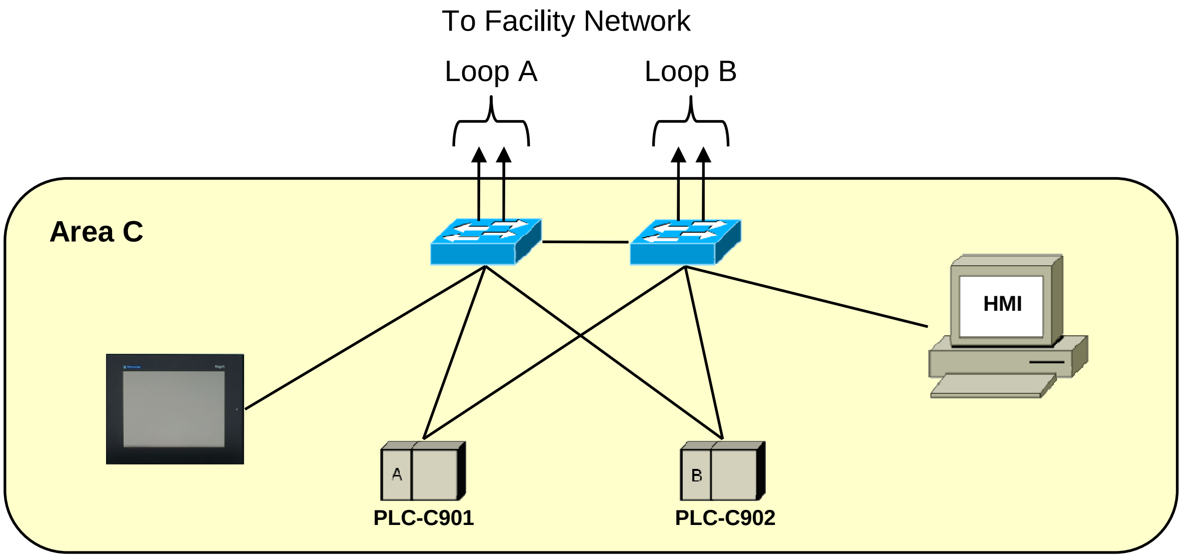


Figure 10-14 : Area Network Example Configuration D

Figure 10-14 shows a potential architecture where redundant controllers are connected redundantly to the two process switches. Any single failure of the primary process switches or PLCs does not affect the control of the shown PLCs. This architecture would be appropriate for critical process control.

Some specific recommendations regarding use of this configuration are as follows:

- Provide spare ports on the main switch, ideally 25% spare capacity at initial construction.
- Ensure that the routing of the cables to the two switches is independent, such that a single point of mechanical failure does not interrupt all communications.

10.10 Network Selection Criteria

In some cases it may not be clear whether to connect a device to the process network or a field network. While specific evaluation is required in each case, general guidelines are presented in Table 10-4.

Table 10-4 : Network Selection Criteria

Criteria	Process Network	Field Network
Is the data critical for real-time control?	No	Yes
Is the majority of the device data required by the PLC controller or the HMI?	HMI	PLC
Latency Requirements	> 100 ms	< 100 ms

Note: The criteria must be evaluated as a set, as the answer for a single criterion is not necessarily the appropriate selection.

For example, a potentially difficult choice might be whether to connect a gas detection controller to the process network or a field network. Most of the data would be utilized by the HMI for trending and alarming and all safety critical annunciation and control would be hardwired. However, it may be desired to increase the ventilation rate in an area if the gas levels start to approach safety setpoints, and this data would be required by the PLC. Based upon the criteria identified in Table 10-4, it is deemed that the preferable network would be the process network, as short latency is not required, and most of the data is utilized by the HMI.

10.11 Master Controllers

10.11.1 Potential Configurations

The proposed architecture utilizes multiple non-redundant PLCs to control parallel process streams, in such a manner that failure of a single PLC for a short duration is a manageable situation. There are cases where master control is required to coordinate between parallel processes. A good example is raw sewage pumping. Assuming that there are four VFD driven raw sewage pumps, with P-G101, and P-G103 connected to PLC-G901 and P-G102 and P-G104 connected to PLC-G902. There are two level sensors for the wet well that are utilized by the master controller to control the pumps. Four options for locating the master control are:

- In a separate master PLC with redundant controller
- In a separate master PLC with a single controller
- In either of the pump PLCs, PLC-G901 or PLC-G902
- In both of the pump PLCs, PLC-G901 and PLC-G902, with methods of selection between the active master controller.

The ultimate objective of potentially placing the master control in a master PLC is to achieve the highest level of reliability. Given that a single failure should not interrupt all pumping, at first glance it appears that utilization of a separate master PLC with redundant controllers may be an effective solution. While this solution would provide a high level of reliability, it may be overkill in some cases.

Locating the pump master control in a separate master PLC with a single controller is acceptable as well, provided that appropriate backup systems are designed into the automation system. Under this scenario, it is proposed that each pump would have three modes of control: *Auto Master*, *Auto Independent*, and *Manual* via the HMI. In *Auto Master* mode, the separate master controller would provide pump on/off signals and pump speed commands. In *Auto Independent* mode, the pump PLC would locally and independently determine the pump operation, based upon an independent connection to a level sensor. It is deemed that this independent control, while not ideal, would be sufficient for short duration operation in the event of the master controller failure.

The third control option is to locate the master control logic in one of the pump PLCs, say PLC-G901. In the event of the master PLC failure, the alternate PLC would place the pumps into an *Auto Independent* mode, as discussed above. This is an acceptable scenario, provided that maintenance or failures of PLC-G901 would not be more frequent than for a separate master PLC.

The fourth control option is to locate the master control logic in both of the pump PLCs and allow for automatic selection of the active master control logic PLC. In the event of the master PLC failure, the alternate PLC would automatically take over as the master controller. In this specific example, this would be a potential solution, however it should be noted that the additional programming complexity must be weighed against the advantages of this configuration.

10.11.2 Area Control Philosophy

It is recommended that the concept of Area Control be adopted, where all controllers for a process area are physically located within the process area to be controlled. All PLC controllers for an area should ideally be dedicated to the process area. Where a process area is small, it could potentially be covered completely by one or more of another area's PLCs. However, it is recommended that control of a process area by PLCs both within the process area and external to the process area, be avoided. This principle is depicted in Figure 10-15.

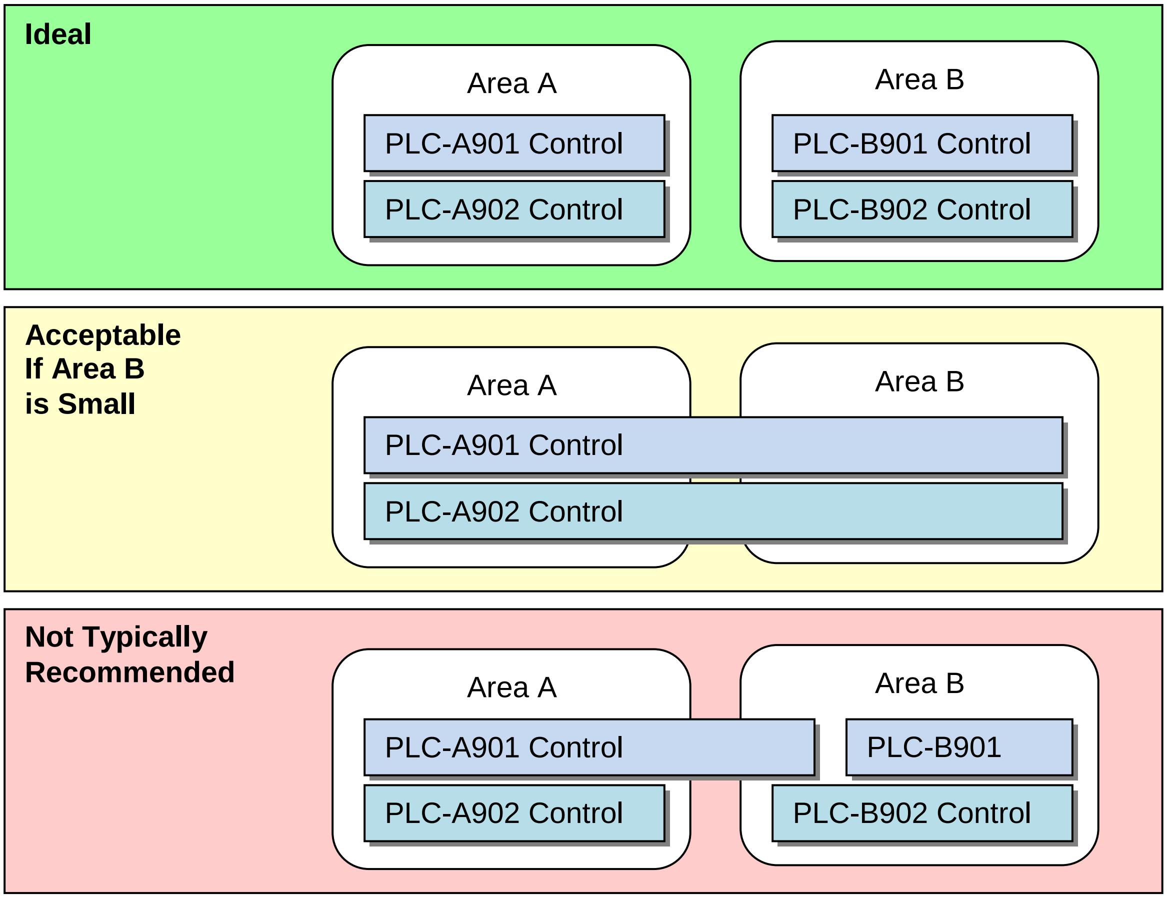


Figure 10-15 : Area Control Philosophy

The area control philosophy is recommended due to the following:

- It avoids cases where power system issues in one process area can affect the other process area through the common control system.
- Reduction of copper I/O wiring between process areas reduces ground loop issues.
- Network communications are typically more straightforward to design and isolate as required.
- It slightly reduces the reliability requirement associated with the facility process network's inter-area links.
- The linking between process and PLC processors is more obvious and clear to operations and maintenance personnel. If a PLC that controls a portion of another process is taken out of service, and personnel do not remember that it controls a portion of another process, there could be significant disruption to the operation of the facility.

It is noted that there could be justifiable exceptions to the above recommendation where a portion of a process in one area is very tightly coupled with another process area, however these cases should be appropriately justified and documented.

10.12 Server Room

The server room is where the HMI servers, historian, and other servers would be located. It is expected that this would be located within the Administration area of the facility, and adjacent to the primary control room. Refer to Section 14.0 for numerous recommendations that apply to the server room(s) at each facility.

10.13 Example PLC Architecture

10.13.1 Process Requirements

This section presents a potential PLC architecture for an example Primary Clarifier Process. The example system process requirements are summarized as follows:

- Four Primary Clarifier Tanks (1 – 4) with
  - Travelling bridge rake system to collect sludge and scum.
  - Influent sluice gate on each tank, controlled by an electric actuator.
  - Discharge sluice gate on each tank, controlled by an electric actuator.
  - Scum collector rake on each tank.
  - Five sludge hoppers on each tank.
- On each sludge hopper (total 20), an automatic on/off valve is provided to sequence sludge pumping.
- One sludge pump is provided per clarifier.
- One scum pump is provided for Clarifiers 1 & 2, and a second scum pump is provided for Clarifier 3 & 4. There are manual interconnects to the sludge pumps to allow the scum to be pumped via the sludge pumps, if the scum pump is out of service.
- Four HVAC supply air handlers and eight exhaust fans service the tank area. Two supply air handlers and four exhaust fans are associated with Clarifiers 1 & 2 and the remaining service Clarifiers 3 & 4.
- One HVAC air handler services the pump galleries.
- Miscellaneous small HVAC systems for the electrical and control rooms, and other spaces.

The process availability requirements for this sample process are defined as follows:

- Two of the four tanks are required to meet minimum requirements for dry weather flows.
- All four tanks are required to meet minimum requirements for wet weather flows.
- Interruption of the sludge and/or scum collection system on any operating tank is acceptable for a maximum of four hours.
- Interruption of ventilation at any time will require that personnel leave the area. Total interruption of ventilation for longer than 30 minutes is not deemed to be acceptable. Operation with half of the ventilation is deemed to be acceptable for a day, provided special precautions are taken for personnel in the space.

The electrical system is set up with the following:

- Two intelligent MCCs are provided with separate feeders, and the loads split as follows:
  - MCC-P01
    - All Clarifier 1 loads including electric actuators, travelling bridge, scum collector, and sludge pump.
    - All Clarifier 3 loads including electric actuators, travelling bridge, scum collector, and sludge pump.
    - The scum pump for Clarifiers 1 & 2.
    - One of the supply fans and two of the exhaust fans for Clarifiers 1 & 2.
    - One of the supply fans and two of the exhaust fans for Clarifiers 3 & 4.
  - MCC-P02
    - All remaining loads not serviced by MCC-P01.
- One intelligent motor control center, MCC-P09E, powered from a transfer switch that switches between MCC-P01 and generator backed power, to feed essential loads. Essential loads powered are:
  - AHU-P601E – one of the air handlers supplying air to the Clarifier 1 and 2 area.
  - EF-P611E and EF-P612E, two of the exhaust fans for the Clarifier 1 and 2 area.
  - AHU-P631E – one of the air handlers supplying air to the Clarifier 3 and 4 area.
  - EF-P641 and EF-P-642E, two of the exhaust fans for the Clarifier 3 and 4 area.

Note: This example assumes that standby generation is not required to maintain the actual process equipment during a power failure.

10.13.2 Proposed Automation Architecture

The automation system is proposed to be configured with three single controller PLCs controlling the majority of the process, and additional micro PLCs located on each of the primary clarifier travelling bridges. A brief description of the control architecture is as follows:

- The first controller, PLC-P901, controls:
    - Clarifiers 1 and 3
    - Approximately half the HVAC system, including the essential HVAC leads.
- The first controller, PLC-P902, controls:
    - Clarifiers 2 and 4
    - The other half of the HVAC system
- The third controller, PLC-P905, controls the miscellaneous HVAC systems.
- Four remote I/O nodes in the pump gallery, one per clarifier, which connect the following:
    - Sludge hopper valves
    - Sludge pump instrumentation
- The sludge hopper valves would have a local operator station with an Open/Close/Remote switch per valve.
- Each travelling bridge would be controlled by a micro PLC, communicating over wireless Ethernet. These PLCs are identified as PLC-P201 through PLC-P204. These PLCs could potentially be hardened to provide longer life within the corrosive environment.
- All MCC intelligent motor starters configured to stay in last state upon communication failure with the PLC except:
    - Scum pumps and sludge pumps, which would stop upon a communication failure

The proposed network architecture for this example primary clarifier system is shown in Figure 10-16. For this application, it is proposed that all field networks are Ethernet based. The architecture presented would work for an Ethernet/IP, Modbus TCP, or a PROFINET network. Each MCC would have a dedicated managed network switch, which would allow for redundant communication with the network switches NSW-P991 and NSW-P992. The remote I/O nodes would be connected via a ring architecture to the same switches. The connection of the three major PLCs is proposed to be via a single network link to one of the field network switches. Failure of the network cable between the switch and the PLC would lead to the same consequences as PLC failure, which are deemed to be acceptable (See Section 10.13.3).

As wiring of network connections to the travelling bridges has complexities, it is proposed that wireless communications are utilized to the travelling bridge PLCs. The consequences of failure of the wireless connection are minimal, with loss of monitoring, and the scum and sludge systems would not know when the travelling bridge completed a cycle. However, it would be straightforward to include PLC logic to initiate sludge pumping at a minimum interval, upon failure of wireless communication.

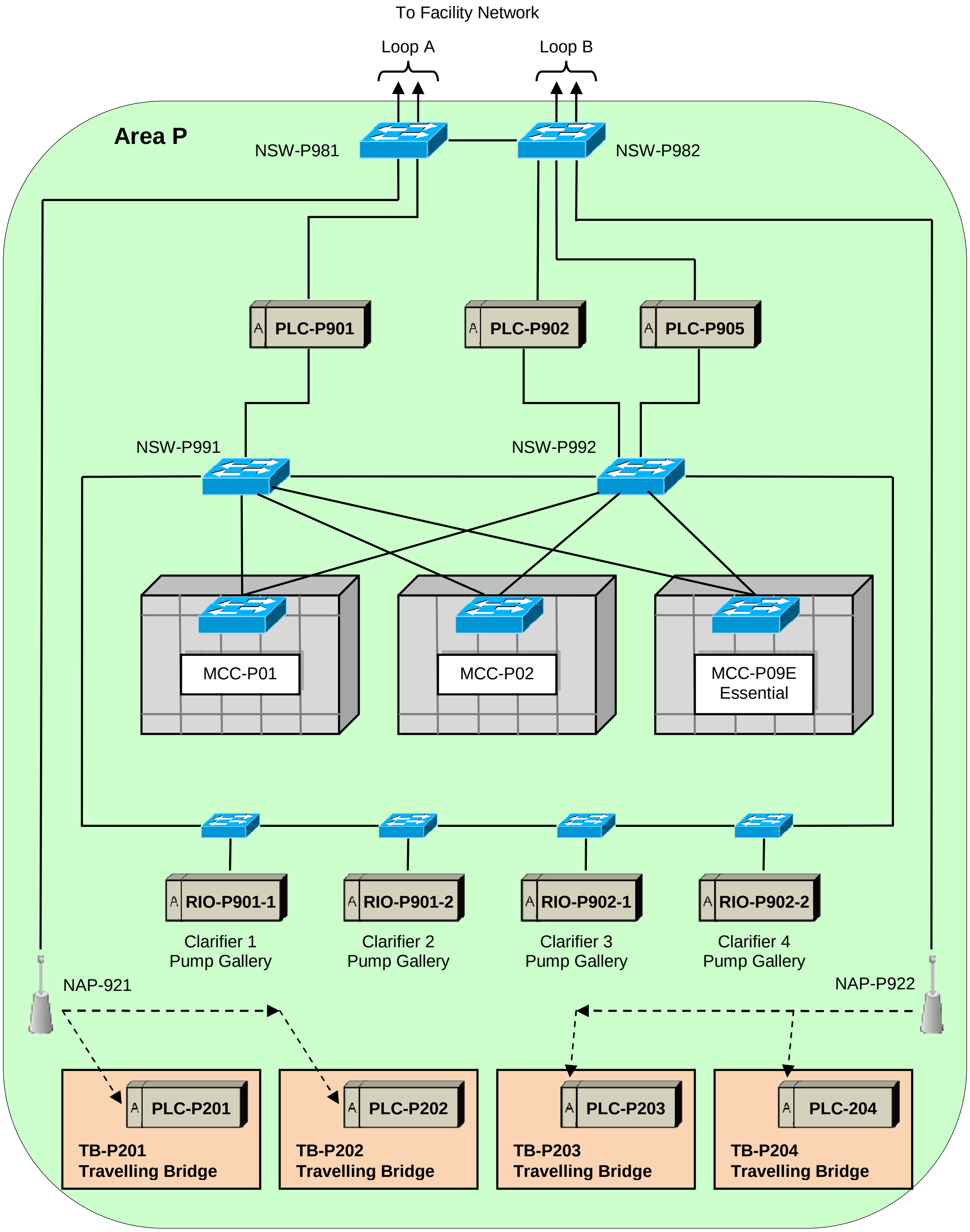


Figure 10-16 : Example System Network Architecture

10.13.3 Failure Analysis

In the event of a failure, it is critical that the process operation exceeds the minimum process requirements. In the event of a PLC-P901 failure, Clarifiers 1 and 3 equipment would be out of service. Flow through the clarifier would continue, although sludge and scum collection would be interrupted. As per the stated minimum process requirements, this is acceptable provided that the length of interruption would be less than four hours. It is reasonable to expect that most PLC failures can be addressed within four hours and thus PLC failures that exceed four hours should be quite rare. In addition, operators would have the option to locally control the sludge and scum systems, which could potentially extend the acceptable failure window.

A review of the proposed Ethernet communication network was also performed. While there are failure modes which could shut down equipment, the consequences associated with failure are deemed to be acceptable. A summary of the failure modes is presented in Table 10-5.

Table 10-5 : Example System Failure Analysis

Item	Failure	Primary Consequence	Repair Time	Manual Local Control
PLC-P901	Controller failure	Clarifier 1 and Clarifier 3 sludge and scum collection interrupted. Clarifier ventilation fans would continue operating in the last state, but clarifier ventilation heating controls would go to the fail-safe position.	4 h	Y (1)
PLC-P902		Same as PLC-P901, except Clarifier 2 and Clarifier 4	4 h	Y
PLC-P903		Miscellaneous ventilation motors would keep running (last state). Ventilation heating controls would go to the fail-safe position.	4 h	Y
PLC-P201 PLC-P202 PLC-P203 PLC-P204		Failure of the travelling bridge (single failure).	4 h	Y
RIO-P901-1 RIO-P901-2 RIO-P902-1 RIO-P902-2	Remote I/O Failure	The automatic sludge and scum collection of a single clarifier would be interrupted.	4 h	Y
MCC-P01	Network Failure	Related ventilation equipment would keep running (last state). Clarifier 1 and Clarifier 3 sludge and scum collection interrupted.	4 h	Y
MCC-P02	Network Failure	Related ventilation equipment would keep running (last state) until stopped locally. Clarifier 2 and Clarifier 4 sludge and scum collection interrupted.	4 h	Y
MCC-P03E	Network Failure	Related ventilation equipment would keep running (last state).	4 h	Y
NSW-P981	Network Switch Failure	Loss of HMI monitoring for PLC-P901 equipment and Clarifier 1 and 2 travelling bridges.	4 h	Y
NSW-P982		Loss of HMI monitoring for PLC-P902 and PLC-P903 equipment and Clarifier 3 and 4 travelling bridges.	4 h	Y
NSW-P991		Same as failure of PLC-P901	4 h	Y
NSW-P992		Same as failure of PLC-P902 and PLC-P905 combined.	4 h	Y
NAP-P921 NAP-P922	Network Failure	Failure of the wireless link to the travelling bridges would cause limited control degradation for the associated clarifiers.	8 h	Y

Notes:

1. *The manual control capability for the heating control is expected to be limited.*

10.14 Application Software Logic

The major PLC manufacturers currently support most, if not all of the IEC 61131 languages, which are identified and briefly described in Table 10-6.

Table 10-6 : IEC 61131 Languages

Language	Description	Ideal Usage
Ladder Logic	Control logic is graphically represented using rungs of relay logic that are similar to electrical control diagrams.	Simple, discrete logic such as motor control
Function Block Programming	Control logic is graphically represented using blocks with defined inputs and outputs, and the blocks are interconnected with connection lines. Logic is encapsulated within the function blocks.	Analog control loops
Structured Text	A text based programming language that resembles C and Pascal.	Calculations, if/then scenarios, and complex logic
Instruction List	A low level language that uses basic instructions, and resembles assembly language.	Logic that requires a high rate of execution
Sequential Function Chart	Control logic is graphically represented in a flowchart type manner, with discrete steps, actions and transitions. The details of the logic associated with each state must be programmed in one of the other languages.	State engine logic

The City's current DCS programming system is based upon a function block diagram style language, while ladder logic has been historically used in PLCs, and is well understood by most personnel. Structured text is significantly less common in control system programming, but would be quickly understood by anyone with some PC software programming experience. Instruction List is a very low level language and would not be frequently utilized, as it is more difficult to program and read. Sequential Function Chart is not commonly utilized as the associated functionality can be programmed within other logic. However, Sequential Function Chart can provide a benefit in the manner state engine control logic is presented to the programmer, if the control system vendor provides a good implementation.

It is generally recommended that most programming logic utilize ladder logic for discrete control and function block programming for control loops. Where complex logic is required that would not be straightforward to implement in ladder logic or function block, the use of structured text would be appropriate. The use of Sequential Function Chart is dependent upon the vendor's implementation of the logic, and it would only be utilized for state logic. Finally, it is recommended that the use of instruction list not be permitted.

It should also be noted that some vendors may offer C or other high level language support. It is recommended to avoid other add on languages where possible, as the set of recommended IEC 61131 programming languages provide sufficient diversity to cover all typical applications.

10.15 Automation System Vendor Selection

The selection of a control system vendor is a critical task in the overall design process. It is recommended that this be completed prior to the initiation of detailed design, to ensure that the automation detailed design can be implemented based on the specifics of the control system. As there are significant differences between various vendor's products, the detailed design of control systems without vendor selection would be more difficult and would result in generalizations that would not be ideal or acceptable.

The City of Winnipeg has procurement policies that dictate requirements regarding competitive procurement. At this time, it is understood that the City of Winnipeg has a general procedure for equipment standardization utilizing the Bid Opportunity / Request for Proposal process, however this procedure has never been implemented. Thus, it is expected that this project will require significant discussion with the City of Winnipeg Materials Management division regarding the specific details of implementation.

The procurement process for the PLC and HMI is expected to be significantly more complex than for the remaining components. This equipment will provide the basis for the control system for the facilities and therefore the selection of the appropriate system is critical.

It is anticipated that the selection of the PLC and HMI will include a two-stage evaluation process. After the bidders' proposals are received, the first stage of evaluation will eliminate obvious non-contenders and select two or three preferred bidders. Experience has shown that the most effective approach for selection, to fully flush out vendor system capabilities and issues, will require that the preferred bidders to set up a demonstration system. This demonstration system will then be the basis of the 2nd stage of evaluation. To provide incentive for bidders, it may be required to provide a fixed payment to all preferred bidders to partially compensate their costs for setting up the demonstration system.

One of the primary issues of concern associated with the standardization of the PLC and HMI equipment will be the future purchase costs after selection. The expansion and upgrade of the wastewater treatment plants will occur over a number of years into the future. It would therefore be desirable to have to the greatest extent possible, a reasonable level of price certainty for a period of time that would, at the least, span the period of expansion and possibly even beyond.

A feasible means for determination of comparable equipment costs could be achieved through the configuration of a “prototype plant” arrangement. This would provide a comparable basis to the present wastewater treatment plans, and would provide a reasonable indication of expected quantities and system configuration to provide appropriate context to vendor pricing. It is expected that this approach would ultimately lead to reasonably representative unit pricing, which could be then used as the basis for price comparison with actual purchases to ensure future cost certainty. It is also expected that the vendors will be requested to submit proposals regarding escalation for future years and the vendor’s proposals would be evaluated on the level of cost certainty provided.

A sample of some mandatory criteria for the evaluation of control system vendors is provided in Table 10-7. Note that this list is not exhaustive, and would need to be fleshed out during the development of the control system specification. In addition, a sample of high level evaluation criteria is presented in Table 10-8. The full set of bid evaluation criteria would be developed as part of the selection process, and it is recommended to make the criteria sufficiently comprehensive to address all aspects of the control system, without becoming too detailed that the evaluator flexibility is restricted. For example, if it is discovered during the evaluation that a vendor has a useful feature, this should not be excluded from the evaluation simply because there was not a question / category for this item. It is expected that significant additional discussion on the detailed control system specification and evaluation will be required.

Table 10-7 : Sample Mandatory Criteria for Automation Vendors

Item	Criteria
1	Industrial-grade controls
2	Twenty years of experience in automation system manufacture.
3	Ethernet communication capability.
4	Support for all IEC61131 Programming languages except Instruction List.
5	Hot standby capability
6	Modular I/O
7	Support of both local and Ethernet remote I/O architectures
8	HMI System must support Client Server Architecture and Redundant Servers
9	HMI System must support Web Server
10	Historian Support with Central Historian Server

Table 10-8 : High Level Bid Evaluation Criteria

Item	Description	Score Evaluation
General		
G1	Price	Quantitative Assessment Based on Sample System
G2	Price Certainty	Qualitative Assessment Based on Bidder Proposal
G3	Reference Projects	Based on references.
G4	Local Service and Support Network	Assessed based upon information provided by vendor.
G5	Comprehensiveness of Documentation Library	Assessed based upon information and online access provided by vendor.
G6	Service Model – Are multiple vendors available to service and program the system.	Assessed based upon openness of service model.
Technical		
T1	Power Supply Redundancy	Qualitative assessment.
T2	Controller Redundancy Capability	Qualitative assessment.
T3	I/O Module Flexibility, Type, and Capability	Qualitative assessment.
T4	Processing Power	Based on Evaluation System
Communications		
C1	Support of Ethernet/IP, Modbus TCP, and PROFINET	Based upon number natively supported. Less points for Modbus TCP.
C2	Fieldbus Support	Assess points per fieldbus. Not all fieldbuses will be scored equally.
C3	Potential Redundancy and Flexibility of Communication Modules	Qualitative assessment.
C4	Smart Field Device Integration	Qualitative assessment.
HMI System		
H1	Proposed System Configuration and Limitations	Qualitative Assessment of Evaluation System
H2	Templating / Object Graphic Reuse Capabilities	Qualitative Assessment of Evaluation System
H3	Historian Capabilities	Qualitative Assessment
H4	Reporting Capabilities	Qualitative Assessment
H5	Central Historian Server Capabilities	Qualitative Assessment
H6	Web Server Capabilities	Qualitative Assessment

Item	Description	Score Evaluation
H7	Asset Management System Integration	Qualitative Assessment
H8	Enterprise System Integration Capabilities	Qualitative Assessment
H9	Support for Virtualization and Terminal Services.	Qualitative Assessment
H10	Support for Portable Operator Devices	Qualitative Assessment
H11	Ease of use	Qualitative Assessment of Evaluation System
Control Logic Programming		
P1	Features	Qualitative Assessment of Evaluation System
P2	Advanced Features, such as a Logic Version Control System	Qualitative Assessment of Evaluation System
P3	Ease of Use	Qualitative Assessment of Evaluation System
P4	Simulation Capabilities	Qualitative Assessment of Evaluation System

11.0 MIGRATION STRATEGY

11.1 Existing DCS

11.1.1 Existing Installation

The existing DCS at the three facilities is an ABB/Bailey Infi90 DCS system. The current system has provided reliable service since installation for 25 years, however some parts of the system are nearing end of life. The age of the installed systems are summarized in Table 11-1.

Generally, the condition of the components within the NEWPCC facility are believed to be better than the SEWPCC and WEWPCC facilities, as a reasonably comprehensive upgrade of the NEWPCC facility DCS was performed in 2005. The upgrade included power supplies, communications modules, and controllers. It is generally expected that the NEWPCC DCS hardware should operate reliably for a period of ten years from the date of the upgrade, which is to 2015, prior to the occurrence of any significant component end of life issues.

Table 11-1 : Existing DCS Age

Facility	Process Area	Power Supplies	Processors	I/O	Notes
NEWPCC	Main Building	2005	2005	1990	Upgrade in 2005
	Grit Building	2005	2005	1990	
	Primary Clarifiers	2005	2005	1986	
	Reactors	2005	2005	1986	
	Secondary Clarifiers	2005	2005	1988	
	UV Disinfection	2006	N/A	2006	Constructed 2006
	Digesters	2005	2005	1987	Upgrade in 2005
	Boilers	2005	2005	1987	
	Dewatering	2005	2005	1990	
	Nitrogen Removal	2008	2008	2008	Constructed 2008
SEWPCC	Admin Building	1992	2011	1992	Processors replaced as part of Reliability Upgrades
	Grit Building	1993	2011	1993	
	Service Building	1993	1993	1993	
	Primary Clarifiers	1993	1993	1993	
	Reactors	1992	1992	1992	
	Secondary Clarifiers	1992	1992	1992	
	UV Disinfection	N/A	N/A	N/A	PLC Control
WEWPCC	Perimeter Road (PCU 4)	1993	1993	1993	
	Headworks / Primary Areas (PCU 1)	1993	2008	1993 / 2008	Upgrades as part of WEWPCC BNR Upgrades
	Secondary Clarifiers (PCU 2)	1993	2008	1993 / 2008	Upgrades as part of WEWPCC BNR Upgrades. HPG800 modules added ~2011.
	Utilities (PCU 3)	1993	1993	1993	

Notes:

1. *The dates in the document reflect the installation date of the majority of modules. There are exceptions due to module replacements.*

11.1.2 Manufacturer Support of the Existing DCS

The existing manufacturer (ABB) support for some of the critical existing DCS components is summarized in Table 11-2. The manufacturer definitions for the various product lifecycle phases are as follows:

- *Active* – The product is actively manufactured, marketed, and sold.
- *Classic* – The product is no longer marketed or sold, but spare parts continue to be manufactured.
- *Limited* – Spare parts may be available from existing stock, or parts can be repaired. ABB support is on a best effort basis.
- *Obsolete* – The product is no longer supported.

Table 11-2 : Support for DCS Components

Component	Lifecycle Status	Support Status	Notes
MFP Processors	Limited	OK	MFP Processors can be readily replaced with BRC410 processors.
BRC Processors	Active	OK	
Rack I/O	Limited	OK	Numerous modules are in the Limited phase, but can typically be swapped out for equivalent current modules in the Active phase.
	Active	OK	
800 series I/O	Active	OK	
Weidmuller based termination boards	Classic	Issue	ABB will move these products into the Limited lifecycle stage in December 2012.
Cabinet Power Supplies (MPS1)	Limited	Recommend Upgrade	Upgrades to MPSIII power supplies are recommended.
Composer	Active	OK	
PCV	Classic	Recommend Upgrade	ABB has PGP (S+) software as an upgrade option.

Note: The above data is based upon ABB documentation.

While some components are in the *Limited* lifecycle stage, the manufacturer has upgrade paths available to provide continued support for the products. It should be noted that ABB has a policy of providing spare parts for a minimum of ten years after the product leaves the *Active* lifecycle stage.

There are DCS components at all three wastewater treatment facilities that are no longer in the *Active* production phase. The most significant components that should be considered for upgrade are the rack power supplies at the SEWPCC and WEWPCC facilities and the PCV HMI system at all three facilities. However, there may be other components requiring upgrade to allow for continued service, and it is recommended to perform a review of the DCS system at each facility to ensure that the DCS can provide continued service until replacement is planned. This proposed work is summarized in Section 21.1.

11.1.3 Existing DCS HMI

The current PCV HMI system is essentially obsolete and few compatible computer hardware spare parts are available. While ABB has, as of May 2011, officially classified the PCV product in the *Classic* lifecycle stage, new hardware for the software version that the City owns (version 5.4) can no longer be purchased. The latest version of PCV, 5.5b, which the City does not own, can be installed an HP Z400 computer, however ABB has advised as of August 2012 that this computer series is in the final production run. Specific details regarding the PCV HMI software and proposed upgrade paths are discussed in the *Wastewater DCS HMI Evaluation* report prepared by SNC-Lavalin Inc. and dated August 2010.

The current PCV hardware is past end-of-life and is not expected to remain in a maintainable state for long. Thus, it is recommended to initiate replacement of the HMI as soon as possible. The replacement should be initiated at the NEWPCC and WEWPCC facilities. Given that a new control system will be initially installed at the SEWPCC facility, a potential option would be to maintain SEWPCC PCV operation until the upgrades, by utilizing the scavenged computer hardware from the NEWPCC and WEWPCC to maintain the operation of the SEWPCC PCV installation. However, further review of the overall schedule is recommended prior to accepting this option.

11.2 DCS Replacement Schedule

The recommended scheduling for replacement of various DCS components is identified in Table 11-3 below.

Table 11-3 : Recommended DCS Replacement Schedule

Facility	Completion Date	Work	Notes
SEWPCC	ASAP	Obtain PCV hardware spares via HMI upgrades at NEWPCC & WEWPCC or alternately replace the HMI system.	
	2013 Q3	Perform a review of the SEWPCC DCS and upgrade as required to maintain operation until replacement.	
	2016	Perform migration to the new automation system. See Section 11.3.	Dependent upon SEWPCC upgrade schedule.
NEWPCC	ASAP	Replace the PCV HMI System	
	2014 Q4	Perform a review of the NEWPCC DCS and upgrade as required to maintain operation until replacement.	
	TBD	Perform migration to the new automation system. See Section 11.3.	Dependent upon the NEWPCC upgrade schedule.
WEWPCC	ASAP	Replace the PCV HMI System	
	2013 Q3	Perform a review of the WEWPCC DCS and upgrade as required to maintain operation until replacement.	
	TBD	Perform migration to the new automation system. See Section 11.3.	Dependent upon the WEWPCC upgrade schedule.

11.3 Overall Migration Strategy

The migration of the existing DCS to the new control system will require significant planning and coordination. There are two overall potential strategies for migration, which will be identified as HMI Lead and Parallel Swing-over Implementation.

11.3.1 HMI Lead Migration

Under the HMI Lead Migration strategy, the DCS HMI system would initially be replaced with a new HMI that can communicate with the existing Infi90 DCS. All the graphics, trends, alarms, etc would be migrated and commissioned to provide the existing functionality on the new HMI. The second stage of the migration would be to install the new PLC controllers and connect and commission the associated HMI interfaces. Finally, the Infi90 DCS controllers would be migrated to the new PLC controllers.

Note: This approach is based upon the replacement of the existing PCV HMI software with the HMI software selected for the final configuration of the automation system. This section does not discuss or preclude the potential for replacement of the PCV HMI software with ABB's S+ (PGP) HMI product, which has migration capabilities from the existing PCV HMI. See Section 20.2.

The primary advantage to this approach is that it allows for an early replacement of the obsolete PCV HMI, without throwing away any HMI investment. It also allows for a relatively expedient HMI conversion, and thus the Operations personnel will continue to have a single HMI system with which to view and operate the facility.

However, one disadvantage of this approach is that it would limit the selection of the new HMI to a few vendors that have proven solutions for Infi90 communications. The HMI vendors with known solutions are ABB, Siemens PCS, Wonderware, and Emerson DeltaV.

The second disadvantage to this approach is that it is potentially too late to implement. Given that the existing HMI is obsolete and required immediate replacement, migration of the HMI with the associated development and commissioning phases would take a significant amount of time that is not available. The only viable migration option at the moment is to the ABB PGP (S+) HMI product, which has a PCV conversion application that requires minimal development. However, the City's long term choice for an HMI package is not likely to be the ABB PGP product, reducing the viability of this approach.

It should also be noted that this approach would have higher value if the modification requirement to the existing facilities are limited. While the detailed scope of upgrades at the facilities is not known, it is expected that the requirement for modification to the control systems of the existing facilities will not be insignificant.

11.3.2 Parallel Swing-over Migration

The parallel swing-over migration is the preferred alternative given the current situation. In this scenario, the new control system would be set up in parallel with the existing DCS system, with systems and equipment transferred over from the existing DCS to the new control system one at a time.

The primary advantage to this scenario is that it eliminates the requirement to set up the new HMI (selected for the final configuration) to communicate with the existing DCS, which simplifies the migration process and also the responsibility associated with the new control system.

Note: This approach does preclude the potential for the temporary replacement of the PCV HMI software with ABB's S+ (PGP) HMI product, which has migration capabilities from the existing PCV HMI. See Section 20.2.

The most significant weakness associated with this scenario is that the operator will have two HMI systems to utilize. Initially the DCS HMI will control the entire facility, while over time, the monitoring and control will be migrated from the DCS HMI system to the new control system HMI. This migration could extend over a significant period of time, and be a significant source of frustration for Operations personnel. The City has expressed the desire that the migration period should be limited to a maximum of 12 months. It is also noted that the DCS HMI must remain active until the end of the entire migration process.

This alternative is preferred over the HMI Lead Migration strategy as it does not require the new HMI system to communicate with the existing DCS, which can limit choices in selection, and also may require significant HMI commissioning of DCS controls that will be decommissioned within a short timeframe.

This approach is expected to be implemented on an area basis starting with the SEWPCC as the upgrade of this plant is understood to be scheduled for implementation shortly. This is reflected in the DCS replacement schedule described in Section 11.2.

11.4 DCS Migration Details

11.4.1 HMI Migration

As it is planned that there will be both a DCS HMI and a new HMI system active at the facility simultaneously, it is recommended that the upgrade designs include sufficient control room space in the main control room for dual HMI computer systems and operator terminals. Where operator terminal space will not be available in area control rooms, it is recommended that use of KVM (Keyboard-Video-Mouse) technology be considered to reduce desktop space. At minimum, one terminal must be provided in the control room for the existing HMI until the transition is 100% complete.

It is also recommended that a system be developed whereby it is clear to the operators if a specific piece of equipment has been commissioned on the control system. By utilizing an *uncommissioned* status point on the HMI, it may be possible to “gray out” the associated graphic if the equipment is not commissioned. A system to indicate decommissioned equipment will also need to be developed for the DCS HMI; however it is recommended to utilize the simplest approach possible to minimize DCS HMI rework.

The proposed HMI system must be developed from the ground-up and should not reutilize any significant portion of the existing HMI system. Alarms from the existing HMI should be exported, rationalized, updated with appropriate current descriptors, and cross referenced to ensure that corresponding alarms are addressed in the new system. Graphics and trend screens from the existing HMI should be exported and cross referenced to the new HMI screens. Not all graphics will be copied directly, and rationalization will be required.

11.4.2 DCS PCU Migration

The migration of the existing DCS PCUs to the new control system will not be simple, especially within the constraints of an operating facility. It is expected that the migration of equipment not significantly changed by the upgrades will take place by connecting the existing Infi90 I/O to new PLC I/O. Many control system vendors have developed custom cordsets, which can connect existing Infi90 field termination units to the PLC I/O modules. This allows field wiring to remain unmodified, and allows the transition to occur during a relatively short shutdown window. It is anticipated that the PLC I/O would be mounted in the existing DCS PCU enclosure where the current DCS modules reside, however this solution would be dependent upon the control system vendor selected and the details of the specific installation. The PLC I/O could either be remote I/O, or connected to a local processor, which would be determined as part of detailed design.

The general migration sequence would be as follows:

- Perform a complete factory acceptance test (FAT) on the area PLCs and HMI.
- Install new PLCs in the area and connect the new equipment.
- Existing equipment with significant modifications would be rewired to new PLC I/O in new PLC cabinets. This would include decommissioning of associated DCS I/O
- Existing DCS controlled equipment with minimal modifications would be converted to PLC control during a short shutdown window.
    - All PLC I/O backplanes and cordsets would need to be prefabricated for rapid implementation and tie in to the existing DCS cabinets, where feasible.
    - During the shutdown, transition a PCU to PLC control. Subsequent commissioning of all associated equipment would subsequently commence.
- Final integration of miscellaneous systems and components.
- This above process would be replicated on a per PCU and area basis.

12.0 HMI AND ENTERPRISE SYSTEMS

12.1 Introduction

The Human Machine Interface (HMI) system provides operator monitoring and supervisory control of the wastewater treatment facilities. The HMI system is the operator's primary means to manage the process. The HMI server system also provides the interface between the PLC network and the historian and other enterprise data users.

12.2 System Architecture

The recommended general architecture for the HMI system is shown in Figure 12-1. Note that the detailed architecture is subject to change based upon the specific implementation requirements of the control system vendor selected.

The HMI servers are to be completely redundant with failover capability, and connected to redundant Ethernet networks. Components such as the Historian and Domain Server do not necessarily need to be redundant, provided that methods of addressing failures are provided. For example, if the HMI Servers have a store-and-forward methodology for historical data, which can temporarily cache data for a duration sufficient to replace the historian server, then no further redundancy is deemed to be required.

The HMI servers are located on a separate network, identified as the Supervisory Network. This network is isolated from the Process Network via layer 3 switches, which are capable of routing the appropriate communication between the networks. Separate server network interfaces are provided for the process and supervisory networks.

The Development Workstation allows for PLC HMI, and network configuration. It is connected to both the supervisory and process networks to provide more complete connectivity in the event of network abnormalities. The Remote Development Server provides most of the same applications as the Development Workstation, but acts as a terminal server to remote maintenance and external personnel. This remote access server provides a level of network security for remote access.

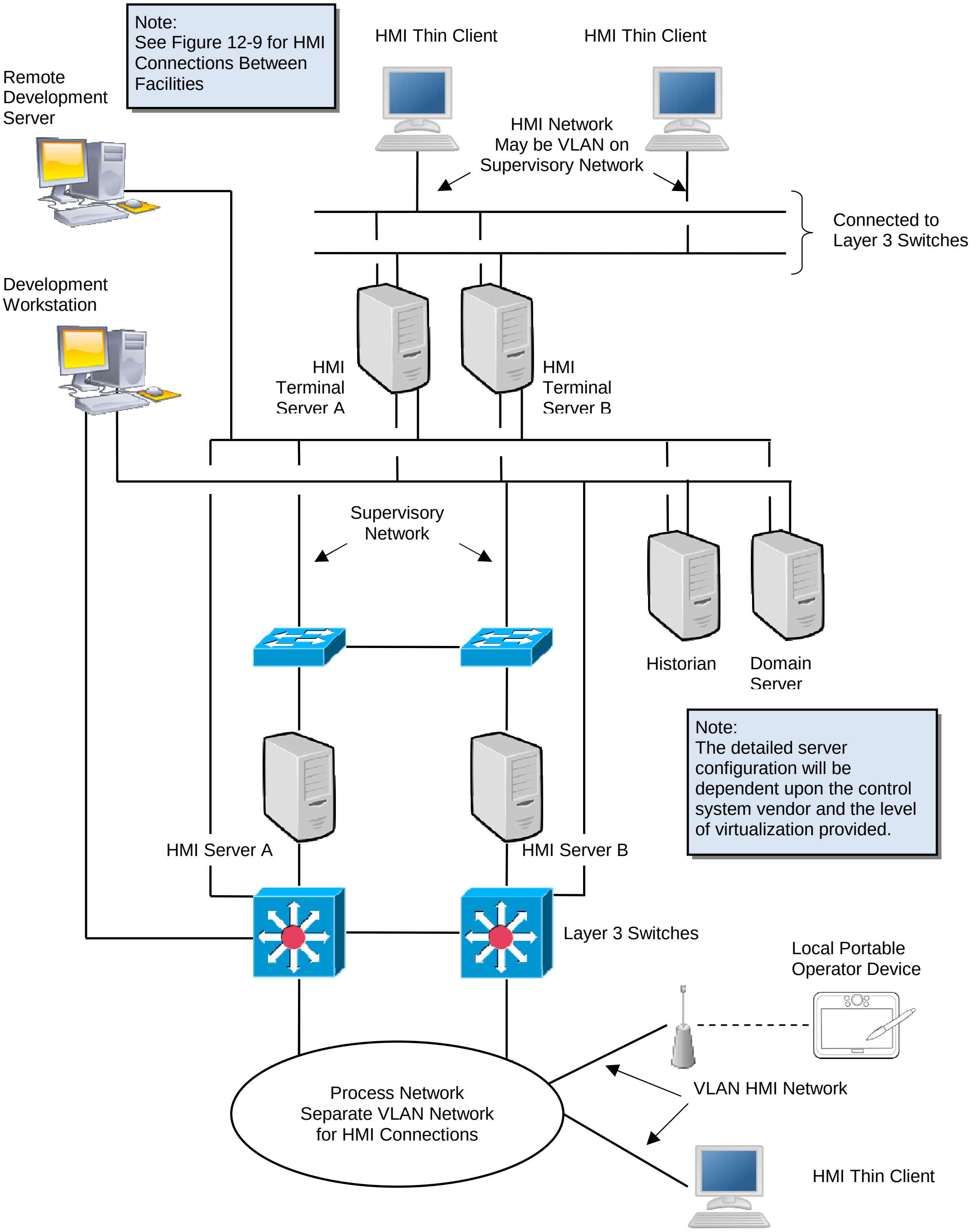


Figure 12-1 : HMI System Architecture

12.3 HMI Client Configurations

12.3.1 Terminal Services

HMI clients from many current vendors can be provided in either a thick client or thin client configuration. A thick client configuration has HMI software loaded on a computer with a full operating system, such as Microsoft Windows, and communicates to a HMI Server to obtain the process data. The client must be loaded with software and updated with patches as required. The existing DCS HMI configuration utilizes thick clients. On the other hand, the use of thin clients together with terminal servers has been adopted by many HMI systems over the last ten years. This is now an established technique to provide HMI capabilities with a more simple configuration.

Thin clients are very basic client implementations that have a user interface (display and input) and network connectivity. The software that runs the actual client application is located on a terminal server, which serves many clients. The thin client can be an industrial thin client, a desktop thin client that appears to be a standard computer without a hard drive, a full desktop computer with thin client software, a web browser interface, or a portable operator device such as a PDA.

The primary advantages of thin clients compared to thick clients are as follows:

- Thin clients have a lower total cost of ownership due to reduced configuration and maintenance requirements as would be the case with thick clients.
- Thin clients allow for more straightforward deployment of remote client capabilities.
- Thin clients have a smaller footprint.
- A single server software installation supports multiple thin clients.
- All client software maintenance, such as application modifications and patches are performed on the centralized servers rather than on multiple clients.
- Multi-session capability can be provided, where a single thin client can view multiple server connections.

It should be noted that the City of Winnipeg Water Treatment Plant utilizes thin clients based upon a Wonderware Terminal Server system.

It is recommended that terminal services be utilized for all client HMI access, and that redundant terminal servers be utilized to ensure that client access is provided in the event of a single server failure.

12.3.2 Desktop Thin Clients

Desktop thin clients will be utilized in the main control room, and in designated area control rooms. A keyboard, mouse, and monitor will be provided at a desk. It is recommended that the area control rooms utilize a similar monitor resolution as the main control room, to avoid development issues associated with screen rescaling. The desktop thin clients will have complete access to the entire facility, provided the logon credentials permit such access.

12.3.3 Touchscreen Thin Clients

Touchscreen thin clients will be utilized in various locations throughout facility, where a desktop client is not provided. The touchscreen thin clients should be based upon a fanless design, with at least a 305 mm (12”) screen and 1024x768 pixel resolution. As the pixel resolution will be reduced from the desktop clients, it is anticipated that dedicated screens will be developed for the touchscreen displays. It is recommended that the selection of touchscreen thin clients also reference the resolution of portable operator devices to determine if a common resolution can be attained. As it is not desirable to recreate all screens at varying resolutions, it is recommended that the use of touchscreen thin clients be limited to areas where use of a desktop thin client is not appropriate and a HMI interface is necessary.

The previous discussion highlighted that attention should be paid to the pixel resolution of the operator interface devices, to avoid regeneration of HMI screens. Some will argue that numerous HMI vendor packages offer screen rescaling capabilities, thus eliminating the requirements for dedicated resolution screens. However, practical experience with dynamically resized screens usually leads to limited results, and non-scaled screens are significantly superior. It is also noted that screen scrolling / panning is an alternative to screen redevelopment, however this is recommended only for infrequent use. For example, it would be deemed acceptable that a touchscreen thin client in the Primary Clarifiers area utilize a scrolled screen to view the UV disinfection screen.

12.3.4 Local Independent Touchscreen

The third type of HMI to be utilized is a local independent touchscreen, which communicates directly to the PLC. The advantage of this configuration is that it can operate in the event of a facility network or major HMI server malfunction. The primary disadvantage of this configuration is the additional development and maintenance associated with an independent HMI node. The local touchscreen HMI must be managed separately, which includes changes regarding alarming, security, process configuration, and network management. Thus, the use of local independent touchscreens is only recommended where there is a critical process and local view is determined to be a critical requirement, or where required to coordinate directly with a vendor packaged system. Examples of some situations where a local independent touchscreen may be utilized are for raw sewage pump control, due to its criticality, and for the monitoring of a packaged UV system.

12.3.5 Local Wireless Operator Device

It is desired to have portable operator devices available within the wastewater treatment plants. These could either be a small Personal Digital Assistant (PDA) style device, or a tablet PC. These devices would act as a thin client and connect to the terminal servers over a wireless connection. The ability to provide operators with mobile access to the HMI is deemed to be a valuable feature. It should be noted that the local wireless operator devices would connect via a network access point to the physical process network, however this connection would be logically segregated, via a VLAN configuration, as part of the HMI network connected to the terminal servers. Further discussion regarding the networking in provided in Section 14.0.

Most major vendors have a solution to allow for portable operator devices, however the level of support and configuration required will vary. In some cases it would be required to develop a separate HMI application for portable devices with smaller screens. While ideally it would be desirable to have complete HMI functionality, even the provision of an alarming interface would be useful and thus alone provides a basis for the implementation.

It is proposed that these devices utilize a tablet style interface, to provide a sufficient viewing area to allow for effective touchscreen use. A minimum of a 1024 x 768 screen resolution is recommended. It is expected that this operator interface will significantly change the way operators perform their tasks.

It is recommended that the level of vendor support for portable operator devices be evaluated as part of the control system vendor selection, as discussed in Section 10.15.

The connection of wireless operator devices within the facility would be via a wireless LAN connection, and communicate via the HMI VLAN to the terminal servers. Further discussion regarding security may be found in Section 15.0.

It could be proposed that the value of the area control rooms and local touchscreens is extremely limited with the introduction of local operator devices. While this is true to an extent, it is still proposed that most fixed operator terminals remain based on the following rationale:

- Not all personnel will likely have portable operator terminals, due to cost and security issues.
- Fixed terminals can be utilized by other personnel for viewing only, such as mechanical and electrical maintenance personnel.
- Batteries on portable operator terminals have a limited life, and it is expected that there will be a significant number of occasions where the portable device is not available due to battery charging.
- Wireless networks are not expected to be redundant, and the failure of the wireless network is expected to be more frequent than for the wired network.

12.3.6 Remote Portable Operator Devices

It is also desired to utilize portable devices to access the wastewater treatment plant system from anywhere. This could either be a laptop, tablet or smartphone connection over a cellular network. The operator interface provided would be similar to that provided to local portable operator devices. Given that the communications would be less secure, additional secure communications and authentication would be required. See Section 15.0 for further discussion regarding remote access.

Given the similarity of local and remote portable operator devices, consideration could be given to eliminating the local device, and only utilizing remote type devices with cellular connection. However, it is beneficial to distinguish between local and remote operator devices for the following reasons:

- Local devices using a local wireless LAN connection would have faster, more responsive access.
- Wireless dead-spots in the facility can be easily addressed using additional access points.
- The logon procedure for local devices can be simpler, and utilize longer inactivity timeouts.
- The security implementation for a local wireless network can be more basic, with less authentication.
- Local wireless devices provide a straightforward method to provide junior operators with local wireless control capability, without granting the capability from outside the facility.

12.4 Other Considerations

12.4.1 Server Virtualization

Server virtualization is a system whereby logical computer server systems are installed on a virtualization layer rather than directly on computer hardware. It allows multiple virtual servers to be installed on a single physical server, without compromising the integrity of each virtual server. Each virtual server has its own operating system and applications, and logically appears to be an independent hardware computer. Server virtualization has the following significant potential advantages:

- The number of hardware servers required can potentially be reduced, which can positively impact available space and heat loading in the server room. In addition, virtual servers can be relatively easily redistributed across different hardware servers as loading changes.
- The affect of hardware and operating system changes can be reduced as the virtualization layer isolates the operating system from the hardware. The operating system does not need to be re-installed with the correct service packs and patches when hardware is replaced.
- System management is simplified as the virtualization interface provides remote access and a consistent node interface.
- The reliability of the server system can be improved by utilizing system snapshots to allow for server system rollback, and hardware can be replaced without impact on the virtual servers it contains.

It is recommended to utilize server virtualization where appropriate to do so and the control system vendor approves the configuration. These decisions must be made after control system vendor selection.

12.4.2 HMI Network

The HMI and Supervisory networks shown in Figure 12-1 are shown as physically separated. This segregation is primarily motivated by security and it is deemed acceptable to utilize VLAN segregation to form separate physical networks on a single physical network. It is also proposed to utilize VLAN segregation to distribute the HMI Network over the physical Process Network to the various process areas of the facility.

12.5 Supporting Infrastructure

It is recommended that the following supporting infrastructure for the HMI systems be provided.

- Server rooms should be separate from the control room and other offices. It should be segregated from the remainder of the building by a two-hour fire separation, and the design should accommodate fire detection. The requirement for fire suppression should be reviewed at design time, and should be based upon the likelihood of a significant fire.
- Each server room should be provided with a dedicated pressurization unit, with media filtration, and an air recirculation system with cooling. Multiple cooling evaporator units are preferred over a single unit to allow for a base level of cooling during maintenance events. Consider multiple recirculation fans if temperatures are likely to exceed unacceptable levels within a short interval of a fan failure. Recirculation fans and at least a base level of cooling must be backed up by a standby generator.
- Development workstations, which typically have a higher level of access to the automation networks, should be in physically secure areas. The development office should have appropriate security measures. If the office has a common suspended ceiling plenum with other office spaces, at minimum a motion detector should be placed in the office, that is connected to a separate security zone. Potentially, the development workstation office could be integrated with the sever room.
- Wastewater facilities that serve a large population and contain a central control centre for multiple facilities should have higher reliability requirements for the HMI and server system:
  - Provide two independent server rooms for all HMI and main networking equipment. The server and networking equipment should be distributed such that the complete loss of any server room does not significantly impact facility operations. The server rooms should be each within a two-hour fire separation, or alternately be within a separate building. It is anticipated that the NEWPCC facility should have two dedicated server rooms.
  - Provide a redundant UPS installation, with distributed power. UPS-A would be installed in Server Room A and supply the A power feed for all dual-

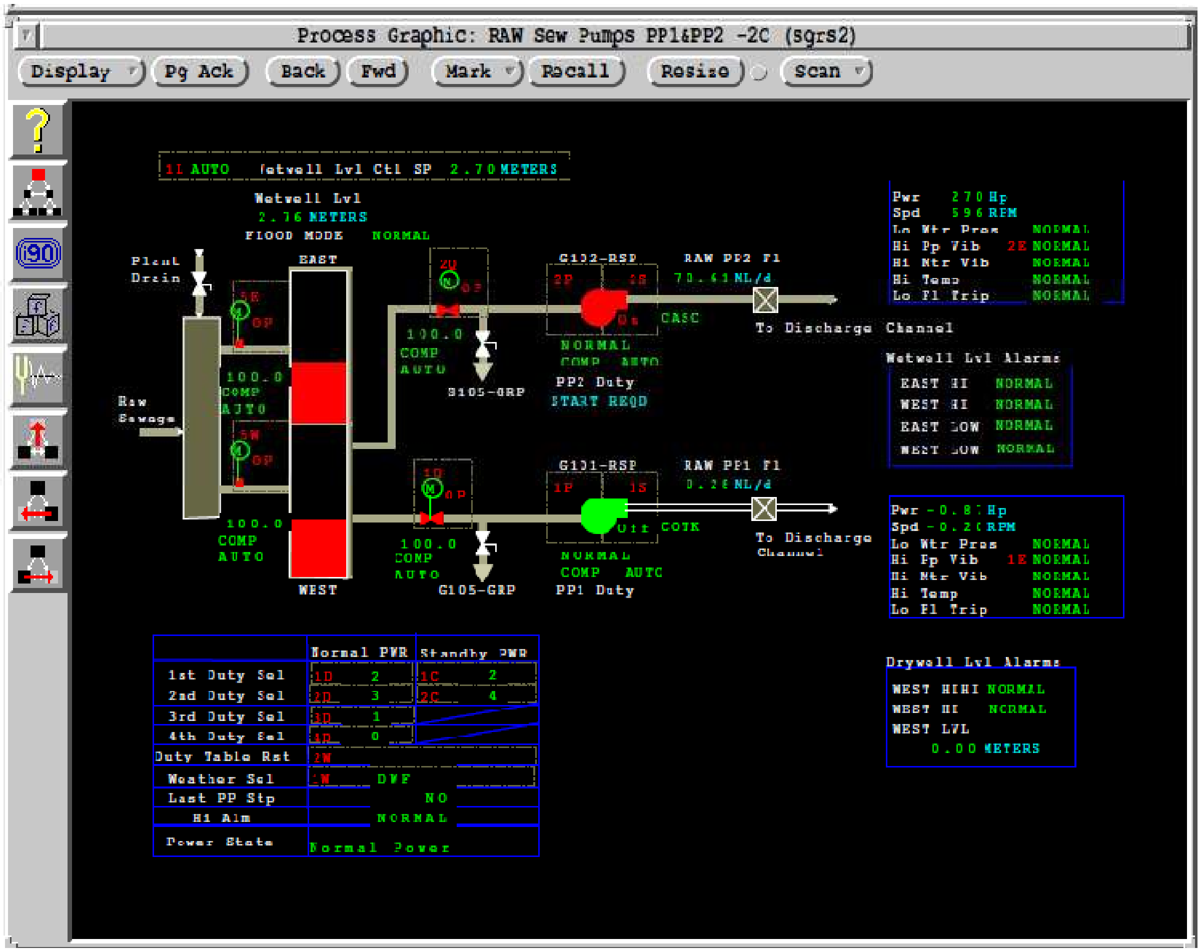
corded loads in both server rooms. UPS-B would be located in server Room B and would supply the B power feed for all dual-corded loads in both server rooms. At least one of the UPS units should be backed up by a standby generator. Paralleled UPS installations with a common output are not acceptable.

- For most small to medium sized wastewater facilities, a single server room is deemed to be sufficient, and should be configured as follows:
    - Networks should be configured such that in the event a server room is completely lost, automatic plant control is not significantly affected, other than loss of the HMI. Contingency plans should be in place to install a temporary HMI Server / Client computer in a backup location within an eight hour period.
    - Provide a single UPS installation, with backup power from a standby generator to feed all A power feeds for dual corded loads. The B power feeds would be provided by filtered power from a non-essential power source.
- For the designated central control room that is utilized to monitor all three wastewater treatment facilities:
    - Network redundancy within the facility is to be provided, such that in the event of a network failure, at most 50% of the operator terminals are lost.
    - Provide a redundant UPS installation, with distributed power. UPS-A would be installed in Server Room A and supply the A power feed for all dual-corded loads in both server rooms. UPS-B would be located in server Room B and would supply the B power feed for all dual-corded loads in both server rooms. At least one of the UPS units should be backed up by a standby generator. Paralleled UPS installations with a common output are not permitted. In the event that the server rooms would be located far apart, an alternate UPS installation would be required with specific design to achieve the required availability.

12.6 Graphic Scheme

12.6.1 Existing

The existing DCS HMI at the City of Winnipeg wastewater treatment facilities utilizes a graphic scheme that originates to the late 1980s. A sample screen from the SEWPCC facility is presented in Figure 12-2.



	Normal PWR	Standby PWR
1st Duty Sel	1D 2	1C 2
2nd Duty Sel	2D 3	2C 4
3rd Duty Sel	3D 1	
4th Duty Sel	4D 0	
Duty Table Rst	2W	
Weather Sel	1W DWF	
Last PP Stp	NO	
Hi Alm	NORMAL	
Power State	Normal Power	

Figure 12-2 : Existing SEWPCC HMI Screen

Some highlights of the current graphic scheme are as follows:

- A black background is utilized.
- Green is utilized for equipment stopped, and red for equipment run.
- Green is utilized for open valves and red for closed valves.
- Equipment is coloured magenta upon an alarm.
- All I/O information is typically presented on the graphic mimic displays, as well as on group data displays.
- There is a significant use of text on the displays.
- The organization of the graphics is generally in a hierarchy, with a loop of sequential screens for each process area.

12.6.2 Current Industry Direction

Current standards and industry practice relating to the presentation of HMI systems are changing, with emphasis on clearly indicating abnormal situations to operators. By presenting important, relevant information to the operator with prominence, appropriate operator action can be achieved much more rapidly. Normal, routine control of the process is the responsibility of the control system, and the HMI system should be designed to emphasize abnormal situations only that require operator intervention.

Note that the trend in the late 1990s and early 2000s was often to provide HMI systems with highly complex, realistic 3D graphics. While some of these HMI screens were visually stunning, and great marketing tools, they have not proven to be useful for operations personnel. Complex graphics can distract and inhibit rapid comprehension of the process state. In addition, a danger of 3D graphics that attempt to be photo-realistic results in a loss of standardization across all equipment, and the true state of the equipment may not therefore be clear to the operator in all instances.

The current trend is to present operations personnel with relevant information, in a manner that allows for rapid scanning of a screen to identify abnormal situations. The HMI screen should do more than just contain the applicable information, it should present the information with visual clues to guide the operator regarding potential action requirements. A current method of providing visual guidance to the operator that is gaining acceptance is informally known as the shades-of-gray approach. This approach is also presented more formally by organizations such as the Abnormal Situation Management (ASM) Consortium.

In a shades-of-gray approach, the majority of information presented to the operator is a shade of gray. Equipment, process lines, and instruments are all shown as a shade of gray on a light gray background. Thus, typical, constant information is de-emphasized. However, abnormal situations are indicated with the use of bright colours, and the colour red would typically be utilized to indicate a Priority 1 abnormal situation. An example of a graphic developed utilizing this approach is presented in Figure 12-3. Note that the abnormal condition in the graphic is abundantly clear.

Note: If the abnormal condition is not clear, please obtain a color version of this document.

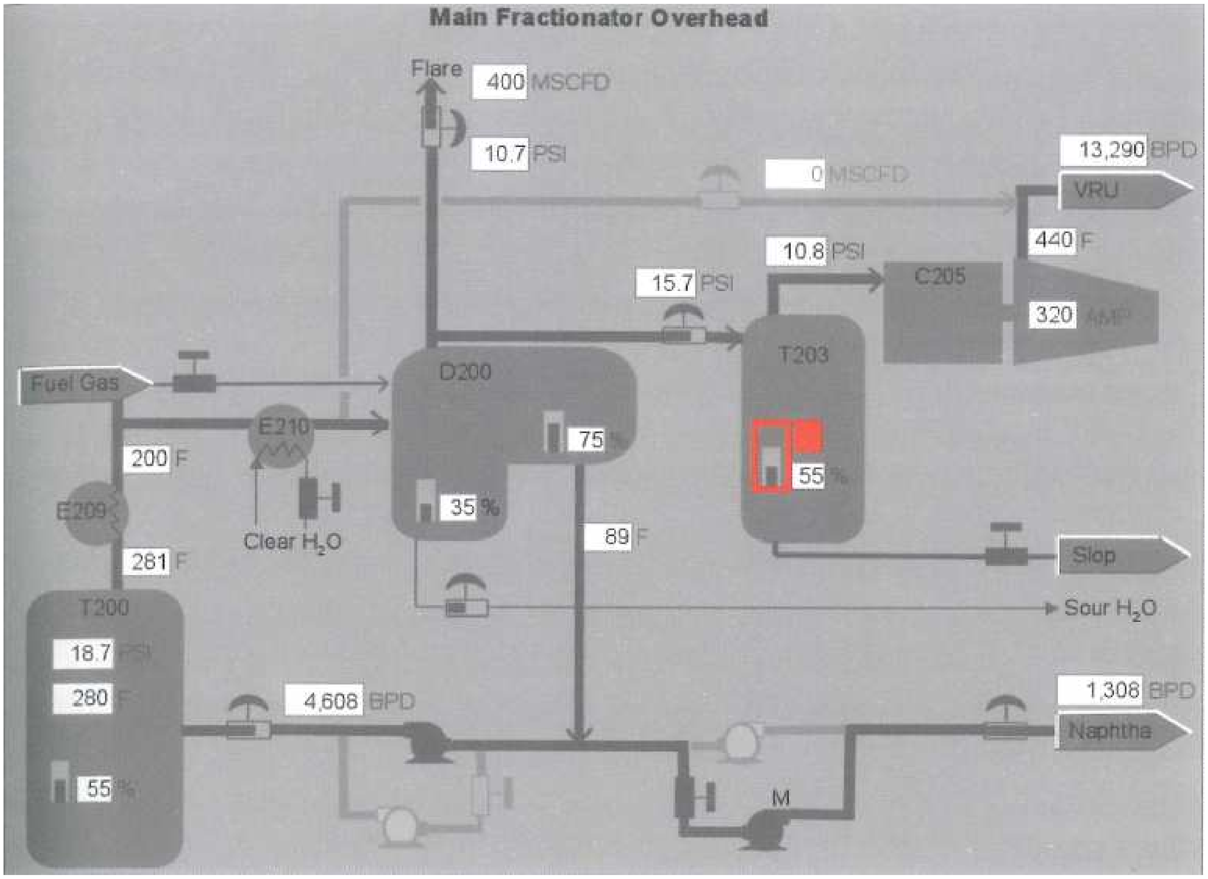


Figure 12-3 : Generally Proposed Graphic Scheme

Above graphic is from ASM Consortium Guidelines – Effective Operator Display Design, 2008.

It should also be noted that ISA is developing a standard SP-101 that is intended to address HMI graphic presentation, however as of this writing, the standard has not been released.

Significant debate has historically been held regarding the use of either the red=run or green=run philosophy. The industry standard is moving towards the use of the colour red as an alarm or emergency colour. The ASM Consortium and other shades-of-gray advocates prefer to avoid the use of green as a run or stopped colour state as well, and utilize shades of gray as equipment run status. The ASM Consortium does not provide clear guidance as to whether a darker or lighter colour should be utilized for run indication, and other shades-of-gray proponents differ in opinion as well. One must also consider the consistency with pilot light colours, where they are provided in the field. It is not possible to utilize shades-of-gray on field pilot lights to show equipment state. Thus, if a run light is installed on a motor starter for example, colour options are limited to a few common selections provided by manufacturers. A white/clear bulb indication may be a potential solution, however white pilot lights are not always visually distinguishable in certain bright lighting conditions.

The NFPA 79 standard definitions regarding the use of coloured pilot lights are shown in Table 12-1. The standard also indicates that the preferred colour for running status is green, while the use of white is permitted and the use of red is not acceptable. Note that the European standard BS / EN 60204 colour definitions are similar to NFPA 79.

Table 12-1 : NFPA 79 Standard Colours

Colour	Purpose		
	Safety of Persons or the Environment	Condition of the Process	State of the Equipment
Red	Danger	Emergency	Faulty
Yellow / Amber	Warning / Caution	Abnormal	Abnormal
Green	Safe	Normal	Normal
Blue	Mandatory Action		
Clear / White	No Specific Meaning Assigned		

The City's current colour philosophy for run status is shown in Figure 12-4, as well as three alternatives based upon current standards are shown in Figure 12-5, Figure 12-6, and Figure 12-7. The style shown in Figure 12-5, classified as the ASM style, proposes that the run status should be a darker gray, to match the pipe colour and indicating continuous fluid flow. However, the issue with this approach is that there is no pilot light colour that correlates to a dark gray colour. The style shown in Figure 12-6, classified as the alternate shades-of-gray style, proposes that the run status should be a white colour, which would correlate with the use of a white pilot light for run status. However, use of a white pilot light for run status is not common, and is not necessarily clear in all lighting conditions.

The recommended colour philosophy for run status is shown in Figure 12-7, which is based upon a best-effort compromise between the shades-of-gray colour scheme, NFPA 79, and industry convention. It is understood that given the City's history with the red=run and green=stopped philosophy, there is an argument to be made that any new philosophy should not use either of these colours for run status, however the ambiguity of the alternatives is not deemed to be desirable. It is believed that neither a dark gray nor a white colour, as shown in the two alternatives, is intuitive for new operations personnel to identify run status. Thus, it is proposed to utilize the colour green for run status, but utilize a slightly subdued shade (RGB 144,208,144) to avoid distraction and utilize the bold, bright colours for alarm indication. While this is not 100% compliant with the ASM Consortium guidelines, it is consistent with NFPA 79 and has been proven to be very intuitive to new operators, who are familiar with the green=go traffic light analogy.

The details of the proposed colour scheme should be documented in the *Automation Design Guide* discussed in Section 18.4.1 and the *HMI Layout and Animation Plan* discussed in Section 18.4.3.

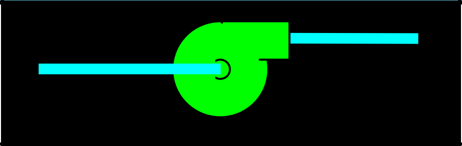
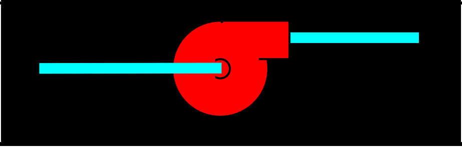
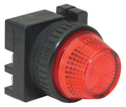
State	HMI Graphic	Pilot Light	Notes
Stopped			Pilot light not typically provided.
Running			

Figure 12-4 : Existing Run Status Indication

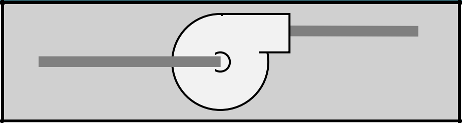
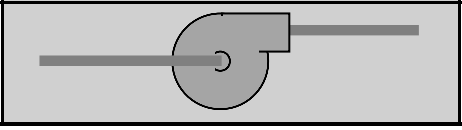
State	HMI Graphic	Pilot Light	Notes
Stopped		Not Defined	Pilot light not typically provided.
Running		Not Defined	Pilot light colour correspondence not clear.

Figure 12-5 : ASM Style Run Status Indication – Option 1

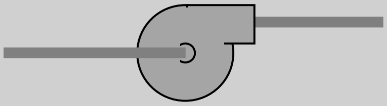
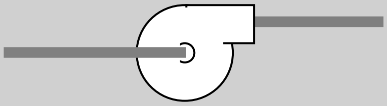
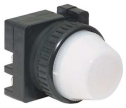
State	HMI Graphic	Pilot Light	Notes
Stopped		Not Defined	Pilot light not typically provided.
Running			

Figure 12-6 : ASM Style Run Status Indication – Option 2

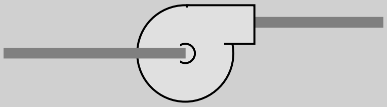
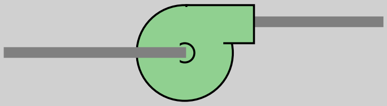
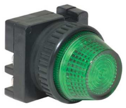
State	HMI Graphic	Pilot Light	Notes
Stopped			Pilot light not typically provided.
Running			HMI graphic green is subdued to avoid distraction of alarm colours.

Figure 12-7 : Proposed Run Status Indication

12.6.3 Recommendations

The following recommendations are made regarding the presentation of HMI graphics:

- Utilize a shades-of-gray approach.
- Utilize a subdued shade of green (RGB 144,208,144) to indicate run status.
- Movement animation should be avoided unless it serves a useful purpose to operators.
- Utilize 2D graphics rather than 3D graphics. 3D graphics should only be utilized to indicate actionable objects, such as buttons.
- Integrate alarm information onto the HMI graphics
- Integrate trends onto the graphics

12.7 Alarm Management

Alarm management is a critical component to wastewater facility operation. Ineffective alarm management has been a frequent root cause of significant industrial failure events around the world, where operations personnel were not able to identify a critical situation that required operator attention. Alarms should be configured to clearly identify abnormal conditions that require intervention. Excessive alarms are just as dangerous as the lack of an alarm, as operators are not capable of absorbing and acting on information above a certain rate.

Some general and specific guidelines regarding alarm management are as follows:

- Set up and document an alarm management program that defines the complete life cycle for alarms. The alarm management program should include:
    - The philosophy of the alarm system,
    - The procedures for: identification of an alarm, rationalization, detailed design, and implementation,
    - Procedures for monitoring and assessment of the alarms, and
    - Change management procedures.
- Ensure that process engineers are included during the design phase as part of the alarm definition and rationalization process.
- Ensure that all alarms are appropriate, relevant, and clear.
- Consider utilizing real-time alarm management, which can include:
    - Alarm Shelving – Temporarily suppress an alarm, with appropriate tracking and control
    - State-based alarming – Where alarms or alarm setpoints are set specifically to the current operating condition
    - Alarm flood suppression

While at glance, setting up a formal alarm management program may seem quite onerous, in reality it is intended to be fairly straightforward to implement. Authorized personnel must be empowered to perform significant alarm management functions without excessive paperwork, provided that appropriate accountability is provided. For example, the programmer may be permitted to directly change the deadband of an alarm based upon a request from an operator, provided that the change is logged. On the other hand, certain changes, such as the deletion of an alarm should be approved by relevant senior operations and engineering personnel to ensure that an unsafe situation is not created by the modification. These items should be documented in the alarm management program. It is also recommended that ISA 18.2 be utilized as a reference document regarding the formalization of an alarm management system. Reference should also be made to EEMUA 191.

The effectiveness of an alarm management system can be measured through the use of metrics. Some recommended guidelines for alarm performance metrics are shown in Table 12-2. Note that these metrics must be tempered with engineering discretion, and deletion of important alarms to meet target alarm rates is not an effective solution.

Table 12-2 : Recommended Alarm Management Metrics

Metric	Average Target Value	Maximum Value	Notes
Alarms Per Day	< 150	300	
Alarms Per Hour	6 (average)	30	
Alarms Per 10 Minutes	1	10	
Percentage of Priority 3 Alarms	80%	<100%	
Percentage of Priority 2 Alarms	15%	25%	
Percentage of Priority 1 Alarms	5%	10%	
Stale Alarms	5	10	Stale alarms are those that are still present after a day.
Alarms that can be ignored (chattering / fleeting / not important)	0%	1%	Action plans need to be in place to address these alarms as they occur.

12.8 HMI System Capabilities

The capabilities of the HMI system should include the following:

- Development Environment
  - Allow a multi-user development environment with minimum manual intervention
  - Development is to utilize an object-based template approach, where both the graphics and the supporting tag database are object based. The use of inheritance to support derived objects must be included.
- Historian
  - The historian is to be integrated into the development environment, and it shall not be required to load a separate tool to modify the logging characteristics of a tagname.
- Redundancy
  - Complete redundancy with fail-over is required for all continuously online services.
  - Upon server or network failure, all clients should have complete operation returned within 30 seconds.
- Operator Interface
  - Provide a high performance system with minimum latency. It is expected that the latency for object update, at the local thin clients, will be less than 0.5 seconds from the time of change in the PLC, under normal operating conditions.
  - Provide an audit trail system than can record all operator actions to a secure location.
  - Provide a flexible security system that includes the ability for verification of the user’s authentication for certain operations. This can be recorded as an electronic signature.
  - Detail screens are to be arranged in a manner similar to P&ID drawings.
  - Overview screens are to be provided for each process area and facility, which display the primary information, for rapid operator absorption.

The above is not an exhaustive list, and further development of the HMI system capabilities will be required as part of the control system selection project.

12.9 Control Rooms

12.9.1 Main Control Room

A main control room will be provided for each facility, as the principal control location. The control room will be utilized to monitor the entire facility. Two operator terminals will be provided, which is consistent with the existing control room configuration at the wastewater facilities. One of the two operator terminals would be provided with dual monitors to provide additional monitoring flexibility. In addition, it is proposed that a large, wall-mount facility overview monitor will be provided, to allow personnel a rapid overview of the entire facility, without switching screens. The facility overview terminal could also be switched to a different view on demand, if required, from one of the operator terminals. A large security video monitor would also be provided. The proposed arrangement of the facility control room terminals are shown in Figure 12-8.

It should be noted that the proposed interface layout requires rationalization based upon the control room layout. Human ergonomics must be considered in the configuration of the operator interface, and the large, wall-mount overview monitors are only appropriate if the position of each monitor is appropriate for viewing without causing ergonomic strain.

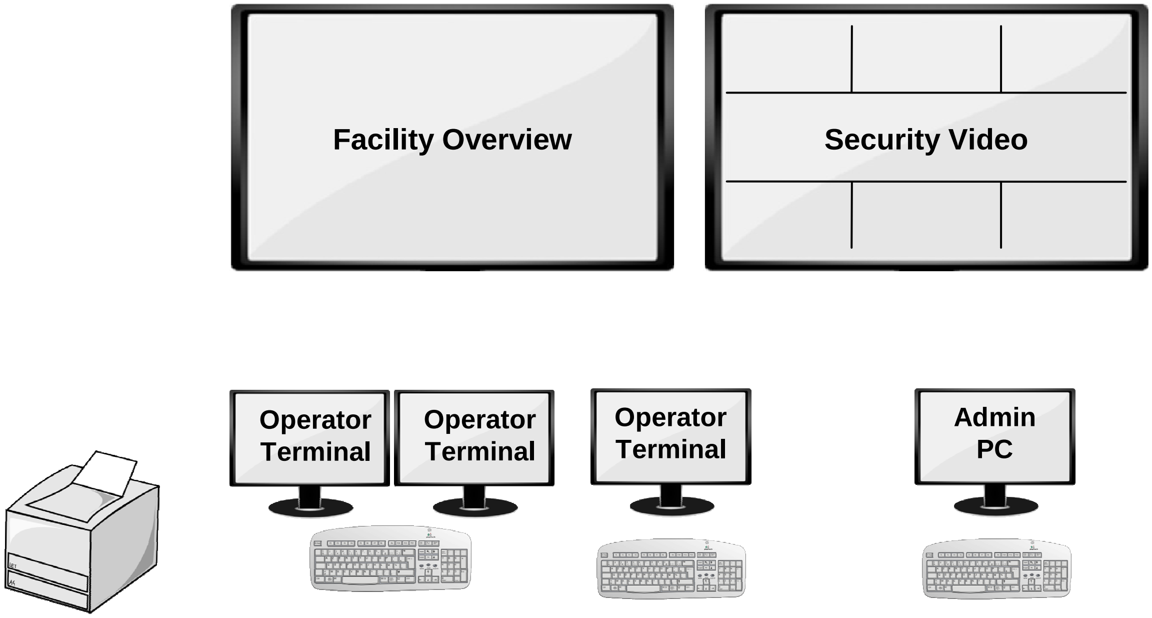


Figure 12-8 : Facility Control Room Arrangement

Note: The above control room arrangement may not apply to the facility designated as having central control.

12.9.2 Area Control Rooms

The existing HMI system at the wastewater treatment facilities has operator terminals located in many, but not all of the process area control rooms. The operator terminals are typically in the same room as the existing DCS controls. Many of these operator terminals are utilized on only an intermittent basis.

The proposed elimination of the Field Device Panels, as discussed in Section 4.2, will slightly increase the requirement for area operator interface terminals, which could either be desktop thin clients, touchscreen thin clients, or in some cases local independent HMI touchscreens, as discussed in Section 12.3. It is proposed that larger or complex process areas have a conditioned control room with a desktop HMI thin client. It is not expected that these area control rooms would contain more than one HMI terminal. The location of these control rooms is highly dependent upon the proposed plant layout, however as a guideline, it is recommended that an area control room with a desktop HMI terminal should be within 150m of most locations within the facility. Where this cannot be achieved, consideration should be given to the installation of a touchscreen HMI thin client.

12.10 Central Control and Monitoring

12.10.1 Location for Centralized Control

Currently, the SEWPCC and WEWPCC facilities are only staffed during normal working hours, while the NEWPCC facility is staffed continuously. The SEWPCC and WEWPCC facility are currently monitored during non-working hours from the NEWPCC facility via a basic grouped alarm interface. It is expected that in the near-term, the NEWPCC facility will remain as the location for centralized control, however this could change in the future. Thus, the City has requested that the system architecture be configured in a manner that the location for central control be flexible, with any of the three facilities capable of monitoring and controlling any other. In addition, it is also desired to have the capability for a central control centre, not located at any of the wastewater treatment plants.

Thus, centralized control capability will be provided, but with location flexibility.

12.10.2 Architecture

As discussed in Section 12.2, it is proposed to install redundant HMI terminal servers at each facility, to serve the local HMI thin clients. In addition, these HMI terminal servers would also serve remote HMI thin clients at the other wastewater facilities, provided appropriate authentication and permissions are set for the user. This will allow authorized personnel at any facility to view and control any other facility.

The architecture discussed is presented in Figure 12-9.

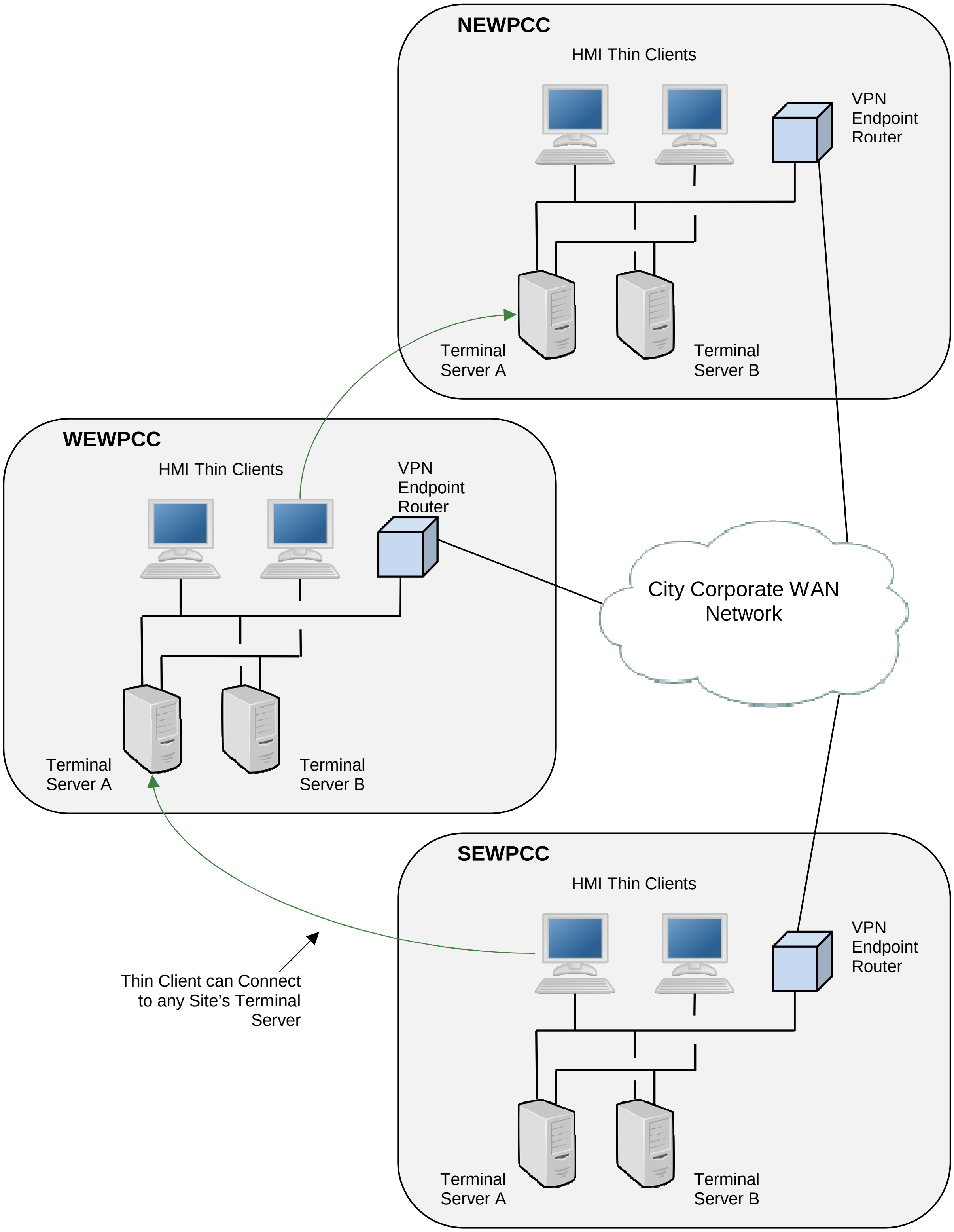


Figure 12-9 : HMI Multi-Site Flexibility

12.10.3 Centralized Control Room

At the other facilities, not designated as the central control centers, additional overview monitors for the other facilities would not be provided, but the client computers would have the capability to switch to the other facilities. Note that control of the other facilities would be limited to those personnel with appropriate security privileges. The proposed centralized control room arrangement is shown in Figure 12-10 and is merely an extension of the arrangement proposed for each of the facility control rooms. Once again, human ergonomics must be considered in the layout of the control room.

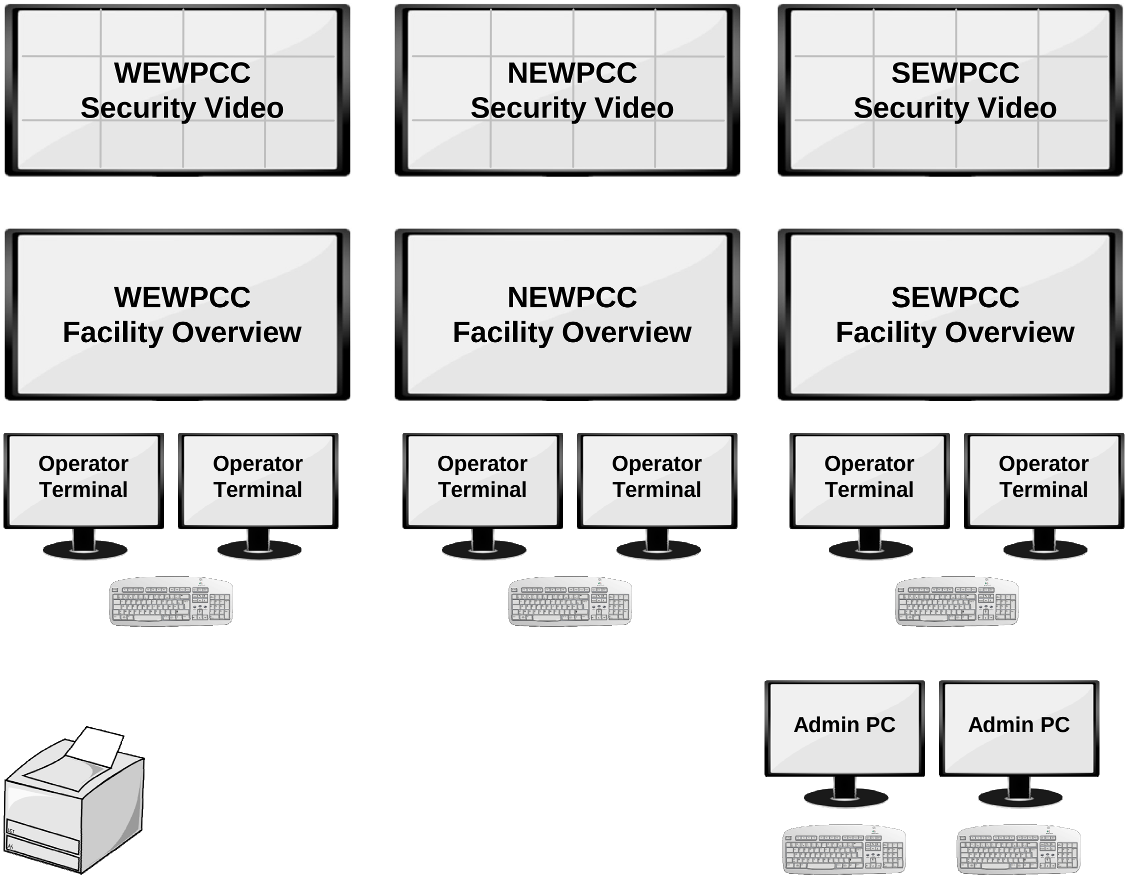


Figure 12-10 : Central Control Room Proposed Arrangement

12.10.4 Contingency Planning

The City's contingency planning must account for potential failure of the central control room. Examples of potential scenarios include fire and loss of the City's wide area networking. The architecture proposed provides an acceptable solution to the scenarios proposed. In the event of fire, the central control can be performed from any of the three wastewater facility control rooms, as the terminal server / thin client architecture allows the thin clients to connect to any facility's servers. Loss of the City's wide area network would simply be addressed by locally manning each of the three wastewater facility control rooms continuously.

12.10.5 Implementation Requirements

The NEWPCC facility control room currently serves as the central control location for the wastewater facility, although only remote monitoring of the SEWPCC and WEWPCC facility via a basic alarm interface is provided. It is envisioned that as part of the SEWPCC upgrades, the basic alarm interface will not be maintained, and thus installation of a HMI thin client at the SEWPCC facility is recommended. This will require supporting networking upgrades at the NEWPCC facility. In addition, it is proposed to install the Central Historian Server at the central control room location, along with the web server, which is presented in Section 13.4.

It is expected that the overall NEWPCC facility upgrades will include a new control room and server rooms. However, delivery of this project will not be complete prior to SEWPCC construction. Thus, it is deemed that upgrades to the existing NEWPCC control room and associated server room will be required. This is proposed to be implemented as a separate project, as presented in Section 21.4.7.

12.11 HMI Remote Access Requirements

Remote access to the HMI is required to allow off-site or on-call operations personnel to support the operation of the facilities. In addition, remote access is also desired for other City personnel to view the current status of the facility. For example, it would be useful for the facility supervisor to pull up a window to the HMI system to view which sludge pump is out of service. The architecture details of the remote access vary depending upon the application.

12.11.1 Mobile Operator Remote Access – View Only

The first type of remote access is for operations personnel who are not within the wastewater facilities, and require mobile access. The summary of the proposed remote access architecture is shown in Figure 12-11. In the figure, a cellular connection is shown, however, any technology with a connection to the Internet, such as WiFi, would also be capable. The operator would connect to the City corporate network using a VPN connection and then log on to the DMZ Terminal server using a username and password. View only access would be provided with this architecture.

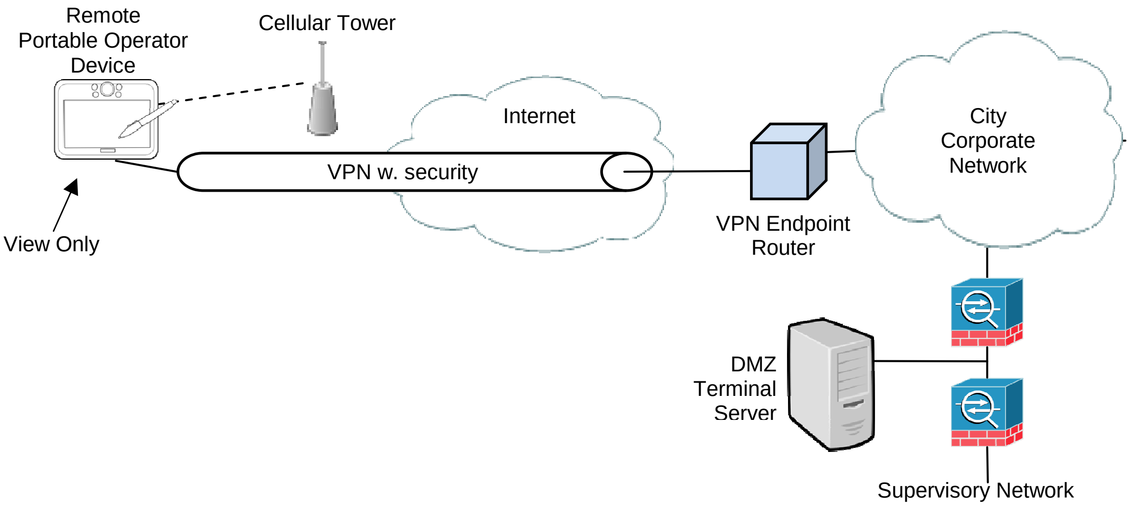


Figure 12-11 : Mobile Operator Remote Access – View Only

12.11.2 Mobile Operator Remote Access – Control Capable

The second type of remote access is similar to that described in the previous section, except that the portable device is also capable of remote control. The proposed architecture to implement this is shown in Figure 12-12. In this case, the remote portable operator device must be considered as trusted, and it is recommended that a hardened device is utilized, with minimal other services enabled. Two-factor security (See Section 15.2.1) must be utilized to ensure that access is not easily compromised, as in this case the access is direct to the HMI Network, and is not brokered through the DMZ Zone. Further discussion of the security requirements is contained within Section 15.0.

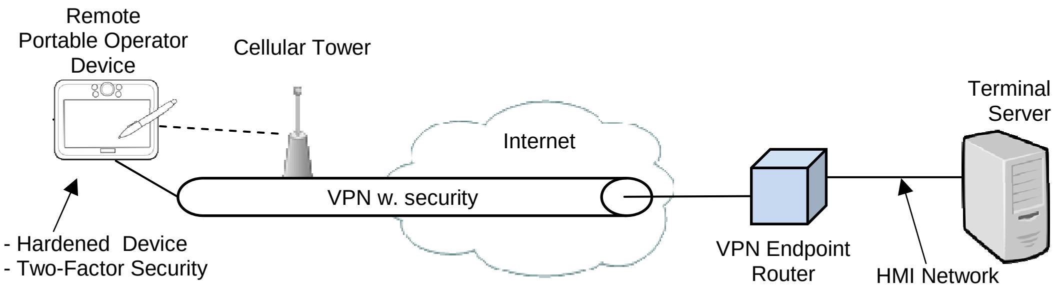


Figure 12-12 : Mobile Operator Remote Access – Control Capable

It is recommended that the City review the requirement for remote, control capable, operator access, and only implement if required.

12.11.3 City Employee Remote Access – View Only

Remote access would also be useful to City employees to view the current status of the wastewater treatment operations. This access could be utilized by supervisors, engineers, or maintenance personnel. The proposed architecture to implement this is shown in Figure 12-13. Access would be provided to users with appropriate user/password authentication. It should also be noted that the number of simultaneous users would be limited to the number of licenses allocated.

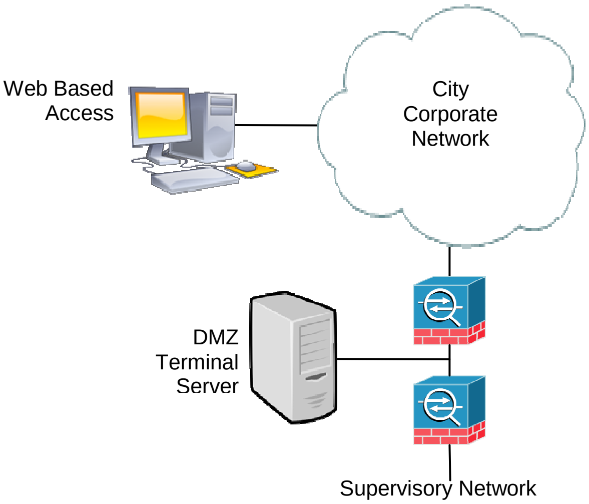


Figure 12-13 : City Employee Remote Access – View Only

12.12 Collections System Integration

The City of Winnipeg maintains an independent SCADA installation to monitor the wastewater collections facilities, which includes the lift stations that deliver the wastewater to the treatment facilities. The Collections facilities are currently monitored by a separate operations group, and thus these facilities have historically been segregated.

Data that would be useful to Collections personnel include:

- Current and historical raw sewage flow at each treatment facility.
- Any alarms or conditions that would limit the ability of the treatment facility to accept wastewater.

Data from the Collections system that would be useful to the treatment plant operations personnel include:

- Rainfall data
- Operational status of significant lift station facilities, such as Community Row Lift Station.
- Lift station discharge flow rates or wet well levels.

The sharing of this data between groups can potentially be implemented via various methods. One would be to provide OPC interfaces between the Collections and Wastewater systems, and allow each system to pull data from the other system. The advantage of this scenario is that the data could be integrated onto native HMI graphic windows.

An alternate method of sharing data between the groups can be implemented through the use of thin client technology, where remote access to the other group is provided via terminal server, view-only client. The advantage of this system is that it would be more straightforward to implement, with significantly less development and maintenance, and would allow for the sharing of any data available on each HMI system. Unless there is a specific requirement for a more integrated environment, it is recommended that this technique be utilized for communication between the systems.

It is also recommended that the City investigate the concept of utilizing a common central data historian for the wastewater collections and treatment systems. This is discussed further in Section 13.4.

Further details regarding the Collections SCADA system are available in the report *Wastewater System SCADA Study*, prepared by SNC-Lavalin Inc. and dated April of 2012.

12.13 Enterprise System Integration

12.13.1 Introduction

The integration of the HMI with enterprise systems is desired to improve the efficiency of the overall wastewater treatment operations, maintenance, and management. Historically, automation systems and enterprise systems were implemented as separate islands, with no automated integration, other than perhaps manual data entry. Significant industry effort within recent history has been made to develop solutions that allow for more straightforward integration of the enterprise and automation systems.

Three enterprise systems within the City of Winnipeg organization have been identified as potential candidates for integration.

12.13.2 Computerized Work Management System

The City has a Computerized Work Management System (CWMS) that tracks assets and work orders, and is utilized extensively by the maintenance personnel in the wastewater treatment facilities. The City's current system is based upon the Oracle Work and Asset Management Implementation (WAM), that was previously identified as Synergen. It is desired that there is a level of integration between the CWMS system and the automation system. Desired features include:

- Abnormal events, such as an alarm or a high process level, can be configured to automatically generate a work order with the appropriate parameters.
- Utilize equipment runtimes to generate work orders with the appropriate parameters.
- Manually initiate a work order from the HMI. (lower priority)
- View work orders for specific equipment from the HMI. (lower priority)

It is recommended that as part of the process to select a control system vendor, the vendor be requested to propose the method of implementation of an interface with the Computerized Work Management system, and the corresponding costs. The vendor's response will be evaluated based upon the proposed integration method, references of similar systems, and cost. While it is expected that there will be a means of integration with most vendors, some may have significant advantages in available integration software.

While the integration of CWMS is expected to be useful, it is expected that there will also be a significant cost to integration. At this stage cost estimation is extremely difficult, as the details of the existing CWMS system are unknown. An order of magnitude estimate is $500,000 provided that a base transaction broker has been installed.

12.13.3 Laboratory Information Management System

It is desired that the Laboratory Information Management System (LIMS) is integrated with the automation system. It is understood that the City's current LIMS installation is a custom implementation based upon a database backend. The primary purpose of the integration would be to share data. It would be useful to see information, such as the latest effluent quality analysis, appear directly on the HMI to provide operations personnel with more direct feedback of the overall facility performance. Entry of the LIMS data into a common database with plant operational data would allow for reporting to search for correlations between operational events and sample quality.

It is recommended that as part of the process to select a control system vendor, the vendor be requested to propose the method of implementation of an interface with the LIMS system, and the corresponding costs. The vendor's response will be evaluated based upon the proposed integration method, references of similar systems, and cost. While it is expected that there will be a means of integration with most vendors, some may have significant advantages in available integration software.

While the integration of LIMS is expected to be useful, it is expected that there will also be a significant cost to integration. At this stage cost estimation is extremely difficult, as the capabilities of the existing LIMS system are unknown. An order of magnitude estimate is again set at $500,000 provided that a base transaction broker has been installed.

12.13.4 Process Control Management System

The City has identified the requirement for a process control management system, which is intended to improve decision making for maintenance and liquid/solids process control. As part of this process, it has been proposed to create a computerized data management system to enhance communication of process performance to management and provide a secure repository with auditable entry activity. This system will reduce the time required by management and operations to analyze and communicate critical process information. The Project Plan for this initiative identified three potential options for implementation of the computerized system: a stand-alone database designed specifically for water information management and process control, utilization of the automation system HMI and associated components, and utilization of existing enterprise systems.

Decisions regarding integration of the process control management system are beyond the scope of this report, however it is suggested that integration of this system with the automation system is deemed to be beneficial.

12.13.5 Implementation Methodologies

Integration of automation and enterprise systems has historically been difficult due to proprietary technologies utilized with each system. However, current implementations of automation software typically utilize a significantly higher level of open components that allow for more straightforward implementation. The use of relational databases and open communication utilizing OPC has significantly opened the door for integration. However, there are significant differences between automation system interfaces and enterprise system databases, and communication between them has significant potential for difficulty.

The industry as a whole recognized this integration challenge and the ISA-95 series of standards have been developed to aid in integrating enterprise systems and automation systems. The standards can provide guidance in the development of the specific requirements, as well as provide a basis for the development of systems, as it defines common object models for integration. It should be noted that ISA-95 is somewhat oriented towards manufacturing, however there is expected to be sufficient common ground to merit its use.

Where pre-packaged solutions are identified, it is recommended that one of the evaluation criteria should be ISA-95 compliance. Where custom solutions are developed, it is recommended that ISA 95-be referenced and utilized to the greatest extent possible.

12.13.6 Enterprise System Integration Recommendation

There is potential benefit to CWMS and LIMS integration. However, at this point the City has significant challenges ahead with the wastewater treatment plant upgrades and integration of these enterprise applications is of significantly lower priority compared to most other work identified within this report. Given that the cost of integration is also expected to be significant, and the City's personnel resources are stretched with current projects, it is recommended to take a phased approach. The control system selection process should identify enterprise system integration requirements in the control system specification as desired capabilities and the vendors would be required to submit proposals with capabilities, along with cost estimates. It is expected that some of the vendors will offer add-on software packages that can be utilized in the integration design process. These capabilities would be included in the evaluation, to maximize future integration capabilities. Where the vendor offers a specific software package to aid in enterprise integration, it is expected that this software would be purchased with the control system to allow for the proposed integration. An example of enterprise integration software is the Wonderware Enterprise Integration Application. The second phase would be to develop the specific integration applications to meet the City's requirements at an appropriate date subsequent to the initial installation.

Ultimately, it is the goal of the enterprise system integration to have a single point of entry, or collection, for all data.

12.14 Advanced Model Predictive Control

Model predictive control is an advanced method of process control where a model of the process is created to predict the future output behaviour, and this output is in turn utilized to provide improved control to the process. For example, in a wastewater application, a model of the facility process could potentially be created to estimate one or more effluent quality attributes. This can in turn be utilized to better control the process. Typically, effluent quality is difficult to implement as part of a control strategy, due to the significant lag time associated with laboratory analysis of samples. The model predictive control can potentially create a simulated on-line measurement of effluent quality, which can then be utilized in the control strategy.

Model predictive control can be utilized on a small or large scale. On a smaller scale, it could potentially be programmed into the PLCs as part of the control strategy. For example, a model of an aeration system could be created to estimate total blower demand based upon process requirements, and adjust blower air production prior to waiting for the pressure to drop. The advantage of model predictive control in each of these cases must be assessed, to see if there is significant benefit compared to simpler control strategies such as PID control loops.

On a larger, more complex scale, modelling of wastewater effluent quality is not a straightforward task. At least one commercial vendor has a proprietary solution that utilizes empirical measurements to develop a software model. A data logger is attached to the control system to log data, which is then analyzed at the vendor's facility, and a software model is produced. This software model can run on an independent computer and interface with the control system. Typically this is a high level control strategy that acts more as an "advanced operator" then a fast control loop. The system can change control loop setpoints to try to maximize the desired "off-line" variables, which are estimated by the software model.

It should also be noted that the potential "off-line" process data associated with model predictive control is primarily expected to be data associated with LIMS and the Process Control Management System, discussed in Sections 12.13.3 and 12.13.4.

At this time, the requirement for model predictive control at the wastewater facilities has not been established; however the City would like to ensure that the capability to install this in the future is provided. Simple model predictive control can be implemented in almost any PLC, and is not expected to be a defining issue between vendors. Complex model predictive control typically can involve a 3rd party vendor, and the use of a standard interface such as OPC. OPC support would be specified as part of the control system selection, however once again, most vendors support this, and it is not expected to be a significant issue.

13.0 HISTORICAL DATA AND REPORTING

13.1 Overview

Historical data collection and archival will be addressed via the installation of historian systems at the wastewater treatment facilities. The historians will store data in a manner that allows for straightforward data analysis and information sharing, including advanced trending and reporting capabilities.

13.2 Logging Requirements

Retention of and access to historical data is essential for the operation and maintenance of the wastewater treatment facilities. Historical data can typically be viewed as the specific set of values of a process variable at some time in history, or summary data such as the average flow for a day. In addition, it is also typical to log event data, such as process alarms and operator actions.

Historical data is useful for analysis, and can be utilized for the following purposes:

- Process analysis and optimization
- Predictive and preventative equipment maintenance
- Health and safety reporting
- Operations reporting
- Compliance reporting against licensing requirements
- Failure analysis
- Basis for future upgrades and enhancements to the facilities.

The automation system historian will provide storage and retrieval of historical data. The historian can be configured to store a massive amount of historical data. However, it is poor design practice to historize and archive more data than necessary, as this can lead to unnecessary system hardware and maintenance costs as well as difficulties associated with the management of excess data.

Types of data, along with examples, that should be considered for historical data logging are identified in Table 13-1. Note that the identified data is high-level and further refinement is required to provide systems integrators with the required information to clearly define historian and logging requirements. It is recommended that a Historical Data Retention Standard be created, which will formally document the City's requirements for storage and retention of historical data. This is discussed further in Section 18.4.4.

Table 13-1 : Data Logging Requirements

Item	Type	Examples	Uses	Suggested Retention
Alarms	Δ	P-G101 Bearing Temp High SF-S630 Run Fault	Maintenance	10 years
Significant Operator Actions	Δ	P-G101 Manual Start EF-P642 Alarm Reset SG-G302 Manual Close	Maintenance Operations Forensic Investigation	3 years
Daily Plant Process Variables	d	Total Plant Flow – Day Min/Max/Avg Effluent Temp. – Day Min/Max/Avg	Operations Planning	Indefinitely
Plant Process Variables	m	Total Plant Flow Influent Temperature Bank 1 Electrical kVA	Operations Planning	10 years
Major Equipment States	Δ	P-G101 Raw Sewage Pump Running	Maintenance Operations Future Design	5 years
Major Equipment Process Variables	ΔDB	FT-G1011 Raw Sewage Pump Flow FV-S251 Position MCC-M01 Current		5 years
Minor Equipment States	Δ	Sump Pump Running	Maintenance Operations	1 year
Minor Equipment Process Variables	ΔDB	Heat Recovery Flushing Water Discharge Temperature	Maintenance Operations	1 month

Legend:

-	Not Logged
Δ	Delta – Logged on change
ΔDB	Delta – with a deadband
d	Logged daily
h	Logged hourly
m	Logged every minute
s	Logged approximately every second

It should also be noted that in addition to the data itself, a data quality attribute should also be logged together with the data. If a sensor is offline, or providing poor quality readings, the historian can be then configured to filter, or qualify, the data based upon quality. If quality attributes were not to be provided, this could impact the accuracy of potential report data, and possibly lead the reader into erroneous conclusions if the quality issue is not identified manually.

13.3 Reporting Requirements

Efficient access to historical data is just as important as the logging of the information. Information that is inaccessible or requires excessive effort to obtain is just as ineffective as not recording the information. Data reporting requirements are commonly under-specified and poorly delivered in automation systems. The Functional Requirement Specifications, discussed in Section 19.3.11 must fully specify the reports required, along with the detailed report format requirements. A sample of a concise method to specify basic reporting requirements is shown in Table 13-2, however it should be noted that for complex reports additional information would be required, along with a sample report.

Table 13-2 : Sample Report Specifications

Report	Fields	Filters	Format
Alarm History	Date/Time, Tagname, Equipment, Description, State	Date & Time Equipment Tagname	1 row per alarm
Alarm Frequency	Tagname, Equipment, Description, Total Alarms	Date & Time Equipment Tagname	1 row per alarm, group by equipment, Summary line for each equipment, Summary line for report
Audit Trail	Date / Time, Operator, Item, Event	Date & Time Operator Event	1 row per event
Plant Flow - Daily	Date / Time, Min Flow Rate, Avg. Flow Rate, Max Flow Rate, Total Flow	Date & Time	1 row per day, Summary line
Runtime Totals	Equipment, Total Runtime	Date & Time Equipment	1 row per equipment

Specific features that should be available from the reporting system include:

- Ad-hoc report generation.
- Ad-hoc trend generation.
- Automatic generation of scheduled reports, including e-mailing to a predefined list of recipients.
- Reports generated in a presentable PDF format, and can subsequently be printed or saved.
- Data export to Microsoft Excel capability.
- Access to the reports via a web interface.
- Advanced trending capability

13.4 Architecture

It is proposed to install a site historian at each site to log local site data at a fairly high resolution. Data would then be replicated to the Central Historian Server for long term archival and retrieval by other City users. The data replicated on the Central Historian Server would not necessarily need to be the full set of data contained on each Site Historian, but could be selected information designated for longer term storage, and as required for access by general users. It is expected that the Central Historian Server will be located at the location for the central control room, which is assumed at this time to be the NEWPCC facility. The Central Historian Server would be connected to the networks within a De-Militarized Zone (DMZ), to isolate external City corporate traffic from the automation system network. It should be clarified that access to the DMZ would be via the City's corporate network, and not via the general Internet. It would not be acceptable to locate the Central Historian Server in a manner such that it is accessible to the general public. Access to the historian would be either through a web server, also located within the DMZ, or direct to the historian, as required.

The proposed architecture is presented in Figure 13-1.

It should also be noted that the City may consider utilizing the Central Historian Server for archiving historical data from the Collections SCADA system. Further discussion regarding the specific details of this configuration would be required.

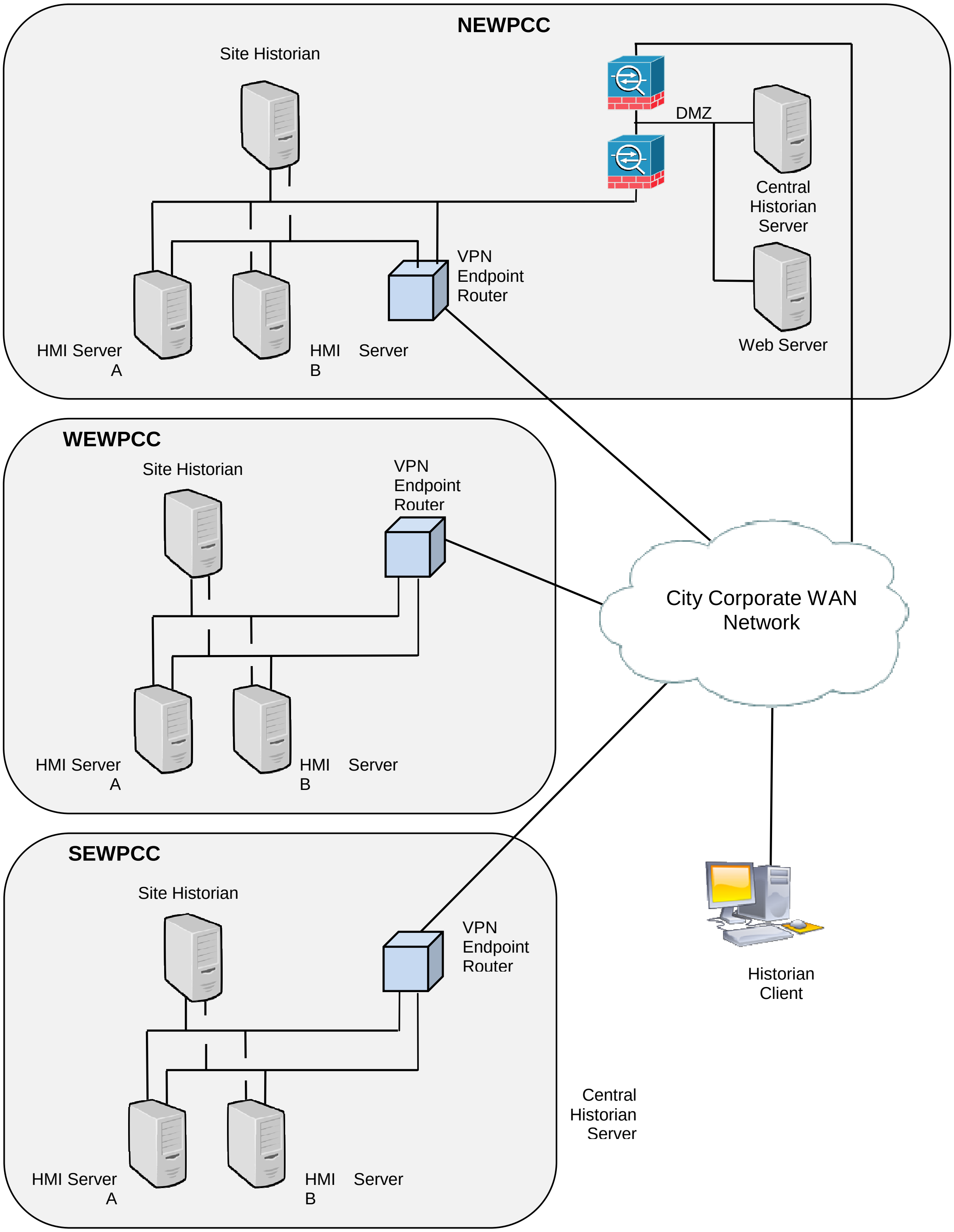


Figure 13-1 : Historian Architecture

13.5 Backup Requirements

The historical data logged will have significant value, and appropriate precautions are required to ensure that the data is preserved in the event of a system failure. Specific attributes that should be included in the system design and implementation are as follows:

- A local historian server should be located at each facility, and replicate data to the Central Historian Server, located at the Central Control Centre facility.
- Each historian should utilize a RAID hard drive array and redundant power supplies.
- The Central Historian Server should be appropriately backed up to a physically independent location.
- The HMI server system should be set up in a manner that if the local historian is not active, the historical data will be locally stored until the historian is active (store and forward).

14.0 NETWORKING

14.1 Network Requirements

Networking is the interconnection of computers, PLCs, and other field devices. This section is limited to discussion of Ethernet based networks, which will be utilized extensively within the automation system, as well as for numerous other purposes within the wastewater facilities. The primary advantage of an Ethernet network is that it provides a standard, well established means of communication. In commercial buildings, it is not uncommon to have a single integrated physical Ethernet network that handles all functional requirements, although some logical segregation of the network may be required. However, in a wastewater treatment facility, as in other industrial environments, use of a single physical Ethernet network is not appropriate. Figure 14-1 present some significant applications within the wastewater treatment facilities that will utilize Ethernet networks, along with the physical network that is proposed to service each application.

The first physical Ethernet network proposed is the Admin network, which will be utilized for general office integration, as well as non-automation applications such as CWMS. It is expected that the City’s IT group will be involved with the planning for this network, and will be responsible for the maintenance of it. Installation of the network wiring will be a very significant part of the Admin network cost, and thus it is recommended that the automation design teams provide networking cabinets and cabling allocated for the Admin network.

The next Ethernet network proposed is the Security network. While it could potentially be integrated with the Admin network, there are two distinct advantages to segregation: bandwidth and security. The use of the security network for the actual security system and public address is expected to comprise only a minor portion of the network capacity, however the bandwidth requirements of Ethernet video can be significant. In addition, it is expected that the Admin network will be the least secure physical network, with access ports distributed in offices and other less secure areas of the facility, and it is not desired that someone could easily access or disrupt the data on the security network. While the use of VLANs, which segregate a physical network into separate secure logical networks, presents a potential configuration that could reduce hardware and cabling requirements, this is not ideal from a security perspective. For example, it is deemed too easy to misconfigure a switch's VLAN configuration upon switch replacement and open a potential security hole.

Table 14-1 : Proposed Ethernet Physical Network Segregation

	Physical Network					
Application	**Admin**	**Security**	**Supervisory**	**Process**	**Field**	**Notes**
CWMS	Y					
General Office Use	Y					Includes internet access, e-mail, etc.
Historian Server			Y			
HMI Clients			Y	Y		VLAN segregated
MCC Integration					Y	
PLC - PLC				Y		
PLC - HMI			Y	Y		
Public Address		Y				
Remote I/O					Y	Physically segregated, typically limited area.
Security		Y				VLAN segregated
Video		Y				See Note. Potentially VLAN segregated
Voice (Telephone)	Y					VLAN segregated

Note: *The networking requirements for video can be significant and are dependent upon the number of cameras, resolution, frame rate, and compression. For example, 20 standard definition cameras, with a frame rate of 2 fps, and MPEG-4 compression is estimated to have a bandwidth requirement of 4 Mbps. However, if the same 20 cameras were high-definition 2 megapixel cameras with a frame rate of 15 fps and H.264 compression, the bandwidth requirement would be approximately 195 Mbps, or ~20% of a gigabit network connection.*

The Supervisory network is within the domain of the automation system, and is expected to be physically located in the facility main area server and control rooms. It would connect the

HMI servers, directory servers, historians, domain servers (as required), as well as the HMI clients within the control room area. However, it should be noted that while the HMI network is carried over the physical Supervisory network, it is logically isolated using VLANs.

The Process physical network is utilized to connect the PLCs and HMIs, and has been significantly discussed in Section 10.0. Note that the HMI client traffic over this network is segregated via a VLAN. The Process Network must be completely physically segregated from the Admin and Security Networks.

The Field physical network is utilized to connect the PLCs to field devices and motor starters, and has been significantly discussed in Section 10.0. It is recommended that in the near future, this network is physically separated from all other networks due to the criticality of this network.

14.2 Wide Area Network Communications

Site to site communications are utilized to connect remote trusted networks together, in a manner that allows them to communicate as if they were local. It is proposed that the NEWPCC, SEWPCC, and WEWPCC facilities utilize dedicated VPN network connections to join the automation networks. The proposed wide area network (WAN) architecture is presented in Figure 14-1. Note that while the automation networks must be segregated from that administration and security networks, the details of the segregation are not clearly identified. It is expected that all networks will be routed over a common WAN network, which may be provided by a 3rd party. While security may be provided on the overall channel for City communications to the site, it is expected that additional segregated VPN channels are created with endpoints at the wastewater facilities, to provide dedicated security for the automation communications, and isolation from the other networks.

The bandwidth requirements for site to site links will be dependent upon numerous factors that are not yet well defined. At this time it is estimated that the automation system requirements for the SEWPCC and WEWPCC facilities will be a minimum of a 100 Mbps connection for each, and a 200 Mbps connection to the NEWPCC. However, these bandwidths do not include included administration and security network requirements, which must be added to the overall WAN link bandwidth requirements.

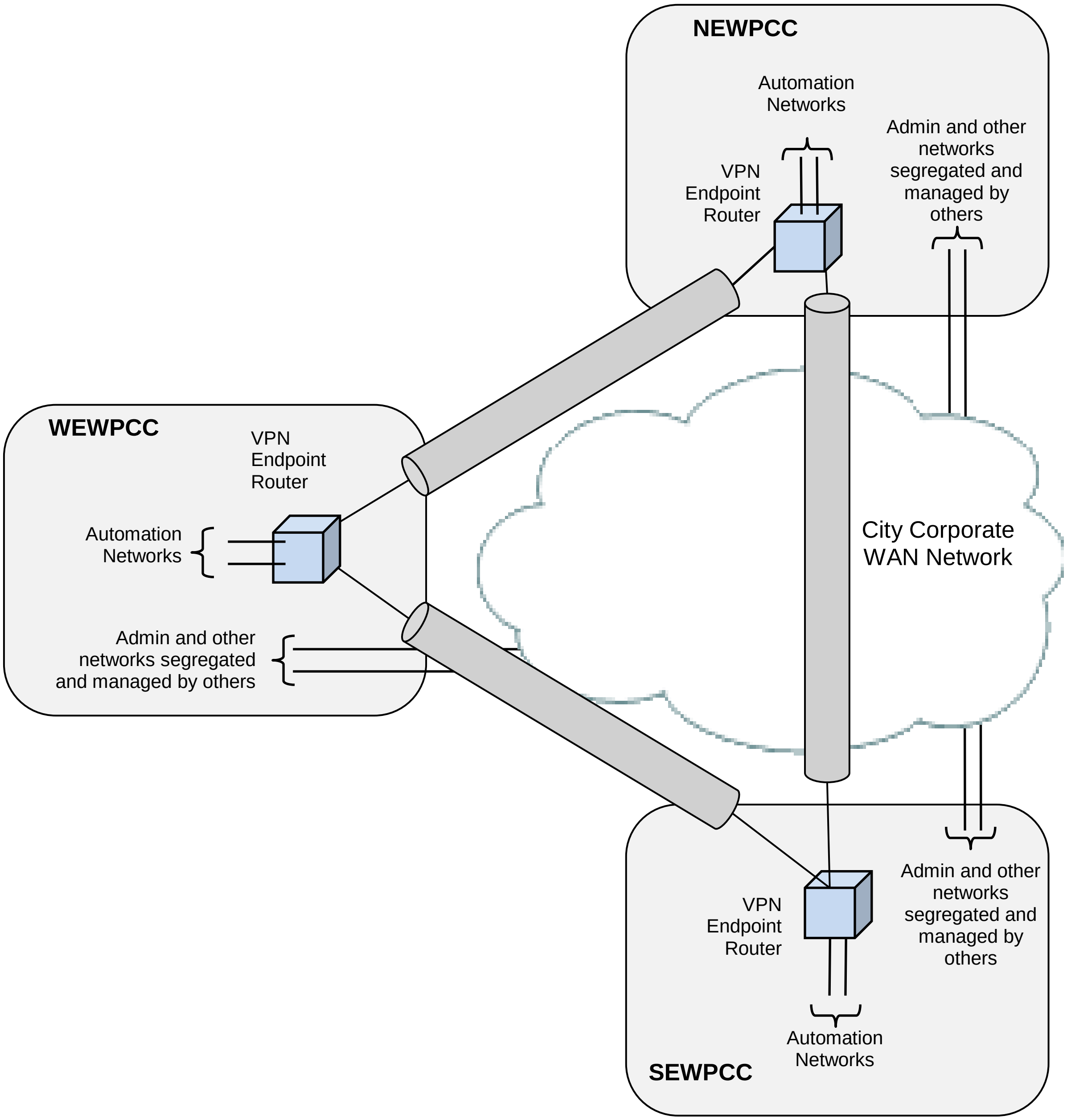

NEWPCC
Automation Networks
VPN Endpoint Router
Admin and other networks segregated and managed by others
WEWPCC
VPN Endpoint Router
Automation Networks
Admin and other networks segregated and managed by others
City Corporate WAN Network
SEWPCC
VPN Endpoint Router
Admin and other networks segregated and managed by others
Automation Networks

Figure 14-1 : WAN Network Links

Availability requirements are expected to be above 99.9%, with less than 8 hours per year of downtime. In addition, it is expected that the links will not be dependent upon any single central point. For example, in the event of a failure of the NEWPCC facility, the SEWPCC to WEWPCC facility communication should remain available.

It is expected that the City’s IT division will be responsible for setting up and maintaining the overall WAN links, however significant coordination with the automation designers will be required to establish the appropriate VPN connections between the sites.

14.3 Demilitarized Zone

The demilitarized zone is a commonly utilized technique to segregate networks in a secure manner. The demilitarized zone provides a network where data can be shared between the automation system and the enterprise systems. Ideally no network traffic is allowed to directly cross the demilitarized zone between the automation and enterprise systems. The most common application of a demilitarized zone is on an organization’s interface to the outside world, where public web servers are placed in the DMZ.

Relative to automation installations, the City’s corporate network is considered untrusted, and it is recommended to utilize a DMZ approach to communications between the automation system networks and the City’s corporate network. This DMZ zone however would not be accessible via the general public Internet, unless a VPN connection to the City’s corporate network is established.

It is expected that the primary automation DMZ will be established at the Central Control location, which at this time is assumed to be the NEWPCC facility. It is proposed that the DMZ at this location house the automation web server, Central Historian Server, and any enterprise integration applications developed.

14.4 Process Area Network Layout

The configuration of a typical process network panel, which will be located in the individual facility process areas, is shown in Figure 14-2. Note that the Admin and Security networking are in separate enclosures, with the exception of the fibre cabling and termination. As part detailed design, it is expected that the automation discipline engineers will allocate and provide fibres for the Admin and Security networks, as well as provide wall space for the Admin and Security networking panels. Note that the Field Network switches could potentially be located within the process network panel, however this would be dependent upon the specific design requirements of each process area.

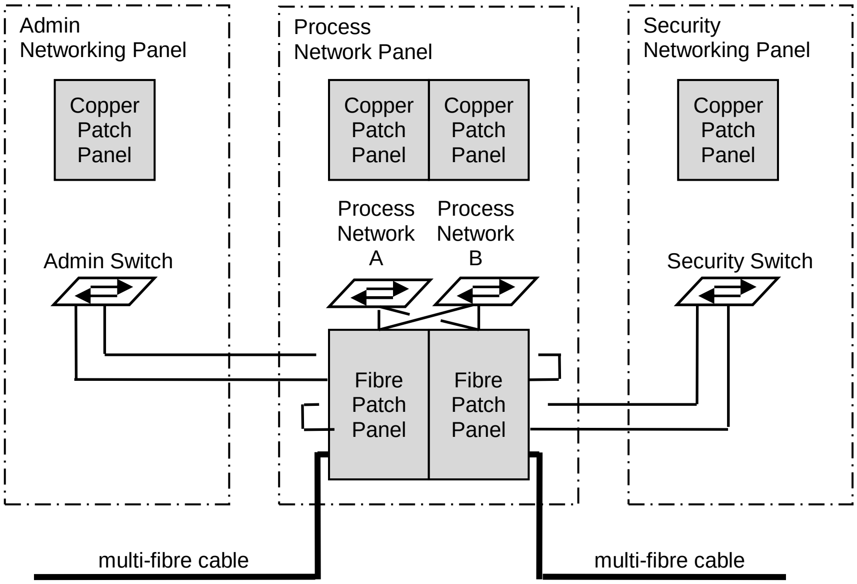


Figure 14-2 : Process Area Network Panel Configuration

14.5 Wireless Integration

Wireless device integration is becoming increasingly common in industrial automation networks. Wireless devices can typically be classified into two categories: interactive devices, such as laptops, tablet PCs and smartphones, and field devices, such as a wireless level transmitter.

Interactive devices typically utilize communication based upon the IEEE 802.11 wireless Ethernet standards. It should also be noted that interactive devices can also communicate over cellular phone based networks, however this utilizes an external network and is discussed separately in Section 15.0. Local implementations of IEEE 802.11 wireless networks are relatively well understood, and the primary issue that must be resolved relates to security. It is expected that basic monitoring and control from a wireless handheld device will be useful to wastewater operations personnel.

On the other hand, wireless field instrumentation devices are typically based upon IEEE 802.15.4 wireless radio, and the ISA-100 and WirelessHART standards are becoming adopted to provide a consistent communication protocols for industrial wireless devices. As discussed, in Section 6.1.4, the primary rationale for utilization of wireless field devices over wired instrumentation is to reduce wiring costs. Given the limited distances within a wastewater treatment application, it is expected that most field devices will be hard-wired. Where wireless field devices are deemed to be appropriate, they should be integrated at the Level 0/1 level with a dedicated wireless ISA-100 or WirelessHART access point.

The integration of wireless systems into the overall facility network must consider the reference model for the control system architecture discussed in Section 10.1. Wireless field devices would be a Level 0 device. For a portable interactive device, a mini-HMI screen would be a Level 2 (Area Supervisory Control) interface. The Level 2 wireless network is essentially an extension of the process control (Level 2) network.

It is proposed that the Level 4 functions such as e-mail and enterprise network access be on a separate network from the Level 2 supervisory control functions. While it may be desired to utilize the operator portable device for e-mail or other business functions, this would be a Level 4 (Site Business Planning and Logistics) interface, and would open the device to potential security issues. It is not recommended that any operator device utilized for control be allowed to communicate directly with an enterprise network.

The proposed wireless device integration is shown in Figure 14-3. The advantages of this approach include the following:

- Avoids cross boundary issues of responsibility between business IT personnel and control system networks.
- Allows for implementation of appropriate security policies for each level of integration.

It should be noted that appropriate security is required on all wireless access points to ensure that unauthorized access is not permitted. This is discussed further in Section 15.0.

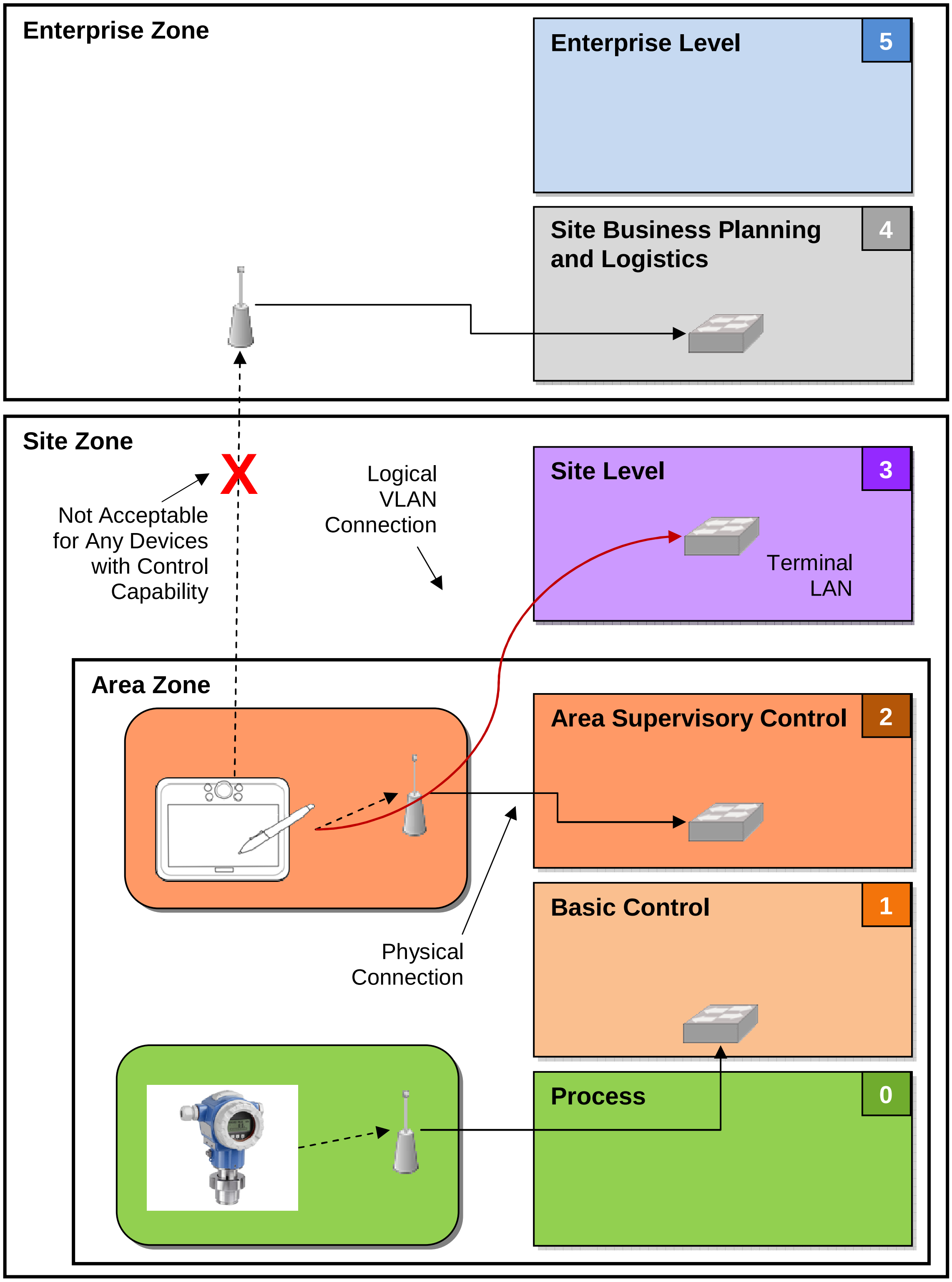


Figure 14-3 : Wireless Device Integration

14.6 Maintenance Responsibility

The responsibility for maintenance of networks in industrial facilities is not as clear as it once was. Approximately fifteen to twenty years ago responsibility was simply divided, with Ethernet networks being the responsibility of the IT group, and control networks were the responsibility of the automation maintenance group. However, in current control system architectures, the Ethernet network can extend right down to the individual motor starter or instrumentation device, and the responsibility boundaries are not necessarily clear.

The City's IT group is well qualified to set-up and service business information systems, and the associated Ethernet networks. However, IT personnel are not typically trained in automation and control systems, and the specific associated networking requirements. Despite the fact that the HMI software is installed on computers and utilizes networks that are physically very similar to business systems, there is a much higher level of availability required of an automation system. One of many potential scenario that could cause problems is automatic security patching of computers by the IT group. The best of intentions could be made by IT personnel to patch the HMI computer's operating system with the latest security patch; however, this could result in the abnormal operation or even potential failure of the HMI system, which may have issues with a specific operating system patch. A second example is the potential misconfiguration of the IGMP Snooping protocol on a managed switch, which could cause an overload on a network utilizing Ethernet/IP and disrupt control. Only personnel trained and experienced with the specific automation installation should provide the ongoing services. It is expected that training of the City's maintenance personnel regarding setup and maintenance of Ethernet networks will be required.

However, IT involvement is not totally excluded, and it is appropriate that IT personnel are included in the following:

- Planning,
- Setup of the demilitarized zones,
- Interfaces with Enterprise networks,
- WAN / VPN connections between facilities,
- Security audits, and
- Common training initiatives on networking.

14.7 Design Criteria

Following are the design criteria that are to be utilized for automation networking design:

- Fibre optic networking
    - Fibre optic networking should always be utilized in the following scenarios:
        - Where distance exceeds 100m.
        - Where there is potential for the systems to have different ground potential.
        - Where there is a significant concern regarding electrical isolation or electrical noise immunity.
    - All segregated physical networks may utilize fibres within a common fibre cable assembly.
    - It will be typical that the fibre patch panel in each process area will be common to all physical networks, to allow for the use of multi-fibre cables for multiple services. However in some cases, the fibre patch panels will be separated, and this would be evaluated on a case-by-case basis.
    - All horizontal fibres are to be terminated in a patch panel by an appropriately trained fibre termination technician.
    - Buried networking cable is to be located in a concrete reinforced ductbank. This allows for straightforward replacement of cables and is less likely to be damaged by unstable soil conditions.
- Copper networking
    - Utilize patch panels at the main server room and the primary area switches. Patch panels are not necessarily required at a PLC control panel.
    - Critical copper network cables are to be located in metallic conduit.
    - Review network routing to ensure that copper networking within corrosive process areas does not significantly affect the reliability of the automation system.
- Network Power Supplies
    - All main server room and primary area switches should have two power supplies, one from UPS power, and the other from non-essential power
    - All MCC switches and other critical field network switches should have two power supplies, one from UPS power, and the other from the nearest non-essential panelboard.
    - Power supply monitoring is required for all dual powered switches. This monitoring may either be external, through hardwired relays on the switch, or via a network connection to the HMI. Switches with Modbus TCP and/or Ethernet/IP communication capability are preferred.

- Performance Requirements
  - All switches will be 100 Mbps minimum.
  - Process network links between process areas will be 1 Gbps minimum.
  - Maximum latency of PLC – HMI communications : 500 ms.
  - Maximum latency of PLC – PLC communication: 500 ms, unless special requirements dictate otherwise, in which case the design requirements must be clearly documented.
  - Maximum latency of PLC – Field device communications: 100 ms.
- Where Ethernet based field devices are utilized, the IP addresses of the devices must be automatically assigned a static IP address via a DHCP system.
  - Consider utilizing a system to automatically configure a device upon replacement. Various vendor-based solutions exist, and would be selected based upon the control system vendor selected.
- As discussed in Section 10.9.2, redundant media is recommended for the facility process network. If the redundant media is in a dual ring architecture, a common cable / conduit assembly for the redundant media may be provided as long as the other side of the ring is routed through an independent path.
- Switches and other network equipment for automation networks such as the process network and field network must be in a locked enclosure separate from the other copper networks. If an Admin or Security network connection is required in the process area, it is anticipated that a fibre patch cord would be pulled through a conduit to an adjacent enclosure where the Admin or Security networking switches would be located.
- Network overview drawings, detail drawings, cable routing drawings, and networking panel layout drawings should be provided as part of the detailed design package. This is discussed further in Section 19.3.8 and 19.3.9.
- Consider and deploy time synchronization services.
- Utilize SNMP for network management.
- Physical access to control system networking ports may introduce security risk. This must be managed together with the overall facility security plan.
- Regardless of the immediate use of Ethernet/IP, it is recommended that all network switches on the process network have IGMP Snooping capability to ensure compatibility with Ethernet/IP. In addition, all area process network switches should have port mirroring capability to aid in troubleshooting.
- All network cabling should be separated from power wiring. Minimum separation is a metal barrier in a cable tray.
- For field networks, there are advantages and disadvantages of utilizing managed switches. Where a small, non-redundant network is utilized unmanaged switches allow for quick replacement, without configuration, in the event of a failure. However,

if redundancy, or a significant amount of broadcast traffic is expected to be on the network, managed switches will be required.

15.0 SECURITY

15.1 Overview

As related to the automation system, risks can generally be associated with the following three categories:

- Physical Intrusion
- Network Intrusion
- Virus, Worms, Malware, etc

The level of security risk can be defined through the use of the following equation:

Risk = Threat x Vulnerability x Target Attractiveness x Consequence

For a wastewater facility, the threat is typically largely unknown, the target attractiveness is normally considered to be relatively low, and the consequence can be significant. The vulnerability however is the easiest variable for the City to control, to reduce the overall risk.

15.2 Network Security

Computer networks are complex due to the numerous applications and users that communicate over the interconnected systems. Unauthorized access to computer networks is well understood as a significant security risk, and appropriate network security systems must be established to ensure that the wastewater automation systems remain secure. The end device trust level, design principle, and expected user authentication requirements of various network users are summarized in Table 15-1.

It should be noted that the end device trust level is not necessarily the trust level of the end user. A trusted user using an unsecure device could unintentionally compromise the network, if not implemented with appropriate security.

Installation of network security systems must be balanced with the complexity entailed. In some cases, the security risk does not warrant a complex security architecture, that has associated installation and maintenance costs. It should also be noted that the availability of

Table 15-1 : Trust Level of Network Users

User / Application	End Device Trust Level	Design Principle	User Authentication
HMI General View Access - Users within corporate network	Low	Web Based via DMZ, Read-Only (No Control)	User / Password
Data Web Site – Corporate and External Users	Low-Med	Web Based via DMZ	User / Password
Enterprise Applications (e.g. LIMS)	Low-Med	Via DMZ Zone	User / Password
External Vendors / Systems Integrators (See Note 1)	Med	VPN connection to Network Remote Desktop Connection to Remote Development Server	VPN Credentials + Two-factor authentication
City Technical Maintenance, Off-site	High	VPN Connection to Corp. Network Remote Desktop Connection to Remote Development Server	VPN Credentials + Two-factor authentication
City Technical Maintenance Within Corporate Network – Remote Support	High	Remote Desktop / Terminal Services connection to Remote Development Server	Two-factor authentication
City Technical Maintenance - Local	High	Access via Development Workstation	User / Password
Remote Portable Operator Device – Outside Facility	Med	VPN connection to Terminal Server, VLAN Segregation, Thin Client, Hardened Device	Two-factor authentication
Local Portable Operator Device Within Facility (includes control)	Med-High	Limited Wireless Range, WPA2 or better security/encryption, VLAN Segregation, Thin Client	Wireless Passkey & User / Password
Operations Personnel within Treatment Facility	Med-High	Thin Clients, VLAN Segregation	User / Password
Operations Personnel within Alternate Facility (NEWPCC / WEWPCC / SEWPCC)	Med-High	Thin Clients, VLAN Segregation, VPN Site connection with IPSEC	User / Password
PLCs	High	Connection to LAN	None
Wireless Field Devices	Med-High	Limited Wireless Range, WPA2 or better security/encryption	Passkey
Wired field devices	High	Connection to LAN	None

Notes:

1. *The access of external vendors and systems integrators will require further coordination with the City's IT department. It is envisioned that the access within the automation control system will be similar to that for City technical personnel.*

a network system could potentially be reduced in a high-security environment. Some network security implementations can become complex, and a simple misconfiguration of a network attached device could impede network communications, and disrupt the automation system. Therefore, a balanced approach is recommended.

15.2.1 Two Factor Authentication

Where the risk of compromised authentication is more likely, and the consequences are significant, it is deemed that two-factor authentication is required. Two-factor authentication requires that access is only provided after two out of three authentication factors are provided. The three potential factors are: knowledge, possession, and inherence. The inherence factor usually involves biometrics, and while technology exists, it is more common to utilize the knowledge and possession factors. Typically, a username/password is used as the knowledge factor, and the possession of a smart device is utilized as the possession factor. One example of a smart device, is the RSA SecureID token, as shown in Figure 15-1, where the person requesting access must enter in a regularly changing number shown on the token. Another example of a possession security authentication is to have the remote server call / message the user’s cell phone with the remainder of the authentication process. There are a number of techniques commercially available, and it is recommended that the City review the available technologies and make a selection that is most appropriate for its needs. It is understood that the City IT department has some implementations in place and consultation with the City’s IT department would be appropriate to see if there are potential synergies.

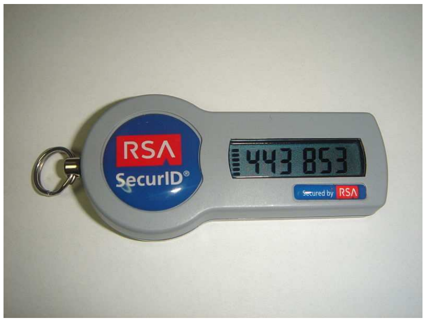


Figure 15-1 : RSA SecureID Token

15.2.2 Connection of Remote Devices

It may be required in some cases to connect remote devices over a physically unsecure connection. An example might be the installation of a small PLC at the wastewater treatment plant outfall, which could be connected to the automation system over an unsecure link. This unsecure link could be a potential weakness in the control system, and implementation of significant security measures on the PLC or its communication protocols is not typically possible.

Where it may be required to connect to a remote site with a simple unsecurable device such as a PLC, a potential solution would be to utilize a VPN endpoint with IPSec (or similar security) to secure the link. The VPN endpoint could be a device such as a small router, and could be physically located within the same enclosure as the PLC or other automation device. An example implementation is shown in Figure 15-2.

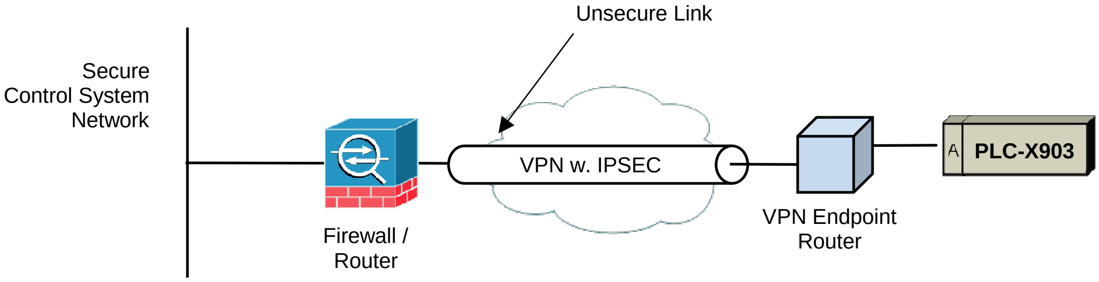


Figure 15-2 : Secure Connection to Remote Simple Device

15.2.3 Local Portable Operator Devices

Wireless operator interface devices are currently being installed in various industrial facilities. Wireless portable devices pose additional security issues compared to stationary devices. Their portability provides additional opportunities for corruption, misuse, or communication interception. For example, an operator could decide to take a portable device outdoors while walking to another building, and could be intercepted while outside the “physical security zone”. While the security requirements of portable devices requires further refinement as part of future work, it is recommended at this stage that local portable devices be utilized within the facility, for monitoring and control, provided that the device is hardened and communicates with the local automation network only.

The wireless radios should be configured in a manner to provide good coverage within the facility, but avoid coverage outside of the facility perimeter. In addition, it is recommended that perimeter security be installed around each facility, which can potentially identify intruders attempting to access the wireless network. It is recommended that as part of a security review, a wireless test system with a yagi directional antenna be driven on all roads around the facility to identify if any area has significant signal strength that could provide an attack opportunity to a network intruder.

15.2.4 Remote Portable Operator Devices

The connection of remote portable operator devices to the automation system is discussed earlier in this document and two architectures are presented in Sections 12.11.1 and 12.11.2 for view only and control capable configurations. It is recommended that control capable remote cellular-based operator devices are only provided if the City deems this is required, as more complex security requirements will apply to devices capable of control. If control is required, it is recommended that only hardened devices be utilized that disable all non-required services, a VPN connection is established to the automation HMI network, and two-factor authentication is utilized.

15.2.5 Wireless Devices and Sensors

The use of wireless sensors and instruments as part of integrated automation systems is increasing. While wireless instruments have the potential to significantly reduce installation costs, their signals are not confined to the physical boundaries of the facility, and thus are more prone to interception. It is recommended to limit the use of wireless communication to instruments where mobility is required or the installation of physical wiring is prohibitive.

15.3 Design Criteria

There are numerous concepts, architectures, and techniques to improve the security of automation systems and Ethernet based networks, and the detailed discussion of the topic is beyond the scope of this document. Some specific design and implementation guidelines for automation system security are identified below:

- General Requirements
  - Establishing security must be an ongoing process, and is not a one-time event.
  - Automation system nodes must not be set-up, updated or modified indiscriminately to meet overall corporate or even vendor policies or guidelines. It is not acceptable to patch a windows operating system immediately on an HMI Server, as soon as the patch is released, as there could be a conflict with the automation software.
  - It is recommended that modifications, such as patch deployment, be performed as part of a managed / planned maintenance process, after appropriate testing is performed.
  - A formal change management documentation system must be implemented.
- Physical Security
  - All facilities will have perimeter security systems, to be part of the facility security system.
  - All buildings will have intrusion detection and access control, to be part of the facility security system.
  - Perimeter security via video or infrared technology should be provided, especially in areas where the local wireless LAN signal strength is sufficient for a wireless attack.
  - All automation enclosures located outside of a building are to be padlocked, and provided with a door switch contact. The door switch would be wired back to the security system, or if more cost effective, could be transmitted to the security system via a digital PLC input in the outdoor enclosure and a relay contact in a PLC adjacent to the security system console.
  - Server rooms are to be locked.
  - The Process network panels are to be locked.
- Network Architecture:
  - The automation system and its networks must be an isolated domain, and not integrated into the overall City of Winnipeg enterprise networks. There will be communication channels between the two domains, however they must be defined, managed channels with appropriate security.

  - The overall City of Winnipeg corporate network must be viewed as an “unsafe” or “compromised” network from the perspective of the automation system.
  - It is recommended to adopt a policy of establishing a secure perimeter around the automation system, to limit the security risk within the domain.
- Network Security
  - Where network ports are in a physically unsecure location, configure port blocking to only allow approved devices to connect.
  - Unless required, disable unnecessary services on the network.
  - Consider using DHCP snooping to prevent various potential IP address attacks on the network; however it should be noted that not all industrial Ethernet switches currently support this feature set.
  - Wireless Security
    - Utilize an encrypted connection for all wireless systems, such as WPA2 or better
    - Ensure the devices with access to the network are secured.
    - Do not ever assume that the wireless network is secure due to low signal strength outside the building. Attackers may utilize high-gain antennas to access the network.
    - Change wireless access passkeys at regular intervals.
- Authentication Requirements
  - Within the wastewater facility (within the security perimeter)
    - Users within the wastewater facilities may generally view but not control without authentication.
    - Authentication is provided by a unique username and password.
  - Outside of the wastewater facilities:
    - All users must be authenticated for access to view any aspect of the automation system (e.g. view an HMI screen).
    - View authentication is provided by a unique username and password.
    - If remote control capability is provided, control authentication is provided by two-factor authentication, which will include a unique username and password, as well as a possession attribute such as a RSA SecureID token.
    - Remote development and support access will require two-factor authentication.
  - User accounts should utilize the following guidelines:

    - Only validated users should have accounts that access the control system.
    - User IDs must have unique names and individual, strong passwords.
    - User access should be limited to the user's requirements.
- Computer Security
  - Use of anti-virus, anti-malware, and similar software should be limited to control system computers on the perimeter of the automation system. For example, it would be appropriate to install this software on a web server, but not on a HMI server, where the anti-virus software could negatively impact the operation of the control system.
- Safety systems should always operate on an *air-gap* principle, where there is no network connection between the control system and the safety system.

16.0 OPERATIONS AND MAINTENANCE CONSIDERATIONS

16.1 Training

Training is a critical component of the proposed wastewater treatment construction and upgrade projects to ensure that operations and maintenance personnel understand the process and equipment installed, and are equipped with the specific knowledge to utilize and maintain the equipment. Specific targeted training will be required for the operations and maintenance groups, with specialized training for in-depth topics.

16.1.1 Automation System General Training – Operations Personnel

As discussed in other sections of this report, it is expected that a new PLC-based automation system will replace the existing DCS at the wastewater treatment facilities. Comprehensive training will be required for operations personnel to ensure that they understand the overall configuration of the system, and are fully versed in the operation of the process using the control system.

Training for operations personnel is to include, but is not necessarily limited to, the following:

- Overview of the new automation system, including the architecture of the system.
- The user interface basics, including security, navigation, alarm system, and trending.
- The organization of the operator screens.
- Control of equipment utilizing the HMI and specific equipment faceplates.
- Modes of control including local and remote, manual / auto.
- Automation system failures, redundancy, and response to failures.

16.1.2 Automation System Training – Maintenance Personnel

Maintenance personnel will require comprehensive training on the configuration and maintenance of the various aspects of the automation system. The depth of training required is quite significant, and it is not expected to be practical to provide comprehensive training to all automation maintenance personnel. It is thus proposed that there will be some level of specialization, and the City will be required to coordinate appropriate training for each member, according to their proposed maintenance role.

It is recommended that general training be provided for all maintenance personnel to ensure that all personnel are provided an overview and general understanding of the entire control system. This would also include training on some basic tasks, such as PLC module replacement.

Typical specialist training would be provided as follows:

- PLC Software Specialist
  - Topics would include PLC programming, configuration, and diagnostics.
- HMI Application Specialist
  - This would include HMI servers, client, historians, web servers, and terminal servers. The training program contents would include setup and configuration, diagnostics and troubleshooting, server replacement, and backup and failover strategies.
- Networking Technician
  - Specialist training for Ethernet networking, which would include setup and configuration , diagnostics and troubleshooting, device replacement, backup and failover strategies, wireless configuration, and security.
- Instrumentation Technician:
  - Specific training would include configuration and maintenance of other fieldbus networks utilized, intelligent motor control centers, intelligent instrumentation, and PLC diagnostics.

It should also be noted that in certain cases, the City may decide to cross-train certain senior personnel, such that they can support multiple roles.

16.1.3 Process Operation Training

It is recommended that the design engineer, or an alternate process expert, provide a component of the training that includes the overall operation of the process, in addition to the specific equipment training typically provided by the contractor or equipment vendor. This training would be comprised of numerous classroom sessions, which would be videotaped for future use.

16.2 Testing and Simulation System

It is recommended that a testing and simulation system be provided to allow for the testing of upgrades, new software implementations, as well as training of operations and maintenance personnel. The system should be set up in a manner such that almost any aspect of the automation system can be demonstrated and simulated, although it is noted that the scope of the simulation system would likely be limited to a portion of the facility at a time. For example, it may not be realistic to model the complete NEWPCC facility at one time, but rather this would be accomplished incrementally in stages by loading specific software configurations on the servers.

It is envisioned that the capabilities of the testing and simulation system will vary, and it is expected that vendor capabilities will be a component of the control system selection evaluation.

It should be noted that only one testing and simulation system is deemed to be required for all three facilities.

A general architecture for the proposed simulation system is shown in Figure 16-1. A terminal server would allow for the connection of thin clients to a terminal server, which in turn communicates with the HMI server. Note that redundancy is not deemed to be required for the permanent simulation system. Depending upon the capabilities of the specific server software installed, it is also possible that multiple servers shown could be installed on one physical server, potentially with the use of virtualization.

A PLC software simulator would run one or more PLC configurations in software. The I/O for the PLC would be simulated by the process simulator, which would be configured with a software model to mimic the operation of the process. For example, if the PLC simulator increased the signal to open a control valve position, the process simulator would correspondingly increase the flow rate. The software process model should automatically adjust the appropriate I/O, however it would not necessarily need to accurately model the exact response of the wastewater process, and a first order simulation is deemed to be sufficient. The process simulator would also include a user interface, which would allow the user to see the status of the process signals, such as whether a valve is open or closed, and modify process and/or I/O conditions to simulate various events. For example, a user could simulate a wet well level sensor failure to the PLC, which could be useful for operator training or for PLC program testing. It should also be noted that use of a process simulator can increase the effectiveness of PLC and HMI configuration testing by a significant factor, resulting in a reduced commissioning time duration.

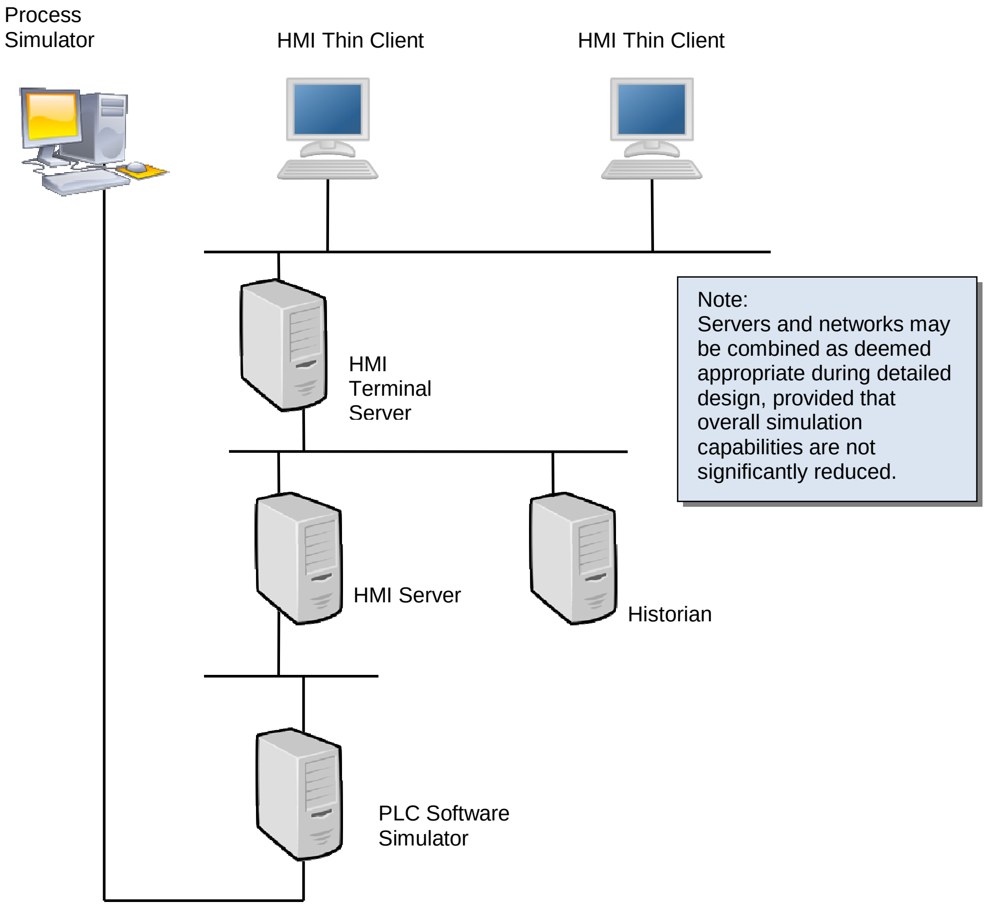

Process Simulator
HMI Thin Client
HMI Thin Client
HMI Terminal Server
Note:
Servers and networks may be combined as deemed appropriate during detailed design, provided that overall simulation capabilities are not significantly reduced.
HMI Server
Historian
PLC Software Simulator

Figure 16-1 : Simulation System

16.3 Other Operations and Maintenance Considerations

Other automation system recommendations, as they relate to operations and maintenance, are as follows:

- It is desired that direct links from the HMI system are provided to operations and maintenance manuals.
- Provide ~20% spare system capacity associated with PLC I/O, processor capacity, power supplies, etc.
- Provide specialty tools required for equipment and instrument maintenance as part of the equipment supply.
- Provide spare parts for equipment. The number of spare parts in stock is to be consistent with the number in service, criticality of the service, time to procure, and expected MTBF.
- The City has expressed interest in using barcodes or QR codes on instruments to ease maintenance and coordination with asset management systems. If the City wishes to implement a system, this would be provided via a separate initiative, as the scope of this system would extend to other disciplines as well.

17.0 EQUIPMENT STANDARDIZATION

17.1 Introduction

The City of Winnipeg has procurement policies that dictate requirements regarding equal access for suppliers to provide goods for the City. However, under certain circumstances where internal efficiencies and cost savings for the City are apparent, it is beneficial for the City to standardize automation equipment vendors for specific equipment. The benefits of equipment standardization depend on the specific equipment, but often include the following:

- Reduced operator training,
- Reduced possibility of operator error due to differences between equipment,
- Reduced training for maintenance personnel,
- Reduced downtime due to maintenance familiarity with equipment,
- Reduced spare part requirements,
- Reduced engineering detailed design costs, as designs can be specific to a vendor and designs can be copied between projects,
- Reduced specification requirements for standardized products as part of subsequent tenders,
- Reduced time needed to evaluate requests for equal during tender periods, and
- Reduced effort and cost for automation integration.

It should also be noted that in some cases, equipment standardization is required for compatibility with existing equipment.

17.2 Existing Equipment Standards

The equipment identified in Table 17-1 summarizes the current state of standardization implemented by the City of Winnipeg Wastewater Department. However, the method of standardization for these products has not necessarily been approved by the City's Materials Management Division.

Table 17-1 : Existing Equipment Standards

Item	Standard Equipment	Method of Standardization	Standardization Benefits
Gas Detection Controller	Draiger Draegergard	Comprehensive Evaluation Report under SEWPCC Reliability Upgrades	More detailed engineering drawings Maintenance Familiarity Training
Gas Detection Sensors	Draiger	Comprehensive Evaluation Report under SEWPCC Reliability Upgrades	More detailed engineering drawings Maintenance Familiarity Training
Uninterruptible Power Supply	Liebert NX Series	Comprehensive Evaluation Report under SEWPCC Reliability Upgrades	More detailed engineering drawings Maintenance Familiarity Increased Reliability Training
Variable Frequency Drives –up to 600V	ABB ACS800 series	Selected by City E&I Dept based upon performance evaluations over a wide variety of installations.	Maintenance Familiarity Training Spare Parts

17.3 Potential Equipment Standards

There are numerous types of equipment that are potential candidates for equipment standardization. The rationale for standardization of a particular type of equipment should be based upon key criteria. It is proposed that the following criteria form the basis of evaluation:

Reliability

Some equipment in the automation domain has varying levels of reliability. Reliability is very difficult to specify, and evaluate as part of a competitive bid process. One of the most effective means to evaluate reliability is through proven use in the application. The significance of this criteria is evaluated based upon the expected level of reliability increase that can be gained by standardizing on a particular vendor and product.

Detailed Engineering Drawing Development

Complex, non-commoditized equipment often has significant differences in the size, implementation, and interface of the equipment. Thus, if the equipment model cannot be specifically identified at design time, it can preclude the ability of the design engineer to provide a complete and detailed design of the installation, and would require the transfer of design responsibility to the contractor, or a two-stage design process predicated upon final equipment selection. Without specific equipment definition, the design drawings can become very general, and are not useful for maintenance or future engineering work at the facility. It can also result in installation and commissioning issues during construction, due to issues that arise from unanticipated differences in equipment. The significance of this criteria is evaluated based upon the difference in critical detail that could be applied to design drawings, if the equipment model is known at design time.

Operations Training and Familiarity

Complex equipment and devices can require significant operator training. Additional costs to the City would arise from time commitments to training and less than optimal utilization and performance that would be attributable to poor product understanding. This criteria is evaluated based upon the level of operator training and familiarity required for successful operation of the equipment.

Maintenance Training and Familiarity

A significant percentage of automation devices require specific training and familiarity to facilitate proper equipment maintenance and setup. It is not efficient or cost effective to require maintenance personnel to be fully conversant with numerous equipment vendor devices for similar applications. Therefore, this criteria is evaluated based upon the level of maintenance training and familiarity required for successful operation of the equipment.

Reduced Automation Integration Time

A significant percentage of current automation devices have significant configurable and flexible software attributes relating to equipment configuration and operation. Proper operation of the complete automation system is dependent upon appropriate configuration, setup, and programming of the configurable aspects of all devices. For example, it may be required to write a different application program within the PLC software to communicate with two different device vendors. There are cost and maintenance disadvantages to providing multiple equipment interfaces. In addition, use of a common vendor allows for reuse of drawings and already proven application interfaces. Thus, this criteria is evaluated based upon the level of vendor specific configuration effort required for automation integration of the equipment into the overall automation system.

Compatibility Issues

Some automation equipment is only operable with other equipment from a common vendor. For example, use of PLC I/O modules from a vendor different than that of the main PLC would present significant compatibility issues, or at minimum loss of some functionality. Therefore, this criteria is evaluated based upon the expected level of compatibility issues expected to be resolved by standardization of equipment.

Spare Parts

Spare parts are evaluated based upon the value of the spare parts, local availability, space requirements, avoidance of duplication, and the ease of replacement with an alternate vendor.

For various automation equipment, the above criteria were assessed and scored on a range of 0 to 5 for each criteria, with a scope of 5 indicating significant value and advantage to the

City arising from cost reduction or use optimization for the particular attribute. The sum of the criteria scores was calculated to provide a general indication of the value to the City for equipment standardization in each specific circumstance. It should be noted that there is a degree of subjectivity in the evaluation, but it does however provide a fairly good general guideline.

17.3.1 Evaluated Equipment

A list of typical equipment required as part of a complete automaton system is presented in Table 17-2 for evaluation of equipment standardization benefit. The list is not comprehensive of all automation components, and excludes all items where it is obvious that standardization provides minimal benefits. For example, automation cables are not included, as there are typically multiple vendors capable of supplying cable that meets the required specifications, with no to minimal effect of the criteria evaluated. It is expected that during the course of any upgrade project, that additional equipment that is not included in Table 17-2 will be identified as a potential candidate for equipment standardization. It is suggested that the criteria presented can be utilized for the future evaluation of other equipment for standardization.

Table 17-2 : Equipment Evaluated for Potential Standardization

Item	Networked	Description
PLC	Y	Programmable Logic Controller or Programmable Automation Controller, including all associated hardware and software. Remote I/O for the PLC would also be included.
HMI Software	Y	The Human Machine Interface would include all associated components including the application server, historian server, and workstation software. Computer hardware would not be included.
VFD	Y	Variable Frequency Drives would be based upon 600V, 6-pulse standard, in a range from 1 – 250 HP. Potential low harmonic drives could be evaluated as part of the standardization.
Intelligent MCCs	Y	Intelligent Motor Control Centers must communicate with the overall control system over a network that must be compatible.
Soft Starters	Y/N	Soft starters would be based upon 600V starters with bypass contactors in a range from 1 – 250 HP.
Protocol Converters / Gateways	Y	Protocol converters and gateways are utilized to connect devices to the control system that communicate via a protocol that is different from the control system's primary native protocol.
Gas Detection System	Y	Gas detection systems must have appropriate CSA approval of the transmitters and controllers, and compatible network communication to allow for full control system integration.
Uninterruptible Power Supplies > 5kVA	Y	Uninterruptible Power Supplies provide continuous power to critical components of the automation system. Reliability is imperative.
Ultrasonic Level Transmitters	Y	Networked ultrasonic level transmitters utilize a fieldbus or Ethernet network to communicate with the automation system.
	N	Non-networked ultrasonic level transmitters typically utilize a 4-20mA signal to communicate with the automation system.
Magnetic Flowmeter	Y	Networked magnetic flowmeters utilize a fieldbus or Ethernet network to communicate with the automation system.
	N	Non-networked magnetic flowmeters typically utilize 4-20mA signal and pulsed discrete outputs to communicate with the automation system.
Valve Actuators – Smaller Quarter Turn	Y	Smaller valve actuators may be electrically or pneumatically operated with on-off or positioning control. Networked versions are controlled and monitored through a fieldbus network.
	N	Smaller valve actuators that are not networked are controlled and monitored via discrete and analog (4-20mA) signals.
Pressure Transmitter	Y	Networked pressure transmitters utilize a fieldbus or Ethernet network to communicate with the automation system.
	N	Non-networked pressure transmitters typically utilize 4-20mA signal to communicate with the automation system.

Item	Networked	Description
Electric Power Meter	Y	Electric Power Meters measure power factor, current, harmonic distortion, and other electrical attributes, and communicate critical values to the automation system.
Valve Actuators – Large Multi-Turn and Quarter Turn	Y	The larger electric valve actuators in this classification are electrically operated with on-off or positioning control. Networked versions are controlled and monitored through a fieldbus network. Two common vendors that have products in this range are Rotork and Limitorque.
Temperature Transmitter	Y	Networked temperature transmitters utilize a fieldbus or Ethernet network to communicate with the automation system.
	N	Non-networked temperature transmitters typically utilize 4-20mA signal to communicate with the automation system.
Network Switches (Managed)	Y	Managed Ethernet switches are configurable and have advanced features to allow for appropriate network configuration.

The evaluation of the identified equipment was performed via a survey of a total of nine individuals from the City of Winnipeg, Veolia, and SNC-Lavalin Inc. The average of the survey values is presented in Table 17-3. Note that in a few cases, survey participants did not feel qualified to comment on a specific type of equipment, and those values are not included in the average.

Table 17-3 : Evaluation of Equipment Standardization Value

Item	Networked	Reliability Through Proven Used	Detailed Engineering Drawing Development	Operations Training and Familiarity	Maintenance Training and Familiarity	Reduced Automation Integration Time	Compatibility Issues	Spare Parts (1)	Score
PLC	Y	3.7	4.3	1.7	4.1	4.9	4.3	3.6	**27**
HMI	Y	3.4	3.5	4.2	4.0	4.7	4.0	3.1	**27**
VFD	Y	3.4	4.2	3.1	4.2	3.8	3.2	4.4	**26**
Intelligent MCCs	Y	3.3	4.4	2.3	4.1	4.0	3.6	4.4	**26**
Soft Starters	Y/N	3.3	3.8	2.3	3.9	3.4	3.3	4.4	**24**
Protocol Converters / Gateways	Y	3.4	3.1	1.1	3.4	4.0	4.3	3.8	**23**
Gas Detection System	Y	3.1	2.8	2.5	3.4	2.6	1.9	3.1	**19**
Uninterruptible Power Supplies > 5kVA	Y	3.0	2.8	1.5	3.3	2.0	1.8	2.9	**17**
Ultrasonic Level Transmitters	Y	2.7	2.7	1.9	3.0	2.4	2.6	3.4	**19**
	N	3.0	2.0	1.8	2.8	1.3	1.7	2.8	**15**
Magnetic Flowmeter	Y	2.6	2.5	1.9	3.3	2.3	2.4	3.0	**18**
	N	2.6	1.9	1.7	3.0	1.3	1.7	2.7	**15**
Valve Actuators – Smaller Quarter Turn	Y	2.6	2.9	2.0	3.0	2.6	2.5	3.0	**19**
	N	2.5	2.3	1.9	2.8	1.5	2.1	2.6	**16**
Pressure Transmitter	Y	2.6	2.5	1.5	3.0	2.4	2.5	3.4	**18**
	N	2.3	1.8	1.3	2.7	1.3	1.7	2.8	**14**
Electric Power Meter	Y	2.4	2.9	1.8	2.8	2.8	2.4	2.0	**17**
Valve Actuators – Large Multi-Turn and Quarter Turn	Y	3.0	3.0	2.6	3.3	3.4	3.0	3.1	**21**
Temperature Transmitter	Y	2.4	2.4	1.4	3.0	2.3	2.6	3.0	**17**
	N	2.2	1.8	1.1	2.6	1.4	1.7	2.4	**13**
Network Switches (Managed)	Y	3.0	3.3	0.9	3.3	3.7	3.4	2.6	**20**

Notes:

1. Spare parts are evaluated based upon the value of the spare parts, local availability, space requirements, and the ease of replacement with an alternate vendor.
2. Electrical Items are included in the above list.

As part of the survey performed, the following additional equipment was identified by some participants as having potential for standardization:

- Analytical Instruments
- Fibre-optic Patchbays
- Test Instrumentation
- Remote I/O

It is expected that these additional items will be evaluated further by the City as the overall wastewater treatment project progresses, and a decision made regarding the potential standardization of these items. Note that Remote I/O could potentially be included under the PLC category and provided by the PLC vendor, but this is not an absolute requirement and in some cases remote I/O from an appropriate alternate vendor may be acceptable.

It is recommended that equipment with a score of 25 or above should be prioritized for standardized selection to ensure that the impairment of the identified criteria can be avoided to the greatest extent possible. Based on the evaluation identified in Table 17-3, the equipment identified includes:

- Programmable Logic Controllers (PLCs),
- Human Machine Interface (HMI) devices,
- VFDs, and
- Intelligent MCCs

In the case of equipment with a score of 20 to 24, it is recommended that a process be implemented to facilitate the early selection of equipment at the front end of the project design. Based on the evaluation identified in Table 17-3, this includes:

- Soft Starters
- Protocol Converters / Gateways
- Network Switches
- Valve Actuators – Large Multi-Turn and Quarter Turn

In the case of equipment with a score of 10-19, it is recommended that a process facilitate selection prior to design completion, to allow incorporation of critical details, should be implements. Based on the evaluation identified in Table 17-3, this includes:

- Gas Detection System
- Uninterruptible Power Supplies > 5 kVA
- Ultrasonic Level Transmitters – Networked & Non-Networked
- Magnetic Flowmeter - Networked & Non-Networked
- Pressure Transmitter - Networked & Non-Networked
- Temperature Transmitter - Networked & Non-Networked
- Electric Power Meter

Items with a score of less than 10 are discretionary, and while there are benefits to standardization, the justification is less obvious. The case for standardization of these items could be deferred for consideration on a case-by-case basis.

It should also be noted that the list in Table 17-3 is not exhaustive, and additional items could be identified as potential candidates for equipment standardization during the design phase. It is recommended that these be flagged for consideration and also evaluated on a case-by-case basis.

17.4 Implementation

It is proposed that the process to implement an equipment standard be dependent upon the value of the equipment. For small items with an individual value less than $5000 and in small quantities, it is proposed that a short report, approved by the Water and Waste Department would be prepared to document the equipment standard. However, for items of more significant value, it will be required to go through a formal process to standardize the identified equipment. It is expected that the standardized equipment would be effective for all future projects for a significant period of time (ten years). It is proposed that the process to formally standardize equipment of significant value would be as follows:

1. Prepare a technical specification for the product to be standardized.
2. Prepare an evaluation plan that includes a detailed point scoring system to evaluate the products proposed by various manufacturers.
3. Identify approximate quantities of the product required, and the required timeframe for the standardization.
4. Prepare an overall Bid Opportunity Package to allow vendors to put forth a proposal.
5. Issue the complete package for review by the City and make changes as per the comments received.

6. Issue the Bid Opportunity to Materials Management for public posting.
7. Receive and review the proposals from the vendors.
8. Request information that is missing or not clear in the proposals, to allow for a comprehensive and fair evaluation.
9. Evaluate each proposal utilizing the detailed point scoring system presented.
10. Award the project. In some cases, there would not be delivery of any product at this point, but rather the standardization would affect future projects.

The above plan will require approval from the City's Materials Management Division prior to implementation.

17.4.1 Duration of the Equipment Standardization

It is expected that there will be a significant cost to implementing the equipment standardization program, and it will not be beneficial to re-evaluate at frequent intervals. It is suggested that the equipment standardization be based upon a period of ten years. However, the standardization should extend only as long as it is in the City's interest to do so. The Bid Opportunity must be written in a manner to ensure that the City can cancel the standardization at any time, for any reason. The rationale for cancelling the standardization would include, but not be necessarily limited to:

- Poor equipment performance,
- Poor vendor support,
- Significant pricing changes, and
- Technological obsolescence.

17.4.2 Price Evaluation

It is expected that the primary issue regarding the evaluation will be associated with the price evaluation. A typical concern would be regarding the ability of the standardized vendor to provide price certainty over a ten year time span.

It is anticipated that the price evaluation would be based upon individual vendor proposals regarding price certainty. Some vendors will be in a position to provide some level of guarantee regarding prices, while other vendors will not be able to provide any certainty. One example of potential price certainty that certain vendors may be in a position to provide is a fixed discount off the company's published list price. Vendors who could provide price certainty would score higher in the price component of the overall evaluation.

18.0 CITY TECHNICAL STANDARDS

18.1 Introduction

It is required that the City prepare technical automation standards to ensure a consistent high-quality automation installation at the wastewater treatment facilities. Without standardization, it is typical that there would be significant variability in implementation details, which could lead to issues during implementation that would impede facility operations and maintenance. In addition, technical standardization can provide an improvement in quality control, as it can help assure that proven design and installation methods are consistently applied.

18.2 Recommended Standards

Recommended City standards documents are identified in Table 18-1.

Table 18-1 : Recommended City Standards Documents

Document	Recommended Scheduling Criteria	Details
Identification Standard	September 2012	See Section 18.3
Automation Design Guide	Coordinate with PLC Vendor Selection	See Section 18.4.1
Tagname Identification Standard	Immediately After PLC Vendor Selection	See Section 18.4.2
HMI Layout and Automation Plan	After HMI Vendor Selection	See Section 18.4.3
Historical Data Retention Standard	Prior to Software Programming / Configuration	See Section 18.4.4
Backup and Disaster Recovery Plan	Prior to Completion of Detailed Design	See Section 18.4.5

18.3 Identification Standard

It is recommended that an Identification Standard be prepared, which can be referenced for consistent and accurate identification for all process, mechanical, electrical, and automation equipment. There are multiple existing identification standards, and they have not been consistently applied. This document will provide clear guidance to department personnel, as well as external consultants, regarding appropriate equipment identification. The identification standard should be developed based upon existing systems specific to City installations, international standards, and general industry practice.

The scope of the identification standard should include:

.1 General Requirements

.1 Scope
.2 Approach to address existing facilities

.2 Process and Mechanical Equipment

.1 Provide identification standard for process and mechanical equipment.
.2 Provide identification standard for manual valves.

.3 Electrical

.1 Provide an identification standard for the following:

.1 Equipment and Panels
.2 Breakers
.3 Motor Starters
.4 Special Cases, such as equipment in parallel and series
.5 Wires and Cables
.6 Identification of circuit numbers on drawings, and for equipment, receptacles, lighting, etc.

.4 Automation

.1 Provide an identification standard for the following:

.1 Panels / Enclosures
.2 Wires
.3 Junction Boxes
.4 I/O

.1 DCS style systems
.2 PLC style systems
.3 Software and hardware control loops

.5 Signal/Variables identification

.2 Provide a loop numbering system with ranges for the various process, HVAC, and miscellaneous systems.

18.4 Automation Standards

18.4.1 Automation Design Guide

An Automation Design Guide would provide detailed guidance regarding specific implementation strategies to the automation designers of new installations and upgrades to the wastewater facilities. The scope for the automation design guide would include the following:

.1 Scope

.2 Definitions

.3 Codes and Standards

.4 Design Requirements

- .1 System Configuration
- .2 Redundancy / Backup
- .3 Manual Control.

.5 Identification

- .1 Reference the Identification Standard

.6 Environmental Requirements

- .1 Identify typical environmental requirements.
- .2 Identify typical enclosure types.

.7 Wiring and Cabling

- .1 Use of Conduits vs. Cables
- .2 Cable Types and Ratings
- .3 Conduit Materials and Sizes
- .4 Device and Pull Boxes
- .5 Junction Boxes
- .6 Cable Trays
- .7 Terminations
- .8 Shield termination and grounding.
- .9 Spacing between systems / Segregation
- .10 Signal noise prevention.

.8 HMI Systems

- .1 Identify typical information to present on HMI systems and control points.
- .2 Reference applicable standards and guides

.9 Local User Interface

- .1 Identify pilot light colours to be utilized.
- .2 Identify typical manual controls.

.10 Control Panels

.1 Identify design requirements for control panels, including:

.1 Spare space
.2 Wireways
.3 Cable entry
.4 Grounding
.5 Terminals
.6 Voltages and voltage separation.

.11 Motor Control

.1 Identify typical control and monitoring points for various scenarios.

.12 Valve Control

.1 Identify typical control and monitoring points for various scenarios.

.13 Field Instrumentation

.1 Identify typical practices and selection criteria.

.14 Process Design Considerations

.1 Flowmeters
.2 Control Valves
.3 Pumps and Motors

.15 Power Supply

.1 Identify power supply requirements including the requirement for Uninterruptible Power Supplies
.2 Branch circuit design
.3 Fusing

.16 Hazardous Locations

.1 Discuss specific requirements for hazardous locations.
.2 Identify preferred methods of protection.

.17 Safety Instrumented Systems

.1 Identify documentation requirements.
.2 Identify referenced standards for compliance.
.3 Identify general design principles.

.18 Grounding

.1 Identify minimum grounding requirements.
.2 Identify good practices to ensure reliable signal communications.
.3 Identify where additional grounding studies are required.

.19 Design Responsibility

.1 Identify typical responsibility for various project design deliverables.

.20 Sample Drawings

.1 Provide sample drawings for the following:

.1 PLC Power Schematic
.2 PLC I/O Module Schematic
.3 Instrument Location Plan
.4 Instrument Loop Diagram
.5 Instrument Segment Diagram
.6 Junction Box Interior and Exterior Layouts

.21 Sample Documents

.1 Instrument List
.2 Functional Requirements Specification

18.4.2 Tagname Identification Standard

A tagname identification standard would provide detailed guidance regarding the identification of software tagnames within the PLC and HMI systems. It would be based upon the Identification Standard discussed in Section 18.3 and would provide additional detail. The scope of the standard would be limited to the new PLC and HMI systems, and would not address the legacy systems at the wastewater facilities.

The standard would include the following:

.1 Scope

.2 Basic Rules

.1 Reference Relevant Data from the Identification Standard
.2 General Tag Format
.3 User-Defined Types (Classes)

.3 Tagname Details

.1 Clearly identify the tagging convention for specific attributes, functions, internal variables, setpoints, I/O, configuration points, etc.

.4 Identification of Control Loops and internal functional systems.

.5 Examples

The Tagname Identification Standard can be influenced by the Control System vendor, and thus it is recommended that this document be prepared after the vendor is selected.

18.4.3 HMI Layout and Animation Plan

An HMI Layout and Animation Plan standard would provide detailed guidance regarding the presentation of graphical and text data on the Human Machine Interface (HMI) stations. It would ensure that data is presented to operations personnel in a clear and consistent manner, to allow for efficient monitoring of the facility processes.

The standard would include the following:

.1 Scope

.2 Definitions

.3 Graphic Mimics / Displays

- .1 General Principles
  - .1 Identify general content and method of presentation. For example, clarify if the graphics are to be based upon 2D P&ID style representations, or 3D graphics.
  - .2 Screen layout, including locations for alarm banner and navigation buttons
  - .3 Space for Spare / Future Systems
- .2 Colour Scheme
  - .1 Background, faceplates, process lines, equipment, etc.
  - .2 Trending colours
  - .3 Alarm colours
  - .4 Equipment status colours
  - .5 Valve status colours
  - .6 Etc.
- .3 Typical Faceplate controls and information
- .4 Display of Text Values (i.e. flowmeter value)
- .5 Display of Equipment Status (i.e. Starter Not Ready)

.4 Alarming System

- .1 Alarm Presentation Philosophy
- .2 Alarm Priorities
- .3 Alarm Callout

.5 Equipment Settings

- .1 Identify where and how equipment settings are displayed and modified.

.6 Miscellaneous

- .1 Operator Help Functions
- .2 Links to Other Documentation
- .3 Security

18.4.4 Historical Data Retention Standard

A Historical Data Retention Standard would provide general guidance regarding the retention of data produced by the control system. The wastewater treatment control systems are capable of generating and storing huge volumes of historical data. However, it is poor design practice to historize and archive more data than necessary, as this can lead to unnecessary system hardware and maintenance costs and difficulties associated with the management of excess data. It should also be noted that costs can be significant when archival of historical data is considered.

It is recommended to create a document identifying data to store in the historian, and duration of archive retention. The scope of the data retention policy could potentially be integrated as part of an overall departmental data lifecycle management initiative.

It is proposed that the standard would include the following topics:

.1 Scope

.2 General Principles

  .1 Availability of Data
  .2 Archival principles

.3 Requirements for Typical Applications

  .1 Retention Periods
  .2 Logging Interval Requirements
  .3 Archival Requirements
  .4 Backup and Disaster Recovery Requirements

.4 Examples

It should be noted that the standard would provide general guidance that will require interpretation to determine the historical logging and retention periods for specific points. For example, the standard could define that equipment operational data that have potential use for maintenance evaluation, but limited long term value should be retained for a period of possibly one year. Retention periods for a specific data point, such as a raw sewage pump ammeter reading, would require interpretation of the standard and potential consultation concerning departmental requirements, to determine the specific retention periods.

18.4.5 Backup and Disaster Recovery Plan

All wastewater control systems require a rigorous and effective backup and data recovery plan and set of procedures. A few potential events that an effective backup and disaster recovery plan would address include:

- Hardware failure,
- Fire,
- Vandalism and theft,
- Software corruption, and
- Accidental errors introduced into an application.

It is recommended that a detailed backup and disaster recovery plan be prepared for the wastewater treatment automation systems. While this document is not technically a standard but rather a specific implementation plan, it is identified due to its importance in ensuring the availability of the control system. Key components to be included in the disaster recovery plan are:

- Identify critical software and hardware components, as well as critical data,
- Regular backups of critical software and data,
- Regular off-site backups to a remote location,
- Hardware spare availability,
- Drawings of the network configuration,
- Identification of acceptable outage and recovery times,
- Documentation of changes to the system, which can be invaluable during disaster recovery efforts,
- Periodic testing of the disaster recovery plan to ensure it meets needs,
- Use of virtual machines to expedite the restoration of services.

19.0 PROJECT DOCUMENTATION

19.1 General Requirements

General requirements for project documentation include the following:

- All design drawings are to be produced to follow the City's drawing standards and utilize the City's drawing numbering system.
    - Consultant / Contractor document identification numbers may be included on the drawings, provided that the text is no larger than 2.5mm high and is not referenced anywhere else on the drawing.
- Shop Drawings are to be logged into a database tracking system in accordance with a format to be specified by the City, and filed both electronically and via paper copies. Note that development of a system for shop drawing storage and retrieval will need to be developed by the City.
- Reports and Studies are to be provided to the City in electronic (PDF) format.
- Lists and tables are generally expected to be prepared and maintained during construction in Microsoft Excel format. After construction is complete, it is expected that the lists be transferred to the City in Excel format. At the City's option, the lists could be imported into a database for use by the facility maintenance personnel.

19.2 Documentation Lifecycle Approach

It is also recommended that documents for the wastewater facilities utilize a lifecycle approach, rather than a construction-based approach. It has historically been quite common that the detailed design documents for the wastewater facilities have been produced with the primary purpose of indicating the required construction, and not for maintenance purposes. As an example, past practice has utilized a construction-based approach where only a small detail of a control system architecture segment, applicable to the new work, has been shown on a plan drawing with many other details. However, this situation is not suitable for maintenance, as personnel would need to find the original architecture drawing, and compare it with the added detail, to determine the overall system architecture. With multiple projects and revisions, the overall documentation can become confused and incomplete.

It is recommended that where existing documents exist, they be updated rather than new drawings created. In the event that the original drawing is not longer suitable for the new work, it should be marked as superseded and a new drawing created. Efforts should be made to provide the City with an overall documentation system for the facility, and not limited to documentation for project specifics only.

It is recommended that the City develop a Document Development and Management standard. This document must subsequently be provided to all team members and be enforced to accomplish the proposed lifecycle approach.

19.3 Minimum Documentation Requirements

The minimum documentation requirements for a comprehensive project are identified in Table 19-1. It should be noted that some documents would not necessarily be applicable to some smaller project, and thus the specific project requirements must be detailed on a project-by-project basis.

Table 19-1 : Minimum Documentation Requirements

Document	Native Format	Preliminary Design	Functional Design	Detailed Design – 66%	Detailed Design – 100%	As-Built	Notes
P&IDs	AutoCAD A1	P	Y	Y	Y	Y	See 19.3.1
System Architecture / Block Diagrams	AutoCAD A1	-	Y	Y	Y	Y	See 19.3.2
Motor Starter Schematics	AutoCAD A1	-	-	T	Y	Y	Include all automation and I/O
Motor Starter Connection Diagrams	AutoCAD A1	-	-	T	Y	Y	may be on same drawings as motor starter schematics
Instrument List	Excel	-	-	-	Y	Y	See 19.3.3
Instrument Location Plans	AutoCAD A1	-	-	Y	Y	Y	See 19.3.4
Instrument Loop Diagrams	AutoCAD 11x17	-	-	T	Y	Y	See 19.3.5
Instrument Segment Diagram	AutoCAD A1	-	-	T	Y	Y	See 19.3.6
Instrument Installation Details	AutoCAD A1	-	-	-	Y	Y	See 19.3.7
Automation Power Distribution Schematics	AutoCAD A1	-	-	T	Y	Y	
PLC/DCS I/O Module Wiring Diagrams	AutoCAD A1	-	-	T	Y	Y	
Control Panel Interior and Exterior Layouts	AutoCAD A1	-	-	T	Y	Y	
Grounding Riser Diagrams and Details	AutoCAD A1	-	-	T	Y	Y	

Document	Native Format	Preliminary Design	Functional Design	Detailed Design – 66%	Detailed Design – 100%	As-Built	Notes
Junction Box Interior and Exterior Layouts	AutoCAD A1	-	-	T	Y	Y	
Conduit Riser Diagrams	AutoCAD A1	-	-	-	Y	Y	
Cable Tray Layouts and Details	AutoCAD A1	-	-	Y	Y	Y	
Equipment Plan Drawings	AutoCAD A1	-	-	Y	Y	Y	
Control Room Layout Drawings	AutoCAD A1	-	-	Y	Y	Y	
Fieldbus Network Diagrams	AutoCAD A1	-	-	Y	Y	Y	
Cable Schedule	Excel	-	-	-	Y	Y	
I/O List	Excel	-	-	-	Y	Y	
PLC/DCS Module List	Excel	-	-	-	Y	Y	
Network Overview Diagrams	AutoCAD A1	-	-	Y	Y	Y	See 19.3.8
Network Details	AutoCAD A1	-	-		Y	Y	See 19.3.9
Network Cable Routing Diagrams	AutoCAD A1	-	-	-	Y	Y	
Network Cabinet Layouts	AutoCAD A1	-	-	-	Y	Y	
Instrument Datasheets	Excel	-	-	T	Y	Y	See 19.3.12
Functional Requirements Specification	Word	-	-	-	Y	Y	See 19.3.8
Safety Instrumented Systems Documentation	various	-	P	Y	Y	Y	See 19.3.13
Instrument Commissioning Forms	Word Form	-	-	-	Y	Y	
Construction Plan	Word	-	-	(1)	(1)	(1)	
Installation, Calibration, and Commissioning Checklists	Word	-	-	-	-	Y	
All Control System Programmable Logic Files and Configuration	Native and PDF	-	-	-	-	Y	

Document	Native Format	Preliminary Design	Functional Design	Detailed Design – 66%	Detailed Design – 100%	As-Built	Notes
HMI Training Manual	Word	-	-	-	-	Y	General features and operation
Operations Manual	Word	-	-	-	-	Y	See 19.3.14
Other Maintenance Documentation	PDF	-	-	-	-	Y	See 19.3.15
Legend P = Preliminary; T = Typical;							

Notes:

1. A Construction Plan, providing a detailed method of implementation, is required when the construction will have a significant impact on the operation of existing systems.

19.3.1 Process and Instrumentation Diagrams

Process and Instrumentation Diagrams (P&IDs) show the details of the process equipment and piping together with the instrumentation utilized to control the process. Standard conventions for P&ID documentation are based upon the ISA 5.1 standard, and specific City standardization is currently being developed as part of the Identification Standard development, discussed in Section 18.3.

The City has expressed a desired to utilize a “smart” P&ID that automatically links to a database and related documents. An example of such a tool is SmartPlant P&ID, produced by Intergraph. An a large project a software package that implements these advanced features can provide significant benefit relating to coordination and automatic cross referencing of information. However, the value of the software is significantly diminished if it is not standardized across the City and the entire design team. Thus, it is recommended that the City take the lead in selection of an appropriate software tool.

19.3.2 System Architecture / Block Diagrams

System Architecture / Block Diagrams should include all significant control system components and network connections in a block diagram format. The information should be presented in a clear concise manner, such that the number of drawings that must be cross-referenced to obtain a high level view of the control system is minimized.

19.3.3 Instrument List

The instrument list should, at minimum, contain the following information:

- Instrument tag identifier
- Instrument Description
- Reference P&ID Drawing
- Reference Loop Drawing
- Reference Plan Drawing
- Reference Installation Detail
- Instrument Datasheet Document Number
- Notes – Can include identification if instrument is new or existing.
- Optional items include:
    - Signal type (4-20, Fieldbus, discrete, etc).
    - Equipment/Line number (typically for in-line devices)
    - Supplied By (I&C Contractor, Package Vendor, City, etc)

19.3.4 Instrument Location Plans

The instrument location plans are plot plans of the building, with outlines of major equipment and vessels shown. In some cases, the outline of major piping will be shown, where this relates to instrument locations. The plan drawing should include the building grid reference. All instruments will be shown on the plan, with instrument tag bubbles.

19.3.5 Instrument Loop Diagrams

Instrument Loop Diagrams act as both a wiring diagram and schematic for discrete and analog instruments associated with a specific function. All devices on the loop diagram are referenced with instrument loop numbers, and all terminals, junction boxes, wires, wire tags, shields, ground connections, and pneumatic tubes are shown. All energy sources such as electric and pneumatic supply should also be clearly shown. All valves should have their fail-position shown. In addition, the interface with the PLC/DCS should be clearly shown along with the applicable I/O address.

See ISA 5.4 for additional guidelines regarding preparation of Instrument Loop Diagrams.

19.3.6 Instrument Segment Diagrams

Instrument Segment Diagrams act as a replacement to loop diagrams for fieldbus based instrumentation. Multiple instruments may be shown on an Instrument Segment Diagram, along with the Fieldbus spurs, terminators, and connection interfaces. In addition, any power supplies for the Fieldbus and individual interface are shown. The content on each Instrument Segment Diagram will be related to the logical connections of the fieldbus segment.

19.3.7 Instrument Installation Details

Instrument installation details should be prepared for most cases. Typical instrument details may be utilized where the installation is similar, but specific installation details should be prepared where there are specific installation constraints or detailed measurements applicable to the installation. For example, a specific installation detail, showing key elevations, should be provided for a wet well level transmitter.

19.3.8 Network Overview Diagrams

Network Overview diagrams provide a graphical, block diagram view of the network. They typically show all network equipment and cabling, and major equipment such as servers, but may not necessarily show every node connected to the network. References to Network Details drawings would be provided to allow for quick reference of specific network information. A specific set of network drawings should be provided for each network. For example, for the process network, it is expected that a Network Overview drawing would be provided for each network facility, each process area, and for the Supervisory network in the server room(s) of the facility. In addition, separate drawings would be provided for the administration network.

19.3.9 Network Details

Network Details drawings are commonly not produced as historically networks were not as integrated as current automation system environments. However, without appropriate documentation, it is not clear how the network is to be constructed, or supported. Networks for control systems have numerous details that must be configured appropriately, and documented, for appropriate control system operation. Details to be included on the Network Details drawings include: equipment identifiers, manufacturer, model numbers, IP addresses, port numbers, media type, connection rate, RSTP information such as route costs, VLAN configuration, and other details as required to fully document the network.

Note: It is recommended to review as part of the security plan if certain details should be hidden on public tender documents to improve facility security.

19.3.10 Process Control Overview

The Process Control Overview is a written description of the manual and automatic process control. It is written in sentence form and provides an overview of the operation of the system. It should be written with two target audiences: process engineers and senior operations personnel. The detail in the process control overview should be limited to critical information to understand the process control. Details such as I/O and comprehensive lists of alarms should be placed in the Functional Requirements Specification.

19.3.11 Functional Requirements Specification

The Functional Requirements Specification will provide detailed information as to the functionality of the control system. Reference *ANSI/ISA-5.06.01-2007 - Functional Requirements Documentation for Control Software Applications* for specific requirements.

Specific items to be included in the functional requirements specification for each piece of equipment are:

- I/O Details including ranges for analogs
- HMI – PLC Interface tag details, including setpoints
- Alarms
- Interlocks
- Control Logic Description

In addition, the following is also required:

- Trending requirements
- Data points required for business system integration
- Historical data logging requirements
- Reporting Requirements

19.3.12 Instrument Datasheets

An instrument datasheet defines the characteristics of an instrument in sufficient detail to allow an instrumentation vendor to supply the required instrument. The requirement for instrument datasheets is dependent upon the instrument in question and the details of the specific project. Instrument data sheets are typically required for the following:

- Analysis Device
- Flowmeter
- Level Switch
- Level Transmitter
- Pressure Switch
- Pressure Transmitter
- Temperature Transmitter
- Control valves

Notes:

1. *For small projects, it may be sufficient to address the required instrument features in the technical specifications, provided the variety of instrument types and ratings is limited.*
2. *It is acceptable to utilize typical instrument datasheets to describe multiple instruments, provided that the instruments and service conditions are identical.*
3. *The above list is not exhaustive.*

The instrument datasheets should follow the general format as presented in ISA 20, however modifications of the datasheets to suit the specifics of the application are accepted.

19.3.13 Safety Instrumented Systems Documentation

Safety Instrumented Systems should be fully documented as per ISA 84.00.01-2004.

19.3.14 Operations Manual

The Operations Manual will detail all aspects required to train operators on requirements for monitoring and control of the wastewater treatment facilities. While the Operations Manual will require input from disciplines other than Automation, it is expected that the Automation engineers will have a major role in preparing the Operations Manual. The Operations Manual will include the following for each system / process area:

- Process Overview including plan and schematic drawings
- A section on each process system / subsystem which includes:
  - Introduction
    - Description of the purpose of the area / system
    - Description of the process and subsystems
    - History of the system. (This can be useful in determining where to find information on the systems).
  - System Description
    - A detailed description of the purpose of the system / subsystem and how it operates.
    - Identify the location and function of each piece of equipment.
    - Plan, schematic, and isometric drawings, as required to clearly represent the location and operation of the process along with each unit of associated equipment. Process flow diagrams with major equipment ratings are mandatory.
  - Automation Description
    - Provide overview plan drawings indicating the location of automation systems, and significant control locations in the facility.
    - Describe the local operator controls in the field.
    - Describe the area operator controls. Drawings of significant control panels will be required.
    - Provide P&ID drawings.
    - Describe the HMI operator controls. Include a screenshot of all major HMI screens.

    - Describe the automatic control of the process. This could potentially be based on the Process Control Narrative.
    - Describe Operator control from the HMI, including adjustment of setpoints and settings.
    - Indicate the typical default value, or range of values, for all setpoints.
    - Alarms – Provide a complete list of alarms, along with typical Operator response.
  - Operational Procedures
    - Describe routine operating procedures and checks.
    - Describe normal and maintenance operational procedures, including taking the equipment out of service.
    - Describe procedures and plans to address various contingency scenarios. For example, describe the procedure if two raw sewage pumps are out of service during wet weather flow.

The Operations Manual should be reasonably comprehensive to provide guidance to operators regarding most typical operating scenarios. It is recommended that the document be prepared in a manner to allow for paper printing, but also efficient electronic access. The documents must be supplied to the City in an editable format, to allow for continuous updates to the manual, as changes are made to the process. It is also recommended that the manual is accessible from the HMI, with direct linking to applicable sections.

19.3.15 Other Maintenance Documentation

A comprehensive set of maintenance documentation should be supplied to allow for effective maintenance of the facilities. In addition to the documentation already presented, this would include, but is not necessarily limited to:

- Shop Drawings,
- Product Submittal Datasheets,
- Vendor Operations and Maintenance Manuals,
- Configuration Passwords,
- Equipment Configuration Files and Settings, and
- Instrument Calibration Sheets

19.4 Computerized Work Management System

The City of Winnipeg utilizes a Computerized Work Management System (CWMS) to manage maintenance of the wastewater treatment facilities. An up-to-date asset database is critical to the effective use of the CWMS. The CWMS asset database must be updated prior to the turnover of the equipment to the City.

Typical current data required for entry into the CWMS currently includes:

> ASSET_NO, PLANT, ASSET_RECORD_TYPE, ASSET_TYPE, ASSET_DESC, ASSET_STATUS, DEPARTMENT, AREA, CRITICALITY, BREAKER_NO, BUILDING, LOCATION, ROOM, MANUFACTURER, MAKE, MODEL_NO, SERIAL_NO, CONTROL_PANEL, TYPE, SIZE, CAPACITY, PUMP_BEARING, HEAD_PRESSURE, FRAME, HP, VOLTS, AMPS, FLA, SF, RPM, PHASE, MOTOR_BEARING, INSULATION CLASS, OUTPUT, RANGE, DCS, LOOP, PID, SHOP, OTHER

Note that not all of the above attributes are applicable to each asset.

In addition, it is recommended that the following field be added for use as part of the proposed upgrades:

- Old Equipment Identifier (For use when equipment is re-identified)

It is proposed that the data for CWMS entry be collected and formatted by the design engineer responsible for the project. The Contractor could potentially assist the design engineer in gathering data, but it is believed that the Design Engineer is in the best position to be able to accurately prepare the data.

19.4.1 Scope of Equipment to be Entered

The scope of equipment to be entered into the CWMS is fairly comprehensive. All process equipment including fans, pumps, conveyors, blowers, etc. shall be entered as assets. In addition, all automation components such as instruments, control valves, control panels, etc shall be entered. The general rule of thumb is that if the device or equipment will require maintenance, it should be entered into the system. Items that will not require entry include wires, junction boxes, tubing, cable tray, etc.

The City of Winnipeg’s CWMS manages and tracks equipment in terms of assets and components. An asset can be many things ranging from a piece of equipment to a room within a building. Each asset has a unique identifier, description, and other information.

The CWMS Asset module links to work orders and maintenance history lists. The Asset module allows City personnel to track asset reliability, runtime, downtime, operational data, attach bills of materials, analyze performance, and numerous other items. It should also be noted that assets can be configured in a parent-child relationship, creating a hierarchy of assets.

The CWMS system also can track components, which are defined in the CWMS system as stock items such as pumps, compressors, shafts, etc that can be installed and removed, and are typically major part within the asset. Work orders and costs can be assigned to components, to allow the system to provide reports relating to the specific asset components, and not only the asset in general.

The assignment of specific either assets or components is a decision that must be made by the City, in a manner consistent with the entire asset management system. It is understood that the City does not currently utilize the component module of the CWMS system, however there is potential for its use in the future. Some guidelines for scope of equipment and categorization are presented below in Table 19-2, however it should be noted that this requires confirmation with the overall plan for the City's CWMS. It should also be noted that the table is not comprehensive, and specific evaluation of items to be included in the CWMS system must be performed on a project by project basis.

Table 19-2 : CWMS Automation Entry Requirements - Preliminary

Item	Entered in CWMS	Type	Notes
PLCs	Yes	Asset	Per logical PLC
Individual PLC Modules	Potential	Component	
Local Touchscreen HMI	Yes	Asset	
HMI Client	Yes	Asset	Per PC
HMI Server	Yes	Asset	Per Server
Network Switch - Managed	Yes	Asset	
Network Switch - Unmanaged	Not Typically	-	
Instrument	Yes	Asset	See Note 1
Control Valve	Yes	Asset	
Gas Detection Sensor	Yes	Asset	Includes transmitter
Control Panel	Yes	Asset	See Note 2
Protocol Gateway	Yes	Asset	
UPS	Yes	Asset	See Note 3
Junction Box	No	-	-
Cable	No	-	-

Notes:

1. *Instruments that are components within an overall assembly, and not individually identified within the P&IDs and control system do not require individual asset definition. For example, a specific sensor within a thermal oxidizer package does not require specific entry as a dedicated asset.*

2. *While a control panel could potentially contain a PLC, it is recommended that they be considered separate assets. The control panel asset would include all minor components contained within.*

2. *It is recommended that both large UPS units and small UPS units contained within control panels be identified as assets due to maintenance requirements.*

20.0 RISK REVIEW

20.1 Overview

The wastewater treatment automation system is a critical system required to monitor and control the wastewater treatment plant process. There are various potential risks associated with the overall automation system that could significantly affect the treatment process. The purpose of this section is to identify the project risks, evaluate and quantify the risks, and provide a high level risk mitigation plan, or at minimum identify the project responsible for the risk mitigation.

The risks in this section are assigned three priority levels, indicating a subjective indication of the level of risk associated with the identified item. The Risk Priority Levels are identified in Table 20-1 below.

1	The identified risk is critical, and has a relatively high probability of affecting the operation of the facilities.
2	The identified risk has significant consequences, and has a reasonable possibility of affecting the operation of the facilities.
3	The identified risk is deemed to either have relatively low potential consequences, or has a relatively low probability of occurring.

Table 20-1 : Risk Priority Levels

20.2 Failure of the Existing DCS HMI

Risk

The existing ABB PCV HMI could potentially fail, which would significantly impact the wastewater treatment plant operations.

1	Failure of the HMI would cause disruption to the operation of the facility.

Analysis

The City initiated a project to upgrade the existing HMI software and hardware. The plan was to upgrade the existing PCV HMI from version 5.4 to version 5.5b, and renew the existing HMI hardware. This approach was not implemented and it is understood that the City now intends to upgrade the HMI systems at the facilities to the ABB S+ (PGP) platform.

Mitigation

It is recommended that replacement of the DCS HMI be performed as soon as possible. At minimum, the HMI at the NEWPCC should be replaced, which would allow the existing NEWPCC hardware to be utilized as spares at the SEWPCC and WEWPCC facilities. This approach would offer a relatively expeditious upgrade that would effectively mitigate the potential risk at the NEWPCC, and greatly reduce failure impacts at the SEWPCC and WEWPCC.

20.3 Failure of the Existing DCS Infi90 Hardware

Risk

The existing ABB Infi90 could potentially fail, which would significantly impact the wastewater treatment plant operations.

2	The existing ABB Infi90 hardware has proven to be reliable; however certain critical components are significantly aged and could potentially fail if not replaced in the short term.

Analysis

The existing DCS hardware has proven to be very reliable, with limited component failures. However, as discussed in Section 11.1, there are certain components which are deemed to be at end of life.

Mitigation

It is recommend that:

- The NVRAM at WEWPCC and SEWPCC facilities be upgraded (Under the HMI Upgrade project)
- Recommend that a project be initiated to review risks at the WEWPCC facility and upgrade for ~10 year life span.
- Once the SEWPCC facility upgrade work plan becomes known, review the replacement timeline of the DCS, review the lifespan of critical DCS components, and replace or upgrade as required. It is recommended that this review take place in early 2013.
- Once the NEWPCC Upgrades work plan becomes known, review the replacement timeline of the DCS, review the lifespan of critical DCS components, and replace or upgrades as required. As the DCS was upgraded in 2005, it is expected that any replacement or upgrades required to extend the life of the DCS will be minimal. It is recommended that this review takes place in early 2014, to allow for planning of required upgrades prior to 2015.

20.4 Review of the Design Documents

Risk

Repeatable successful project delivery is dependent upon effective review of the design documents and deliverables produced by the design engineer and systems integrator. Without appropriate quality control procedures and review, the risk of errors and omissions is increased.

2	The use of effective quality control procedures is required to reduce the probability of errors and omissions in the design and implementation process. The City's internal resources for effective review of the automation (and electrical) disciplines are believed to be limited.

Analysis

Effective project delivery is dependent upon appropriate quality control procedures. One aspect of this is effective owner review of the design documents and deliverables. However, the City's internal resources for effective review of the automation (and electrical) disciplines are believed to be limited. Thus, use of external resources to aid in the review and monitoring of the project would limit the risk of errors or omissions in the design and construction documents. The detailed scope of work to be performed by the external resource would require further review and discussion.

Mitigation

It is recommended that:

- The City hire a qualified owner's electrical and automation engineer to represent the City and review the technical documents prepared by the design engineer and systems integrator.

20.5 Cost Overruns

Risk

As is common in any project, there is a significant risk for cost overruns to occur, which can have an impact on either the ultimate project deliverables or the total financial costs of the project.

2	Appropriate and effective design and project management is required to ensure that projects remain within budget.

Analysis

The automation discipline involves very detailed engineering, construction, and commissioning. Given the level of detail required, there are significant opportunities for design errors or omissions to have a cost impact on the project. Lack of appropriate automation design detail at the preliminary, functional, and detailed design stages provides significant probable opportunity for scope changes through the course of construction, commissioning, and even required modifications after the primary project is complete.

Mitigation

It is recommended that:

- The various design initiatives be required to provide detailed automation plans early in the process, rather than deferring detailed design to the construction stage.
- Review of the proposed design is performed by qualified personnel on behalf of the City, such as through the use of an Owner's Engineer.

20.6 Software Implementation Errors

Risk

It is not uncommon for control system applications to have significant errors that could potentially impact operations.

2	Software errors are common and must be addressed through detailed design of the functional requirements and diligent quality control procedures.

Analysis

Control system software errors are introduced through many sources, however most are introduced as a result of a few primary causes. The first is an insufficiently defined and detailed functional requirements specification. If the desired functionality of the system is not designed and fully specified, it is left up to the programmer, who may not have sufficient expertise regarding the entire process, to make judgements regarding the required functionality. The programmer should not be relied upon to make engineering decisions. The functionality of the system must be sufficiently described that any two independent programmers will produce a software configuration with identical functionality.

The second potential issue is lack qualified programming or commissioning personnel to diligently perform the required work. The third common issue is lack of a full and complete Factory Acceptance Test, which is critical to good software quality control.

Mitigation

It is recommended that:

- A functional requirements specification be prepared that is sufficiently detailed and clear such that it forms the basis for the programming and acceptance checklists. The functionality described must be unambiguous.
- Ensure that the Systems Integrator is qualified to perform the work, as discussed in Section 20.11.
- As part of the Factory Acceptance Test (FAT) process, the Systems Integrator is required to fully demonstrate and document every aspect of the control system to a qualified group of witnesses, which should include representatives from the City operations group, design engineer, and potentially the owner's engineer.
- The commissioning process must be led by experienced personnel familiar with system commissioning and capable of providing the required organization and leadership for the project.

20.7 Unplanned Effect on the Existing Process

Risk

During the construction and transition from the existing control system to the new control system, there is a significant risk that an aspect of the construction work will have an unplanned effect on the existing process.

2	Unless specific review and planning takes place to ensure that the existing process remains operational during the transition period, unplanned events can be expected that will affect operations.

Analysis

Project delivery in new construction typically allows for distinct phases where construction occurs then moves into the commissioning phase, and finally the transfer stage. However, when significant modifications are made to existing processes, a significant amount of planning is required to ensure that the changes during construction will not affect the existing process. For example, if a critical control system interlock with a sensor is not appropriately managed, disconnection of the associated sensor could disrupt the process. Identification of interlocks, critical paths, manual control during switchover and other detailed transition planning is required to ensure a successful transition with minimal interruption.

Mitigation

It is recommended that:

- A specific Construction Work Plan document be prepared to address sequencing of work to avoid interruptions to the process.
- Detailed review processes be implemented to investigate and address the transition of existing automation system to new automation systems.

20.8 Signal Noise and Grounding Issues

Risk

There is a potential for control system communication and infrastructure signals to be corrupted or interrupted by electrical noise and grounding issues.

2	Control system noise and grounding issues can be very difficult and time-consuming to detect, and have a potential significant effect on facility operation.

Analysis

Signal noise and grounding issues can cause significant commissioning and operational problems, and are typically very difficult to diagnose. The best practice to address these issues is to ensure that good design practices are followed during the design and construction.

Mitigation

It is recommended that:

- An Automation Design Guide document be prepared, as discussed in Section 18.4.1, to address standard good practices and adopted standards, which would limit the risk of control system noise and grounding Issues. The proposed design should adopt the principles in the design guide.
- Review of the proposed design is performed by qualified personnel on behalf of the City, such as through the use of an Owner's Engineer.

20.9 Compatibility Issues

Risk

There is a potential for compatibility issues between automation equipment, and if not discovered and addressed early, can affect the commissioning and successful delivery of the project.

3	Compatibility issues, if discovered early, can typically be resolved, possibly by equipment substitution, but if discovered late, can have an impact on the project delivery schedule.

Analysis

Compatibility issues are most likely associated with networked equipment. Variations in protocol, or the level of protocol support, can have an impact on successful communication between the devices. For example, just because the devices both speak PROFIBUS, does not guarantee that they will communicate successfully, as there are different variants, versions, and level of support.

Mitigation

It is recommended that:

- The fieldbus and network protocols be selected based upon the capabilities of the control system vendor.
- The selection of critical networked equipment be standardized, as discussed in Section 17.0.

20.11 Competency of Design Engineer and System Integrator

Risk

The use of a design engineer not skilled in control system design will put the success of the upgrade projects at risk. In addition, if the control system integrator, who is responsible for the implementation and programming of the automation system does not have the required experience or resources, there is a significant risk of delays, issues during commissioning, and operational problems after the upgrades are complete.

3	The potential use of unqualified personnel to implement the automation upgrades would have a significant impact on the success of the projects.

Analysis

The qualification of design personnel and the system integrator is very difficult to measure. Experience also has shown that while certain companies have a higher reputation for automation design and integration, the actual personnel assigned to the project is typically a primary factor in the overall project success.

However, ideal selection of either design engineering personnel or system integrators is difficult to achieve as part of a competitive procurement process where price is utilized as the governing factor. In addition, the means for selection of the design engineer and system integrator are dependent upon the procurement model adopted. Within the expected competitive proposal process, it is believed that the only effective tool at the City's disposal is via bid or proposal evaluation.

Mitigation

It is recommended that:

- As part of the competitive proposal process for design or design-build procurement, ensure that sufficient effort and scoring weight is placed upon effective evaluation of the expertise and capability of the automation design engineering group.
- Initiate a process to pre-qualify system integrators, who will be permitted to perform the work. The format of the actual contract with the systems integrator will be dependent upon the project procurement model selected.

20.12 Automation Maintenance Organization

Risk

The City has noted that the organization structure regarding automation maintenance is not ideal.

3	A less than ideal organizational structure presents additional opportunities for missed work "falling through the cracks" or less in efficiency due to additional coordination requirements.

Analysis

Currently, the responsibility for maintenance of the automation systems is dispersed across at least two groups within the City. It is understood that typically the E&I group has been responsible for the DCS hardware modules, PLCs and PLC programming, while the PCG group has been responsible for the DCS software, networking, and a number of other systems.

While the groups responsible for automation maintenance have worked together, the coordination has not always been ideal, and it is recommended that the City review the organizational structure. Ideally, there would be a single group responsible for all the automation maintenance, with internal specialists to service the various roles.

In addition, it is also recommended that the role of the IT division, as they relate to automation, be formally documented as discussed in Section 14.6.

Mitigation

It is recommended that:

- The City review the organizational structure of the groups responsible for the maintenance of the wastewater automation systems.
- Formally document the automation maintenance organizational structure along with the relationship and role of the IT division.

21.0 IMPLEMENTATION PLAN

21.1 Commissioning

Commissioning of automation systems is a critical component to the successful installation and operation of a wastewater treatment facility. It is recommended that early in the project, a commissioning plan should be developed. The commissioning plan should include:

- Objectives,
- Team members, roles and responsibilities,
- Procedures,
- Operational Implications,
- Functional Testing Requirements,
- Links to Training Requirements, and
- Documentation and deliverables.

It is recommended that the commissioning plan be written from the overall process perspective, with specific sections as applicable to the automation discipline. Given that the process is typically viewed through the automation system, the automation team members typically play a critical role in the commissioning process, and should be included in all commissioning discussions.

21.1.1 CSA Z320

A recent standard CSA Z320-2011, entitled *Building Commissioning*, has been created and it was briefly reviewed to determine if it is applicable for utilization as a basis for the wastewater treatment facility commissioning. The scope of the standard is stated as follows:

> *This Standard provides guidelines for the commissioning of buildings and all related building systems. It applies to new construction and to renovations of existing facilities. It does not apply to operational commissioning of equipment and systems installed by the owner or others.*

The standard contains sections on many building systems, including a section addressing building automation and control systems. The section on building automation relates primarily to building systems such as HVAC and lighting and is quite brief in its specific requirements. Thus, it is believed that the standard is of limited value for identifying detailed commissioning requirements for industrial automation systems.

However, CSA Z320 does provide a significant amount of general guidance regarding commissioning, the commissioning plan, and specific roles of team members. It is recommended that it is utilized as a reference document when preparing the commissioning plan for the wastewater treatment plant upgrades.

21.2 Basis of Schedule

The proposed schedule for the implementation of the recommendations in this report is based upon the current estimated schedule for the SEWPCC Facility Upgrades, which is summarized in Table 21-1 below. As the schedule becomes more defined, it is mandatory that this schedule be updated, along with the implementation dates of all of the automation system recommendation.

Table 21-1 : Assumed SEWPCC Facility Upgrade Schedule

Phase	Duration	Est. Start	Est. Completion
Preliminary Design	6 months	2013 Q1	2013 Q3
Detailed Design	12 months	2013 Q3	2014 Q3
Tender & Award	5 months	2014 Q4	2015 Q1
Construction	36 months	2015 Q2	2018 Q2
Control System Commissioning	24 months	2016 Q2	2018 Q2

21.3 Implementation Responsibility

This document provides an overall plan for the automation system upgrades at the City of Winnipeg wastewater treatment facilities. Most of the work in this document will be the direct responsibility of the primary design team responsible for the wastewater treatment plant upgrades. However, there are some specific recommendations within this document that may be performed as part of other associated assignments, and these are identified in Table 21-2.

Table 21-2 : Work Responsibility

ID	Work	Ref Section	Recommended Responsibility	Proposed Completion Date
-	All recommended work other than that identified below.	-	Primary Design Team	
WR1	Selection of fieldbus networks	7.0	Joint decision with: Design Team City of Winnipeg Owner's Engineer (TBD)	2013 Q3
WR2	Automation System Vendor Selection	10.15 17.0	Separate Project See 21.4.3	2013 Q3
WR3	Upgrade of the Existing DCS HMI System	11.1.3 20.2	City See 21.4.1	ASAP
WR4	Upgrade of the Existing SEWPCC DCS Hardware	11.1 20.3	Separate Project See 21.4.5	2013 Q3
WR5	Upgrade of the Existing WEWPCC DCS Hardware	11.1 20.3	Separate Project See 21.4.6	2013 Q3
WR6	Upgrade of the Existing NEWPCC DCS Hardware	11.1 20.3	Separate Project See 21.4.8	2014 Q4
WR7	Setup of an Alarm Management Program	12.7	City	2016 Q2
WR8	Central Monitoring	12.10	Separate Project See 21.4.7	2016 Q1
WR9	Provide Mobile Hardware for Operator Remote View Access	12.11	City	2018 Q2
WR10	Collections System Integration	12.12	Separate Project See 21.4.12	2017 Q3
WR11	CWMS Integration	12.13.2	Separate Project See 21.4.10	2016 Q4
WR12	LIMS Integration	12.13.3	Separate Project See 21.4.11	2017 Q4
WR13	Process Control Management System Integration	12.13.4	TBD	TBD

ID	Work	Ref Section	Recommended Responsibility	Proposed Completion Date
WR14	Provision of the Central Historian Server	13.4	With NEWPCC Central Control and Server Room Upgrades See 21.4.7	2016 Q1
WR15	Provision of the Web Server	13.4		2016 Q1
WR16	Implementing Data Backup Systems	13.5	City	2016 Q3
WR17	Design of Admin Network	14.0	Design Team with City IT	2014 Q2
WR18	Provision of WAN Connection between Wastewater Facilities	14.2	City IT	2016 Q1
WR19	Setup of NEWPCC DMZ Zone	14.3	With NEWPCC Central Control and Server Room Upgrades See 21.4.7	2016 Q1
WR20	Supply and Configuration of Admin Network Switches	14.4	City IT	In stages: 2016 Q3 – 2018 Q2
WR21	Provision of VPN Connection For Remote Access to City Corporate Network	15.0	City IT	2016 Q1
WR22	Provision of VPN Connection to Remote Development Server, including Two Factor Authentication	12.2 15.0	TBD	2016 Q1
WR23	Design and Installation of Perimeter Security	15.3	TBD	2017 Q1
WR24	Implementation of a Change Management System	15.3	City to Develop Used by Systems Integrators	2013 Q1
WR25	Training – Maintenance Personnel	16.1.2	TBD	2015 Q4

ID	Work	Ref Section	Recommended Responsibility	Proposed Completion Date
WR26	Testing and Simulation System	16.2	TBD (See Note 1)	2016 Q1
WR27	Standardization of Critical Electrical And Automation System Components	17.0	Separate Project See 21.4.3	2014 Q2
WR28	Provision of an Identification Standard	18.3	Separate Project See 21.4.2	2012 Q3
WR29	Provision of City Technical Standards including: Automation Design Guide, Tagname Identification Standard, HMI Layout and Animation Plan, and Historical Data Retention Standard	18.4	Separate Project See 21.4.4	Automation Design Guide 2013 Q3 Remainder 2014 Q3
WR30	Preparation and Implementation of a Backup and Disaster Recovery Plan	18.4.5	City or Separate Project See 21.4.9	2015 Q4
WR31	Selection of a appropriate "smart" P&ID software tool.	19.3.1	City	2012 Q4
WR32	Development of a Document Development and Management Standard	19.2	City	2013 Q2
WR33	CWMS Data Entry (Data to be Supplied by Design Team)	19.4	City	As commissioned: 2016 Q3 – 2018 Q2

Notes:

1. A recommendation regarding responsibility for supply and installation of a Testing and Simulation system is not clear at this time. It would be useful to have this in place at the time of the SEWPCC Upgrades; however it may be more logical to locate this at the Central Control Location facility (currently NEWPCC). It could be added to the SEWPCC Upgrades scope of work, or potentially added to the NEWPCC Central Control and Server Room Upgrades, discussed in Section 21.4.7.

21.4 Associated Project Definition

The recommendations in the report that are deemed to be best implemented as separate projects, but associated with the main design assignment and are presented with expected implementation constraints.

21.4.1 DCS HMI Upgrade

Project	**DCS HMI Upgrade**		
Description	Provide design and contract administration services to upgrade the existing DCS HMI system. The original plan was based upon the City's desire to upgrade the existing PCV installation at all three facilities from PCV V5.4 to V5.5b, and provide new HMI hardware. City internal forces are now planning to replace the HMI with ABB's S+ (PGP) product. In addition, as part of the project, upgrade the NVRAM at the SEWPCC and WEWPCC facilities. Further details are available in Section 20.2.		
Priority	1	The HMI hardware and software are suffering from significant obsolescence issues and spare availability.	
Estimated Duration	8 months		
Recommended Start	ASAP → Project being addressed internally	**Predecessors**	-
Recommended Completion	ASAP	**Dependents**	-

21.4.2 Identification Standard Development

Project / Task	**Identification Standard Development**		
Description	The overall objective for the Identification Standard Development is to prepare a document that can be referenced for consistent and accurate identification for all process, mechanical, electrical, and automation equipment. There are multiple existing identification standards, and they have not been consistently applied. The document will provide clear guidance to department personnel, as well as external consultants, regarding appropriate equipment identification. Further details are available in Section 18.3.		
Priority	1	Required imminently to allow for appropriate identifiers to be utilized consistently throughout the entire design process.	
Estimated Duration	6 months		
Recommended Start	2012 Q2 → **In Progress**	**Predecessors**	-
Recommended Completion	2012 Q4	**Dependents**	Preliminary Design

21.4.3 Critical Electrical and Automation Component Standardization

Project / Task	**Critical Electrical and Automation Component Standardization**		
Description	Coordinate with the City's Materials Management Division to define the process required. Prepare a detailed specification and evaluation system, utilize a Bid Opportunity or Request for Proposal Process to obtain vendor submissions, evaluate, and create a standard for the following components: • UPS Units • Control System • Motor Control Equipment • Protocol Converters / Gateways • Gas Detection Systems • Instrumentation • Electrical Power Meters • Valve Actuators – Large Multi-Turn and Quarter Turn • Industrial-Grade Ethernet Switches Further details are available in Section 17.0.		
Priority	**1**	Required imminently to allow Preliminary Design to be completed.	
Estimated Duration	~18 months		
Recommended Start	**ASAP**	**Predecessors**	-
Recommended Completion	Control System 2013 Q3 Overall 2014 Q2	**Dependents**	Control System Selection Required for Preliminary Design at ~50% Stage

21.4.4 Automation Design Guide and Technical Standards

Project / Task	**Automation Design Guide and Technical Standards**		
Description	Development of technical standards which include: *Automation Design Guide* - Provide detailed guidance and design basis regarding specific implementation strategies for the automation design of new installations and upgrades to the wastewater facilities. *Tagname Identification Standard* - Provide detailed guidance regarding the identification of software tagnames within the PLC and HMI systems. *HMI Layout and Animation Plan* – This standard would provide detailed guidance regarding the presentation of graphical and text data on the Human Machine Interface (HMI) stations. It would ensure that data is presented to operations personnel in a clear and consistent manner, to allow for efficient monitoring of the facility processes. A *Historical Data Retention Standard* would provide general guidance regarding the retention of data produced by the control system, including frequency of logging, and data archival. This is required to manage the huge volumes of historical data the control system is able to produce. Further details are available in Section 18.0.		
Priority	1	Required soon to allow detailed design to proceed.	
Estimated Duration	15 months		
Recommended Start	2012 Q3	**Predecessors**	Ideally PLC and HMI Selection complete prior to Completing Design Guide.
Recommended Completion	2013 Q3 (Automation Design Guide) 2013 Q4 (Remainder)	**Dependents**	Automation Design Guide Required prior to Detailed Design.

21.4.5 SEWPCC DCS Upgrades

Project	**SEWPCC DCS Upgrades**		
Description	Provide a review of replacement timeline of the SEWPCC DCS, and recommend replacements / upgrades of critical DCS components to ensure that the DCS remains operational until replacement is complete. Provide detailed design and contract administration services to provide the necessary DCS upgrades at the SEWPCC facility. See Section 20.3 for further information.		
Priority	**2**	It is suspected that certain DCS components are obsolete and could contribute to reduced reliability at the SEWPCC facility.	
Estimated Duration	4 months		
Recommended Start	2013 Q1	**Predecessors**	-
Recommended Completion	2013 Q3	**Dependents**	-

Note: *The above fee estimate assumes that the City approves a sole source agreement with ABB's standard Terms and Conditions. If this is not the case, the fees are anticipated to be significantly higher.*

21.4.6 WEWPCC DCS Upgrades

Project	**WEWPCC DCS Upgrades**		
Description	Provide a review of replacement timeline of the WEWPCC DCS, and recommend replacements / upgrades of critical DCS components to ensure that the DCS remains operational until replacement is complete. Provide detailed design and contract administration services to provide the necessary DCS upgrades at the WEWPCC facility. See Section 20.3 for further information.		
Priority	**2**	It is suspected that certain DCS components are obsolete and could contribute to reduced reliability at the WEWPCC facility.	
Estimated Duration	6 months		
Recommended Start	2013 Q1	**Predecessors**	-
Recommended Completion	2013 Q3	**Dependents**	-

Note: *The above fee estimate assumes that the City approves a sole source agreement with ABB's standard Terms and Conditions. If this is not the case, the fees cannot be accurately assessed at this time.*

21.4.7 NEWPCC Central Control and Server Room Upgrades

Project	**NEWPCC Central Control and Server Room Upgrades**		
Description	Upgrade the NEWPCC Control and Server Rooms, including networking, to support remote monitoring of the SEWPCC facility, as well as installation of a Central Historian Server and Web Server. See Section 12.10.512.10 for further information.		
Priority	**2**	A DCS upgrade was completed in 2005, and thus the NEWPCC facility DCS should be acceptable until ~2015.	
Estimated Duration	24 months		
Recommended Start	2014 Q1	**Predecessors**	Automation System Vendor Selection
Recommended Completion	2016 Q1	**Dependents**	SEWPCC Commissioning

Note: *The above fee estimate assumes that the City approves a sole source agreement with ABB's standard Terms and Conditions. If this is not the case, the fees cannot be accurately assessed at this time.*

21.4.8 NEWPCC DCS Upgrades

Project	**NEWPCC DCS Upgrades**		
Description	Provide a review of replacement timeline of the NEWPCC DCS, and recommend replacements / upgrades of critical DCS components to ensure that the DCS remains operational until replacement is complete. Provide detailed design and contract administration services to provide the necessary DCS upgrades at the NEWPCC facility. See Section 20.3 for further information.		
Priority	**3**	A DCS upgrade was completed in 2005, and thus the NEWPCC facility DCS should be acceptable until ~2015.	
Estimated Duration	6 months		
Recommended Start	2014 Q2	**Predecessors**	-
Recommended Completion	2014 Q4	**Dependents**	-

Note: *The above fee estimate assumes that the City approves a sole source agreement with ABB's standard Terms and Conditions. If this is not the case, the fees cannot be accurately assessed at this time.*

21.4.9 Backup and Disaster Recovery Plan

Project / Task	**Backup and Disaster Recovery Plan**		
Description	The City of Winnipeg requires a clear, practical plan to address unplanned scenarios such as hardware failure, fire, vandalism and theft, software corruption, and accidental errors introduced into an application. Further details are available in Section 18.4.5.		
Priority	**3**	Required Prior to Completion of Commissioning	
Estimated Duration	4 months		
Recommended Start	2015 Q3	**Predecessors**	PLC and HMI Selection Detailed Design
Recommended Completion	2015 Q4	**Dependents**	-

21.4.10 CWMS Integration

Project / Task	**CWMS Integration**		
Description	Integration of the CWMS system with the HMI to allow for automatic generation of work orders and other features. Further details are available in Section 12.13.2.		
Priority	**3**		
Estimated Duration	12 months		
Recommended Start	2015 Q4	**Predecessors**	PLC and HMI Selection NEWPCC Central Control and Server Room Upgrades (prior to 50%)
Recommended Completion	2016 Q4	**Dependents**	-

21.4.11 LIMS Integration

Project / Task	**LIMS System Integration**		
Description	Integration of the LIMS system with the HMI and Historian to allow for automatic data transfer. Further details are available in Section 12.13.3.		
Priority	**3**		
Estimated Duration	12 months		
Recommended Start	2016 Q4	**Predecessors**	PLC and HMI Selection NEWPCC Central Control and Server Room Upgrades
Recommended Completion	2017 Q4	**Dependents**	-

21.4.12 Collections System Integration

Project / Task	**Collections System Integration**		
Description	Provision of interfaces to allow for automated sharing of operational information between Collections and Wastewater Treatment systems. Further details are available in Section 12.12.		
Priority	**3**		
Estimated Duration	6 months		
Recommended Start	2017 Q1	**Predecessors**	PLC and HMI Selection NEWPCC Central Control and Server Room Upgrades
Recommended Completion	2017 Q3	**Dependents**	-