TULSA Water and Sewer Department

SCADA System Improvements

Alarm Standards

FINAL

PRESENTED TO

Cindy Cantero
City of Tulsa
Water Pollution Control
175 E 2nd Street, Suite 1400, Tulsa, OK 74103

PREPARED BY

Tetra Tech
7645 E. 63rd St.,
Suite 301
Tulsa, Ok 74133

P: *(918) 249-3909*
www.tetratech.com

200-11383-19001
April 05, 2022

CONTENTS

1 INTRODUCTION 8
1.1 Purpose of the Alarm Standard 9
1.2 Scope 9
1.3 Assumptions 9
2 ALARM MANAGEMENT PRINCIPLES 10
2.1 Purpose of the Alarm System 10
2.2 Operator Notifications 10
2.2.1 Definition of an Alarm 10
2.2.2 Other Notification Types 11
3 ALARM DESIGN PRINCIPLES 11
3.1 Supported Alarm States and Modes 12
3.2 Alarm Management Lifecycle 13
4 TERMINOLOGY & REFERENCES 15
4.1 Reference Materials 17
5 ROLES & RESPONSIBILITIES 17
6 ALARM IDENTIFICATION 18
7 ALARM DOCUMENTATION AND RATIONALIZATION 18
7.1 Alarm Rationalization Methodology 18
7.2 Alarm Justification 19
7.3 Consequence of Inaction or Incorrect Action 19
7.4 Operator Response Time 19
7.5 Cause, Confirmation, and Operator Corrective Action 20
7.6 Alarm Priority Determination 20
7.6.1 Alarm Priorities 20
7.6.2 Prioritization Methodology 21
7.6.3 Alarm Priority Distribution 22
7.7 Alarm Setpoint Selection 22
7.8 Alarm Classification and Management of Requirements 22
7.9 Alarm Documentation and the Master Alarm Database 22
8 ALARM DESIGN 23
8.1 Application of Alarm Types 23
8.2 Application of Alarm Deadband 24
8.3 Application of On & Off Delay 24
8.3.1 Control System Diagnostic Alarms 25
9 ALARM SCADA INTERFACE 25

9.1 Alarm Summary Display Characteristics and Usage 25
9.2 Alarm Indications within SCADA Displays 26
9.3 Navigation and Alarm Response 28
9.4 External Annunciators 28
10 ALARM SYSTEM IMPLEMENTATION, OPERATION, AND MAINTENANCE 28
10.1 Alarm Commissioning Practices 28
10.2 Alarm System Testing 28
10.3 Maintenance 29
10.4 Alarm Out-of-Service Procedure 29
10.5 Alarm System Training 30
10.6 Alarm Response Procedures 30
11 ALARM SYSTEM PERFORMANCE MONITORING, ASSESSMENT, AND AUDITS 31
11.1 Alarm System Key Performance Indicators (KPIs) 31
11.2 Alarm Performance Reporting 31
11.2.1 Average Alarm Rate Per 10 Minutes 31
11.2.2 Alarm Flood Analysis 31
11.2.3 Alarm Out-of-Service 32
11.2.4 Alarm Priority Distribution 32
11.2.5 Standing Alarms 32
11.2.6 Frequently Occurring Alarms 32
11.2.7 Fleeting Alarms List 32
11.3 Record / History Preservation 32
11.4 Alarm Audits 32
12 ALARM SYSTEM MANAGEMENT OF CHANGE (MOC) 33
12.1 MOC Applicability 33
12.2 MOC Methodology 34
12.2.1 Formal MOC 34
12.2.2 Informal MOC 34
12.3 MOC Requirements 35
APPENDIX A ALARM RATIONALIZATION PROCESS 36
APPENDIX B ALARM STANDARDS 37
B1 ACTUATOR (ISOLATING) 37
B1.1 Introduction 37
B1.2 Standard Actuator Alarm Design 37
B1.3 Hardwire Alarms 37
B1.4 Software Alarms 38
B1.5 Specialty Actuator Alarm Design 38

B2 ACTUATOR (THROTTLING) 39
B2.1 Introduction 39
B2.2 Standard Actuator Alarm Design 39
B2.2.1 Hardwire Alarms 39
B2.2.2 Software Alarms 40
B2.3 Specialty Actuator Alarm Design 40
B3 CLARIFIER 40
B3.1 Introduction 40
B3.2 Standard Clarifier Alarm Design 41
B3.2.1 Hardwire Alarms 41
B3.2.2 Software Alarms 41
B3.3 Special Clarifier Alarm Design 42
B4 CONTINUOUS INSTRUMENT 43
B4.1 Introduction 43
B4.2 Standard Continuous Instrument Alarm Design 43
B4.2.1 Hardwire Alarms 44
B4.2.2 Software Alarms 44
B4.3 Specialty Continuous Instrument Alarm Design 45
B5 CONTROL PANELS 45
B5.1 Introduction 45
B5.2 Standard Control Panel Alarm Design 45
B5.2.1 Hardwire Alarms 45
B5.2.2 Software Alarms 46
B5.3 Specialty Control Panel Alarm Design 47
B5.3.1 Temperature Monitoring 47
B5.3.2 Panel Intrusion Alarm 47
B6 MANUFACTURER SUPPLIED CONTROL SYSTEMS 47
B6.1 Introduction 47
B6.2 Standard Manufacturer's Equipment Alarm Design 48
B6.2.1 Hardwire Alarms (if a PLC is not provided) 48
B6.2.2 Software Alarms 49
B6.3 Specialty Manufacturer's Equipment Alarm Design 50
B6.3.1 Environmental Monitoring 50
B6.3.2 Ambient Temperature Monitoring 50
B6.3.3 Combustible Gas Detection 50
B6.3.4 Fire/Smoke Detection 51

B6.3.5 Spill/Flood Detection 51
B6.3.6 Vibration Monitoring 51
B6.3.7 Seal Water or Cooling Water Flow Monitoring 51
B6.3.8 Pressure Sensing 51
B7 MEDIUM-VOLTAGE BLOWER 52
B7.1 Introduction 52
B7.2 Standard Blower Alarm Design 52
B7.2.1 Hardwire Alarms 52
B7.2.2 Software Alarms 53
B7.3 Specialty Blower Alarm Design 54
B7.3.1 Vibration Monitoring 54
B7.3.2 Pressure Sensing 54
B8 MIXER 55
B8.1 Introduction 55
B8.2 Standard Mixer Alarm Design 55
B8.2.1 Hardwire Alarms 55
B8.2.2 Software Alarms 56
B8.3 Specialty Mixer Alarm Design 56
B9 PUMP (NON-SUBMERSIBLE) 56
B9.1 Introduction 56
B9.2 Standard Pump Alarm Design 57
B9.2.1 Hardwire Alarms 57
B9.2.2 Software Alarms 57
B9.3 Specialty Pump Alarm Design 58
B9.3.1 Vibration Monitoring 58
B9.3.2 Bearing Temperature 58
B9.3.3 Pressure Sensing 59
B9.3.4 Seal Water Monitoring 59
B10 PUMP (SUBMERSIBLE) 59
B10.1 Introduction 59
B10.2 Standard Pump Alarm Design 60
B10.2.1 Hardwire Alarms 60
B10.2.2 Software Alarms 60
B10.3 Specialty Pump Alarm Design 61
B10.3.1 Pressure Sensing 61
B11 REDUCED-VOLTAGE SOFT STARTERS 62

B11.1 Introduction 62
B11.2 Standard Reduced-Voltage Soft Starter Alarm Design 62
B11.2.1 Hardwire Alarms 62
B11.2.2 Software Alarms 62
B11.3 Specialty Reduced-Voltage Soft Starter Alarm Design 63
B11.3.1 RVSS Communications Failure 63
B11.3.2 Ground Fault 63
B11.3.3 Torque Out of Range 64
B11.3.4 Input Phase Loss 64
B12 VARIABLE-FREQUENCY DRIVES 64
B12.1 Introduction 64
B12.2 Standard Variable-Frequency Drive Alarm Design 64
B12.2.1 Hardwire Alarms 64
B12.2.2 Software Alarms 65
B12.3 Specialty Variable-Frequency Drive Alarm Design 66
B12.3.1 VFD Communications Failure 66
B12.3.2 Ground Fault 66
B12.3.3 Overvoltage 66
B12.3.4 Input Phase Loss 66

List of Tables

Table 2-1 Operator Notifications 10
Table 3-1 Supported Alarm States 12
Table 3-2 Supported Alarm Modes 13
Table 3-3 Stages of the Alarm Management Lifecycle 14
Table 4-1 Common Definitions 15
Table 5-1 Alarm System Responsibilities 18
Table 7-1 Operator Response Times 20
Table 7-2 Prioritization Matrix 21
Table 8-1 Alarm Types 23
Table 9-1 Alarm Summary Configuration 26
Table 9-2 Alarm Indication Matrix 27
Table 12-1 MOC Types 34
Table B1-1 Actuator Minimum Alarms 38
Table B2-1 Actuator Minimum Alarms 40
Table B3-1 Clarifier Minimum Alarms 41
Table B3-2 Clarifier Specialty Clarifier Alarms 43
Table B4-1 Continuous Instrument Minimum Alarms 44
Table B5-1 Equipment Generic Minimum Alarms 46
Table B5-2 Specialty Alarms for Control Panels 47
Table B6-1 Equipment Generic Minimum Alarms 50
Table B6-2 Specialty Equipment Alarms 51
Table B7-1 Medium Voltage Blower Minimum Alarms 54
Table B7-2 Specialty Blower Alarms 55
Table B8-1 Mixer Minimum Alarms 56
Table B9-1 Pump Minimum Alarms 58
Table B9-2 Specialty Pump Alarms 59
Table B10-1 Pump Minimum Alarms 61
Table B10-2 Specialty Pump Alarms 61
Table B11-1 RVSS Minimum Alarms 63
Table B11-2 Specialty RVSS Alarms 64
Table B12-1 VFD Minimum Alarms 65
Table B12-2 Specialty VFD Alarms 66

List of Figures

Figure 1-1 ISA 18.2 Workflow 8
Figure 3-1 Alarm Management Lifecycle per ISA-18.2 14
Figure 7-1 Rationalization Process 19
Figure 9-1 Alarm Summary 26
Figure 9-2 Level 1 Alarm Symbol 27
Figure 9-3 Level 2 Alarm Symbol 27
Figure 9-4 Level 3 Alarm Symbol 27
Figure 9-5 Level 4 Alarm Symbol 27
Figure 9-6 Alarm Navigation 28
Figure A-1 Rationalization Process 36

Revision History

Version	Date	Description
A	October 29, 2019	Draft delivered to client.
B	March 16, 2020	Final document delivered to client.
C	July 9, 2021	Updated to include equipment alarms – Draft delivered to client.
D	April 4, 2022	Final delivered to the client.

1 INTRODUCTION

This alarm standard is based on International Society of Automation (ISA) Standard 18.2 – 2016 Management of Alarm Systems for the Process Industries and contains direct references to the operation and configuration of the SCADA system with the intent to integrate this document with features available within SCADA.

This has been developed as part of the alarm management lifecycle. The alarm management lifecycle is a general methodology for implementation of alarm management functions, to:

- identify resources and personnel required to implement alarms
- develop alarm management standards that relate to organizational goals and purpose
- continually monitor and assess alarm performance
- manage change to the alarm system, standards, and lifecycle stages
- perform audits of the process

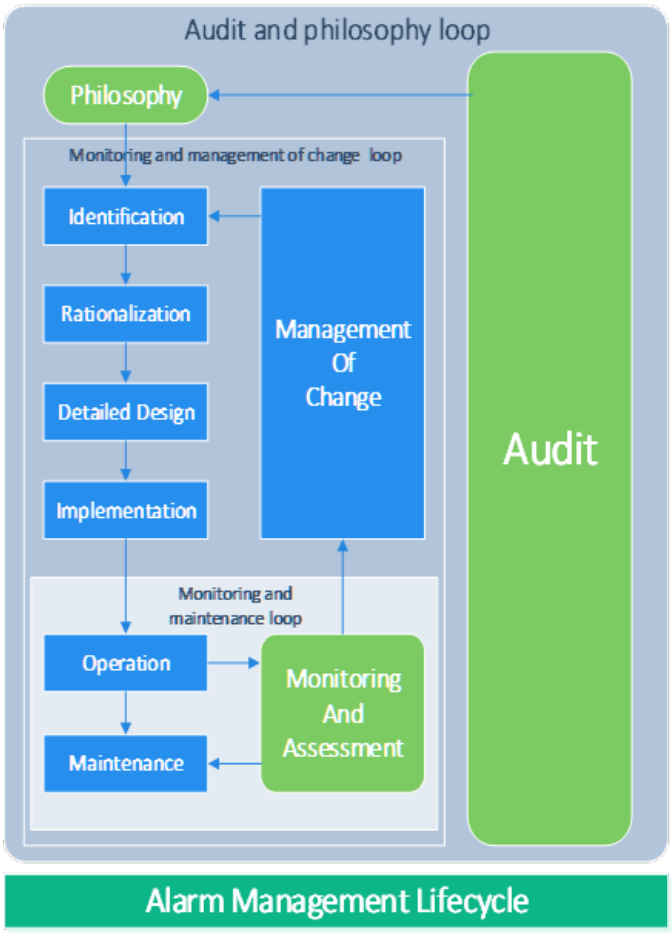

Figure 1-1 ISA 18.2 Workflow

The ISA standard topics will be implemented according to the workflow presented within this standard. This workflow provides a general methodology for implementing the desired management functions that will be selected by Tulsa Water and Sewer. It enables Tulsa Water and Sewer to establish resources and personnel required to implement the Alarm Standard and establish Alarm Management Standards that relate directly to their organization. Future implementation of the standard and management restrictions will be tailored to Tulsa Water and Sewer's operational and business needs.

As with any document or standard defining detailed operations within an organization, this standard must be a "living document" that is periodically updated to reflect changes in operating and organizational conditions. The workflow addresses this issue by identifying entry points into the workflow (in green):

Standard/Philosophy – This is the origin of the workflow and begins with the development of the Alarm Standard (this document). The alarm standard will aid Tulsa Water and Sewer in developing operational consistency, identify risks, and manage a system supporting effective operator response.

Audit – Recurring effort to evaluate alarm systems and the management practices for these systems. This usually occurs when significant changes are made to the organization or SCADA that would change this document.

Monitoring and Assessment – this is a recurring effort that is typically required when minor changes are made to the process or SCADA, such as equipment replacement or minor process changes and upgrades. This task is typically included part of a "continuous improvement process" for process operation. This effort includes:

- Identification – Select process variables that require an alarm function.
- Rationalization – What is the rational for identifying an alarm. What criteria will be established for defining alarms. This is the process to review potential alarms using alarm standard principles for design and document the reason for each alarm.
- Detailed design – Selecting the parameters to establish the alarm condition and when the condition is cleared
- Implementation – Defining how the alarm will be implemented and where it will be generated.
- Operation – Identify what impacts are associated with an alarm. Developing Standard Operating Procedures (SOP) for specific conditions to establish consistency in operator responses.
- Maintenance – Establishing procedures and methods for maintaining the alarm system as well as individual alarms.
- Management of Change – Establishing the process and procedures to validate the design, implementation, and documentation of alarms.

This Alarm Standard follows the ISA Alarm Management Lifecycle workflow.

1.1 Purpose of the Alarm Standard

This alarm standard establishes the basic definitions, principles, and processes for the design, implementation, maintenance, and management of alarm system(s). It contains the alarm system performance goals and describes the key work practices, roles and responsibilities. This document provides guidance for a consistent approach to alarm management and defines how the activities of the alarm management lifecycle will be followed.

A written standard on alarm management is critical to creating and maintaining an effective alarm system over time. A documented alarm standard promotes:

- consistency of alarm design and presentation
- agreement with corporate risk management goals/objectives
- agreement with good engineering practices
- efficient alarm rationalization and design activities
- effective operator response to alarms

1.2 Scope

This document applies to all personnel involved in the design, implementation, operation, maintenance, and modification of new and existing alarm systems. It is intended for both in-house and contractor use.

1.3 Assumptions

The following assumptions are made to successfully implement the principles of this document:

- Equipment shall be designed to be inherently safe without the need for alarms whenever possible.
- No amount of alarm management will replace the surveillance of a competent operator.
- Operators will respond to all annunciated alarms, regardless of priority.
- Systems will be designed so the operator is capable of effectively responding to all alarms in all anticipated scenarios. Operators will be trained on the relevant parts of the alarm system for the plants they operate.
- It will be subject to periodic review and revision as part of an audit process.
- This standard will be a living document to reflect best corporate & industry practice as well as all appropriate national & international regulations.

2 ALARM MANAGEMENT PRINCIPLES

The advent of computer-based control systems has created a situation where it is possible to configure large numbers of alarms with minimal cost or consideration as to whether they are truly necessary. Historically, alarms have also been created in an unstructured manner. This has resulted in:

- Too many alarms being configured (e.g., alarms that do not have associated operator actions).
- Alarms being ill defined (e.g., alarms given incorrect priorities).
- Poor alarm system performance (e.g., bad actors, increased potential for alarm floods).
- Increased potential for operator error (e.g., operator missing an important alarm during a flood or taking incorrect action based on a received alarm).
- Significant demand on operator and engineer resources and additional costs to rectify alarm performance problems.

2.1 Purpose of the Alarm System

The purpose of the alarm system is to notify the operator of abnormal situations requiring timely operator action and to direct their attention so that they can take corrective action and prevent an undesired consequence. The alarm system must be designed for effective handling of a single alarm during normal operation and the handling of many alarms during major upsets.

2.2 Operator Notifications

Operator notifications can represent abnormal or expected events and may or may not require an operator action. This standard will define two types of notification:

Table 2-1 Operator Notifications

Event	Operator Action Required	Operator Action NOT Required
Abnormal	Alarm	Alert or Event
Expected	Prompt	Event

Each operator notification will be managed differently, as required by the risks and potential consequences of the situation. Systems and equipment employed to inform the operator of a change in state of the facility shall be designed so that incoming notifications do not overwhelm but help lead the operator to appropriate action.

2.2.1 Definition of an Alarm

Defining what is an alarm is a foundational part of alarm management. It serves as a guide to all other alarm standards and operational decisions.

> *"An alarm is an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response."*

"An alarm is an audible and/or visible means of indicating" - There must be an indication of the alarm. An alarm limit can be configured to generate control actions or log data but if this limit is not audibly or visually indicated it should not be considered an alarm.

“to the operator” - The indication must be targeted to the operator to be an alarm, not to provide information to an engineer, maintenance technician, or manager.

“an equipment malfunction, process deviation, or abnormal condition” - The alarm must indicate a problem, not a normal process condition or normal operational event (e.g., pump stopped, valve closed). The automation system should be configured to determine if any events have occurred unexpectedly. If an unexpected or abnormal event has occurred and operator action is required, this notification should be classified as an alarm.

“requiring a response.” - There must be a defined operator response to correct the condition and bring the process back to a desired (safe and/or productive) state. If the operator does not need to respond, then the condition should not be an alarm. A notification that has no associated operator action should be defined as an alert or message. Acknowledging the alarm or logging a measurement is not considered an operator response (does not correct the abnormal situation). Typical operator responses to alarms include:

- Request field operator to close a valve.
- Change the setpoint or output of a controller.
- Start a backup pump.
- Raise a corrective action work order.

This agreed upon definition makes it clear that normal process conditions, expected equipment state changes, and/or conditions that do not require responses in a timely fashion are not alarms.

2.2.2 Other Notification Types

Notifications that do not meet the criteria for being an alarm fall into several categories.

Alert - An audible and/or visible means of indicating to the operator an abnormal equipment or process condition that requires awareness, but not a response. An alert will be indicated separately (segregated) from an alarm indication.

Prompt - A notification which requires an action to be taken by the operator as part of normal operation (e.g., start sequence when ready, take a sample, add material A).

Message - Provides information about the status of normal operations that does not require the operator to act. As an example, when a process or piece of equipment has moved from one mode of operation to another, it may be desirable to inform the operator of this progress with a message (e.g., "Backwash Step 2 Complete").

Events - Used for automated logging of discrete changes to the system or process. They are used primarily for review and analysis (e.g., for post incident analysis). Equipment and process events should be elevated to an alarm if there is an associated operator action(s).

3 ALARM DESIGN PRINCIPLES

Alarm design consideration will begin at the engineering and planning stage of any project. Process engineers will consult with the Standards Committee during the design stage to ensure proper alarm standards are met.

Alarms will be identified throughout the design process and be documented in the following:

- Process and Instrument Designs (P&ID’s)
- Process Control Narratives (PCN’s)

The alarm name shall adhere to the Tag Naming Standard and be used on all documentation.

Prior to construction and implementation contractors will provide:

- Submittals identifying the alarms.
- The conditions at which the alarm will trigger.
- The appropriate response to the alarm.

The following basic alarm principles should be applied to alarm design and configuration:

- **Each alarm should alert, inform and guide.**
  The information presented to the operator should not simply be the tag number of the measuring or sensing instrument but shall (where possible) offer an indication of what has gone wrong and why it has occurred.
- **Every alarm presented to the operator should be relevant and unique.**
  Alarms should be designed so that they are worthy of operator action in all plant states and operating conditions in which they are displayed. Each configured alarm shall be unambiguous and not duplicated by other alarms. Multiple alarms should not be annunciated for a single problem or event such as those requiring the same operator action.
- **Every alarm should have a defined (required) response.**
  If there is no associated operator action, then the condition should not be configured as an alarm. An alternative notification type (such as an alert) should be considered.
- **Adequate time should be allowed for the operator to analyze the situation and carry out a defined response.**
  Operator response time includes the time to diagnose the problem and perform the corrective actions. A typical response could include troubleshooting, leaving the control room, contacting other personnel, and performing a manual task (such as closing a manual shut-off valve).
- **Alarms should be explicitly designed to consider human limitations.**
  The number and rate of alarms should be presented to the operator in a way that they can effectively respond to all alarms as well as carrying out their other duties.

3.1 Supported Alarm States and Modes

Within the SCADA system, alarms follow a state-based model. Alarms transition between states due to value changes, or operator actions. The table 2-2 lists the supported alarm states.

Table 3-1 Supported Alarm States

State Name	Description
ACK_RTN	The normal (initial) state indicating: • alarm has returned-to-normal range, and • alarm has been acknowledged.
UNACK_ALM	The unacknowledged state indicating: • alarm is active due to an abnormal condition, and • alarm has NOT been acknowledged.
ACK_ALM	The acknowledged state indicating: • alarm is active due to an abnormal condition, and • alarm has been acknowledged.

State Name	Description
UNACK_RTN	The unacknowledged-return state indicating: • alarm was active due to an abnormal condition, • alarm has returned-to-normal range, and • alarm has NOT been acknowledged.

Additionally, alarm modes turn on or off the notification and distribution of alarms in SCADA based on operator commands. This provides a method for the operator to selectively disable portions of the alarm system for known equipment or site outages to reduce operator load. The following alarm modes are available:

Table 3-2 Supported Alarm Modes

Alarm Mode	Description
Enabled	The normal mode where: • alarm is functional, and • alarm is displayed to operator, and • alarm is stored in history.
Silenced	The silenced mode where: • alarm is functional, and • alarm is NOT displayed to operator, and • alarm is stored in history.
Disabled	The disabled mode indicating: • alarm is NOT functional, and • alarm is NOT displayed to operator, and • alarm is NOT stored in history.

3.2 Alarm Management Lifecycle

Alarm management is a continuous improvement process. The work process for effective alarm management is defined in the ISA-18.2 standard. The key activities of alarm management are executed in the different stages of the lifecycle. The products of each stage are the inputs for the activities of the next stage. See figure 3-1 and table 3-3 for information on the lifecycle.

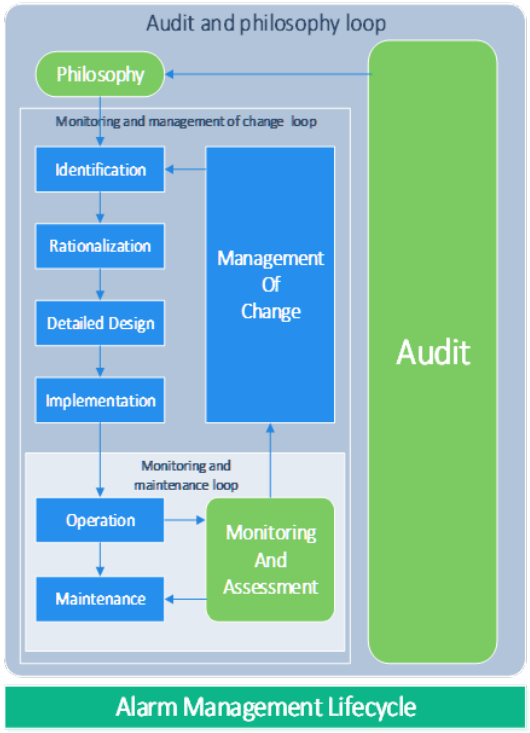

Figure 3-1 Alarm Management Lifecycle per ISA-18.2

Table 3-3 Stages of the Alarm Management Lifecycle

Stage	Activity	Inputs	Outputs
Standard	Define processes for alarm management.	Corporate goals, industry best practices, good engineering practices, alarm management standards.	Alarm standard.
Identification	Determine potential alarms.	Existing alarm database, critical operating limits, key process parameters, PHA report, incident investigations, P&IDs, operating procedures, safety requirements, etc.	List of potential alarms.
Rationalization	Rationalization, classification, prioritization, and documentation.	Alarm standard and list of potential alarms.	Master alarm database, alarm design requirements.

Stage	Activity	Inputs	Outputs
Detailed Design	Basic alarm design, HMI design, and advanced alarming design.	Master alarm database, alarm design requirements.	Completed alarm design.
Implementation	Install alarms, initial testing, and initial training.	Completed alarm design and master alarm database.	Operational alarms and procedures.
Operation	Operator responds to alarms, refresher training.	Operational alarms and procedures.	Alarm event data.
Maintenance	Inspection, repair and replacement, periodic testing.	Alarm monitoring reports, alarm standard, inspection and testing procedures.	Alarm reliability data.
Monitoring & Assessment	Monitor alarm data and report performance.	Alarm event and reliability data and alarm standard.	Alarm monitoring reports, proposed changes.
Management of Change	Process to authorize additions, modifications, and deletions of alarms.	Alarm standard, proposed changes.	Authorized alarm changes.
Audit	Periodic audit of alarm management processes.	Standards, alarm standard, and audit protocol.	Recommendations for Improvement.

4 TERMINOLOGY & REFERENCES

The table below describes common alarm terms used in this standard and the alarm management lifecycle.

Table 4-1 Common Definitions

Term	Definition
Acknowledge	operator action confirming alarm indication
Active	alarm condition is true
Advanced alarming	collection of techniques to manage annunciations during specific conditions
Allowable response time	time between action and annunciation
Annunciation	alarm system calling attention to operator
Assessment	comparison of information from monitoring alarm system against stated goals and performance metrics
Audit	assessment evaluating alarm system performance and work practices used to administer the alarm system
Absolute	setpoint exceeded
Adaptive	setpoint changed by algorithm
Adjustable	operator adjustable setpoint

Benchmark	initial audit designed to identify problem areas for the purpose of formulating improvement plans
Bit-pattern	predetermined pattern of digital signals match
Calculated	generated from calculation versus measured
Chattering	transition active/inactive in a short period of time repeatedly
Controller Output	generated by PID output
Deadband	the range through which an input can be varied without initiating an observable response
Decommission	process to remove alarm from alarm system
Delay (on/off)	debounce - time an alarm remains active after the process measurement has returned within the alarm setpoint
Deviation	difference between two values exceed setpoint
Enforcement	enhanced alarm technique to verify and restore alarm attributes to values in the Master Alarm Database
Event	representation of a solicited or unsolicited state change
Filtering	display alarm records to a given element of the alarm
Fleeting	transition active/inactive in a short period of time without repetition
Flooding	condition where alarm rate is greater than operator can effectively manage
Groups	alarms sorted and combined into groups
Historian	long term repository for alarm records
Highly Managed Alarm	alarm class with additional regulatory/safety requirements
Implementation	transition stage between design and when alarm is put into service
Instrument diagnostic	indication of device or signal fault
Latching	remains in alarm after process returns to normal, requires operator reset
Log	short term repository for alarm records
Mismatch	difference between expected state versus actual
Management	collection of practices for determining, documenting, designing, operating, monitoring and maintaining alarm systems
Master Alarm Database	authorized list of rationalized alarm and associated attributes
Monitoring	measurement and reporting of alarm system performance
Nuisance	annunciates excessively or does not return-to-normal after operator action
Out of range alarms	state of an alarm during which the alarm indication is indefinitely suppressed, typically manually, for reasons such as maintenance
Out of Service	alarm indication is indefinitely suppressed
Philosophy	document establishing basic definitions, principles, and processes to design, implement, and maintain alarm systems
Prioritization	process of assigning level of importance
Rate	number of annunciated alarms, per operator in a specific time period
Rate of Change	change in Process Variable (PV) over time exceeds setpoint
Rationalization	process to review potential alarms using alarm philosophy principles for design and document the reason for each alarm
Recipe-driven	alarm setpoints depend on recipe currently executed
Remote	alarm from remotely operated facility

Reset	operator action unlatching a latched alarm
Re-trigger	automatically re-annunciate and alarm under certain conditions
Return to normal	transition from active to inactive state
Safety	critical for protection of human life or environment
Shelve	temporarily suppress an alarm initiated by an operator with controls that unsuppress the alarm
Silence	operator action that terminates audible annunciation
Sorting	function which orders alarm records to be displayed according to a given element of alarm record
Smart Alarms	operational consistency alarms that check against a control narrative for required steps or a conditional against a series of events
Stale	remains annunciated for an extended time period (typ. 24 hrs)
State	attributes modified or suppressed based upon operating state or process conditions
Statistical	based on statistical process of Process Variable (PV)
Summary	display listing annunciated alarms with selected information
Suppress	prevent annunciation when alarm active
Suppress by design	suppress based upon process conditions
System	collection of hardware and software detecting alarm state, indication to operators, and records changes in alarm state
System diagnostic	fault within system hardware
Unacknowledged	operator has not confirmed recognition of alarm indication

4.1 Reference Materials

Reference information from multiple sources should be utilized to support the alarm rationalization process during alarm development. The Master Alarm Database (MADB) will include entries that point to these items for quick reference to the appropriate support information. Reference sources may include:

- P&IDs
- Instrument Index
- Instrument Calibration Sheets
- PLC I/O Drawings
- PCN's
- Tulsa Water and Sewer Design Standards

In preparation of this document, several references were used to define the required content and industry guidelines for typical settings. Those include:

- ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries
- ISA-TR18.2.1-2018, Alarm Standard
- ISA-TR18.2.2-2016, Alarm Identification and Rationalization
- ISA-TR18.2.3-2015, Basic Alarm Design
- ISA-TR18.2.4-2012, Enhanced and Advanced Alarm Methods
- ISA-TR18.2.5-2012, Alarm System Monitoring, Assessment, and Auditing

5 ROLES & RESPONSIBILITIES

The table below defines the roles and responsibilities of the alarm system.

Table 5-1 Alarm System Responsibilities

Task	Role Description	Individual/Department
System Owner	Responsible for linking the end-user needs with the system implementation and management.	Support Services
System Management and Maintenance	Responsible for managing and maintaining the alarm system configuration in the Process Control System.	Support Services
System Technical Support	Responsible for providing technical support of the alarm system including software and hardware related to the overall system.	Support Services
System Audits	Responsible for facilitating periodic audits of the alarm system to ensure the requirements of the alarm standard are followed.	Support Services

6 ALARM IDENTIFICATION

Alarm identification is typically an external process to the alarm management lifecycle.

The following methods are typically used for identifying the need for an alarm:

- Existing Process Control System and SCADA database configurations.
- Operational requirements based upon regulatory compliance.
- Design criteria established by Design or Maintenance Engineering during process design.
- Equipment and process specifications from Manufacturer, Design, or Maintenance Engineering.
- Institutional knowledge based upon previous observation.
- Other Operations, Maintenance, Engineering, or EH&S requirements.

The identification of an alarm from one or more of these methods does not guarantee that an alarm will be implemented in the SCADA system. The identified alarms must be rationalized prior to performing further design or implementation.

7 ALARM DOCUMENTATION AND RATIONALIZATION

The Rationalization Process is an engineering process to establish which process variables should become alarms in a consistent manner requiring rigor to define legitimate attributes and conditions forcing operator intervention.

The documentation and rationalization (D&R) stage of the alarm management lifecycle is a process for verifying alarms are necessary and meaningful, establishing their design (priority, limit, deadband) and documenting their basis (cause, consequence, corrective action) in the MADB. The MADB and the alarm standard are likely the two most important documents in the alarm management lifecycle. They serve as inputs to most of the follow-on and parallel stages in the lifecycle.

7.1 Alarm Rationalization Methodology

Alarm rationalization follows a structured methodology to review the potential alarm list against the alarm principles and to develop a rationalized list of alarms. The process of rationalizing alarms is a rigorous effort involving many different groups with different backgrounds. The flowchart below depicts the methodology.

During the process, the rationalization team may choose to group alarms together when performing the analysis. This will likely lessen the time to analyze and provide more consistent configurations across the Process Control and SCADA systems. The alarm rationalization process can be seen in Figure 3 and Appendix A.

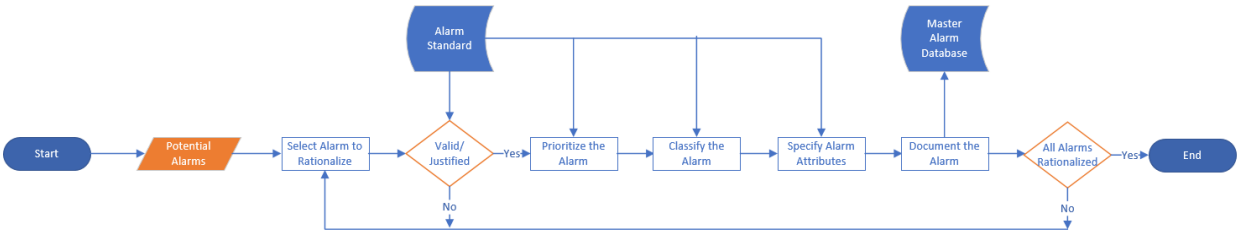

Figure 7-1 Rationalization Process

7.2 Alarm Justification

The alarm justification process is a simple checklist that validates that the alarm being rationalized meets the principles of the alarm standard. Using a checklist format, the rationalization team should assess the following factors:

- ✓ Does the alarm indicate a malfunction, deviation, or abnormal condition?
- ✓ Does the alarm require a timely operator action in order to avoid defined consequences?
- ✓ Is the alarm unique, or are there other alarms that indicate the same condition?
- ✓ Is this alarm the best indicator of the root cause of the abnormal situation?

Although these questions seem straight forward, there will be many instances that can argued either for, or against, an alarm being justified. For this reason, the rationalization process should be performed with a pragmatic team that maintains a consistent approach to justifying the need for alarms.

7.3 Consequence of Inaction or Incorrect Action

Abnormal situations can have potential consequences that relate to multiple key impact areas. These impact areas include:

- Personnel Safety
- Environmental
- Water Quality
- Equipment & Process

Inside each impact area the consequences will be broken into the following groups of severity categories:

- Severe
- Major
- Minor
- None

7.4 Operator Response Time

There are four operator response times, or urgencies, considered for prioritization:

Table 7-1 Operator Response Times

Response Name	Time to Respond
Immediate	< 15 minutes
Rapid	Within a shift
Prompt	Response greater than a shift
Not Urgent	Response greater than a day

7.5 Cause, Confirmation, and Operator Corrective Action

Documenting the information related to an alarm is an important part of the documentation and rationalization process. It provides a record for review, audit, and analysis when compared to actual abnormal conditions and real-world responses. It can also be used as a guide for operators-in-training, or during process upsets.

The first section to document is the cause of the alarm. This is the mostly likely reason(s) that an alarm may be generated (e.g. high-level caused by a valve that failed to close).

Second, document the legitimate values, signals, or other items that would confirm the indication of the alarm (e.g. high-level switch, analog level transmitter, valve position, or other).

Lastly, document the recommended corrective action for the likely cause of the alarm (e.g. close the manual isolation valve upstream of the control valve).

All of this information, along with any other comments, shall be documented in the MADB during rationalization.

7.6 Alarm Priority Determination

Alarm priorities help the operator determine which alarm they should respond to first. Prioritizing alarms following a consistent methodology based on potential consequences and time to respond helps build confidence and trust in the alarm system. It also helps to optimize response during upset conditions so that they are always responding to the situation which is most critical to the organization.

7.6.1 Alarm Priorities

There will be four alarm priorities utilized in the SCADA system:

- Priority 1 – Critical
- Priority 2 – High
- Priority 3 – Medium
- Priority 4 – Low

Within the InTouch system Alarms will be configured as the following to reflect the alarm priority:

- 100 = Priority 1 – Critical
- 200 = Priority 2 – High
- 300 = Priority 3 – Medium
- 400 = Priority 4 – Low

7.6.2 Prioritization Methodology

Alarms will be prioritized based on a matrix of potential consequences and time to respond. By determining the consequences and the time to respond, the rationalization team will have an initial recommendation that can be consistently applied.

To perform the rationalization process, the consequences of action would be reviewed and assigned for all impact areas. From those, the highest category would be used (e.g. an alarm for a severe injury hazard but no other impacts would be a Major consequence). Next, an appropriate operator urgency would be assigned based on the process dynamics, organizational policy, compliance requirement, or other factor (e.g. EH&S should be notified immediately for a severe injury). The intersection of the highest consequence category column and the operator urgency row is the recommended alarm priority (e.g. High Priority Alarm). The prioritization matrix is presented below.

Table 7-2 Prioritization Matrix

Consequences of Actions				
Impact Area	**None**	**Minor**	**Major**	**Severe**
Personnel Safety	None	Minor or no injury, No lost time	One or more severe injury(s)	Fatality or permanently disabling injury
Environmental	None	Incidental release not requiring notification	Minor release resulting in agency notification, permit violation, or fine	Significant release affecting larger community
Water Quality	None	Minor off-spec, within compliance	Compliance limit affecting operability	Compliance limit exceeded, plant shutdown, or boil order
Equipment & Process	None	Impact to individual unit, <$10,000	Impact to multiple units, $10,000 to <$50,000	Impact to large portions of the water system, >$50,000
Operator Urgency				
Not Urgent	No Alarm	Consider revising the alarm for urgency		
Prompt	No Alarm	Low	Low	Medium
Rapid	No Alarm	Low	Medium	High
Immediate	No Alarm	Medium	High	Critical

A prioritization recommendation from the matrix may be overridden based on the experience of the rationalization team, organizational requirements, or other reasons. The final priority decision will be captured in the MADB.

7.6.3 Alarm Priority Distribution

The distribution of annunciated alarm priorities can be used to show the effectiveness of rationalization decisions and the overall alarm system. The ISA 18.2 provides example targets for annunciated alarm distributions for systems with three and four alarm priorities based on human-factors. Only critical alarms will be configured to be called out via the WIN-911 alarm system.

Based on those recommendations, the following priority distribution target will be used:

- Critical < 1%
- High ~ 5%
- Medium ~ 15%
- Low ~ 80%

Should the priority distribution vary greatly from this target, a review of the prioritization matrix and the rationalization decisions may be required.

7.7 Alarm Setpoint Selection

Alarm setpoint selection is an Engineering, Operations, and Maintenance task to be undertaken during rationalization. The specific details for each alarm are to be reviewed by the rationalization team. It should also be understood that some alarms may be set during the manufacturing process with minimal ability to change the alarm setpoint (i.e. a high-pressure switch set from an equipment manufacturer).

In general, select a setpoint that is: far enough away from the consequence threshold to allow an operator adequate time to respond, and not too close to the normal operating range that alarms are triggered because of normal fluctuations.

The experience of the rationalization team should be utilized to determine process dynamics (e.g. rate of change, process variability, signal delays, and other relevant data) along with reasonable thresholds based on past operating experience.

7.8 Alarm Classification and Management of Requirements

Alarm classification is a method of grouping alarms with similar administrative requirements for testing, training, data retention, management of change, and shelving. Each alarm must be assigned to a class per ISA 18.2, during rationalization. After implementation the system will be evaluated, and alarm classes may be implemented.

Alarm Classes can be configured as Alarm Groups. These groups should assist the operator in identifying the alarm and understanding its impact to safety or the treatment process.

7.9 Alarm Documentation and the Master Alarm Database

Alarms will be documented during the rationalization stage in the MADB. The information to include in the MADB is:

- control system tag / reference
- alarm type
- alarm priority
- alarm classification
- alarm comment
- alarm setpoint
- alarm on-delay
- alarm off-delay
- alarm deadband

- potential cause of the alarm
- consequence of inaction
- potential corrective action
- time available to respond
- need for advanced alarm handling

The MADB will be developed and maintained by Support Services. Support Services will start development of the MADB with only critical alarms. Once these are successfully documented, Support Services will transition to adding the remainder of the alarm system.

Projects that will add any new alarms to the SCADA system will be required to submit alarm documentation. This will ensure that the alarms are properly identified, rationalized, and prioritized before implementation.

8 ALARM DESIGN

Alarm design covered in this section relates to the design and configuration of individual process variables and the selection of appropriate alarm types within the Process Control System. See Appendix B for details on alarms associated with each different type of equipment.

The SCADA HMI design component is covered in Section 9.

Basic alarm design is an important foundational component of a well maintained and efficient alarm system. Per ISA 18.2:

> *"Poor design and configuration practices are a leading cause of alarm management issues. It has been found that a large percentage of alarms generated during alarm floods and during steady state operation are from nuisance alarms which have been configured improperly."*

8.1 Application of Alarm Types

One of the keys to creating an effective alarm system is to ensure that the most appropriate alarm type is selected to detect and annunciate each abnormal condition that requires operator response. When selecting alarm types, it is also important to be consistent in the treatment of common pieces of equipment (e.g. fail-to-start alarms for pumps) or types of control (e.g. PID, Lead-Lag). This will improve the operator's ability to determine what is happening during an abnormal situation and will increase the probability of a correct response.

Table 8-1 defines the basic alarm types to be utilized in designing alarms.

Table 8-1 Alarm Types

Alarm Type Group	Detailed Alarm Type (used in SCADA)	Example Alarms
Absolute	Discrete Value HiHi Value Hi Value Lo Value LoLo	Temperature Switch High Level High Flow Low
Deviation	DeviationMinor DeviationMajor	Flow Deviation Level Deviation
Rate-of-Change	ROC Lo ROC Hi	Level Rate-of-Change High

Alarm Type Group	Detailed Alarm Type (used in SCADA)	Example Alarms
Discrepancy	Discrete	Pump Fail-to-Start Pump Fail-to-Stop Valve Full-Stall Valve Transit-Stall
System Diagnostic	System Software	Server Fail Communications Fail
Instrument Diagnostic	Discrete	Instrument Fail Bad PV

8.2 Application of Alarm Deadband

Alarm deadband is a function used to reduce the number of times an alarm triggers for a given abnormal condition, which ideally would be only once. It prevents an alarm from returning to normal until the process variable has moved outside the deadband. Without deadband, or another function like time delay, signal or process noise can cause an alarm to trigger and clear repeatedly. Alarm deadband can be used to address the common alarm problem of chattering alarms, which is a type of nuisance alarm.

If misapplied, alarm deadband can also prevent an alarm from returning to normal when the process state is normal, causing another common alarm problem; stale alarms.

There are several factors that should be considered when determining the setting for alarm deadband including:

- Operating range
- Measurement type
- Signal noise
- Other alarm setpoints

When configured in the PLC (preferred), alarm deadband is available to be set independently for absolute alarm types (e.g. high, low, etc.).

When configured in the SCADA system, a single deadband is utilized for all absolute alarms.

When determining deadband it is important to take special consideration for determining the operating range. The operating range is the full range in which the process variable may operate. This may be considerably different than the configured range of the instrument. For instance, a pumps operating range may be 0-100 PSI, but the instrument may be configured for 0-500 PSI from the factory. Determining a deadband from the configured range would potentially lead to stale alarms.

8.3 Application of On & Off Delay

There are two types of delay functionality associated with alarms. These are on-delay and off-delay. These work differently and have significantly different implications when used. These settings are used to reduce chattering and fleeting alarms.

The on-delay prevents the initial annunciation of an alarm for a specified number of seconds. If the alarm clears during the time, it is never annunciated at all. The off-delay immediately annunciates an alarm, but when the alarm clears, the cleared condition is not put into effect for the specified number of seconds. If the alarm re-occurs during that interval, the cleared condition is never made known and the alarm simply persists.

The correct application of on-delays and off-delays can be very effective in reducing the number of fleeting and chattering alarms. Reducing these types of alarms can prevent most types of nuisance alarms.

On-delays may be effective against both fleeting and chattering alarms. Off-delays may be only effective against chattering alarms, but do not reduce fleeting alarms.

On and off delays should be applied after proper consideration for deadband.

Proper engineering judgment should be employed when setting on and off delays in order to minimize nuisance alarms while maintaining process vigilance and equipment or personnel safety.

8.3.1 Control System Diagnostic Alarms

This type of alarm is used to indicate that a fault has occurred in the control system hardware, software, or components (e.g. communications failure, server failure, application error, rack fault). The control system diagnostic alarms are built-in by the manufacturer for most components and are not generally subject to change. Due to the nature of these alarms, most require a communications technician or a maintenance engineer to diagnose and fix.

Control system alarms should be carefully rationalized based on the overall list of effected equipment, the level of redundancy at the site and system level, and the operator's ability to separately confirm signals and data from other sources.

During rationalization, it should be made very clear which system diagnostic alarms require immediate resolution compared to those that can be handled on a scheduled basis.

9 ALARM SCADA INTERFACE

All alarms are displayed in the control room on HMI displays. Process displays contain alarm indicators. The HMI program will also contain Alarm Banners, an Alarm Summary and Alarm History Displays.

Process display alarms should be displayed utilizing shape, color, and number indicators. This will ensure the alarm condition and severity are easily identified.

9.1 Alarm Summary Display Characteristics and Usage

The alarm summary provides a list of active alarms within the alarm system. The alarm summary display lists only alarm information. The display provides the following information for each alarm:

- Name and Description of the tag in alarm
- Alarm State (Including Acknowledged Status)
- Alarm Priority
- Time/Date the alarm became active
- Alarm Type
- Process Value
- Alarm Setpoint
- Process Area
- Alarm Comment

Table 9-1 Alarm Summary Configuration

Color	Animation	Style	Object/Element Condition
Gray	***None***		Display background
Dark Gray	***None***	***Thin***	Grid
Red	***Flash Shade***	***Bold***	Critical alarm, unacknowledged text
Red	***None***	***Normal***	Critical alarm, acknowledged text
Dark Blue	***None***	***Bold***	High alarm, unacknowledged text
Black	***None***	***Normal***	High alarm, acknowledged text
Dark Blue	***None***	***Bold***	Medium alarm, unacknowledged text
Black	***None***	***Normal***	Medium alarm, acknowledged text
Dark Blue	***None***	***Bold***	Low alarm, unacknowledged text
Black	***None***	***Normal***	Low alarm, acknowledged text
Black	***None***	***Normal***	Return to normal text

Time	Comment	Status	Priority	Type	Value	Setpoint	Name
DD/MM/YYYY	Short Description of the Alarm	UNACK_ALM	100	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	ACK_ALM	100	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_RTN	100	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_ALM	200	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	ACK_ALM	200	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_RTN	200	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_ALM	300	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	ACK_ALM	300	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_RTN	300	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_ALM	400	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	ACK_ALM	400	DSC	###.##	###.##	Tagname
DD/MM/YYYY	Short Description of the Alarm	UNACK_RTN	400	DSC	###.##	###.##	Tagname

Figure 9-1 Alarm Summary

9.2 Alarm Indications within SCADA Displays

Alarm colors and symbols are the most important graphical objects on the HMI, and therefore, use the brightest colors. Alarm symbols use a distinct shape, color, and text used only for alarm conditions in order to make them easily identifiable.

The alarms will be displayed to ensure easy recognition even if the operator is colorblind. Alarm symbols will be placed next to the instrument or equipment that the alarm represents. The symbol should stand out from the display background and draw the operator's attention to the instrument or equipment in alarm. Red, Yellow, Magenta and Cyan should only be used to identify alarms on the HMI display. Table 9-2 identifies the alarm symbol characteristics.

Table 9-2 Alarm Indication Matrix

Severity	Color	Shape	Animation
Critical	Red	Diamond	Flash
High	Yellow	Up Triangle	None
Medium	Magenta	Down Triangle	None
Low	Cyan	Square	None

Level 1 alarm conditions represent critical alarms that need immediate action. Level 1 alarm conditions are represented by a bright red diamond with the number one inset (Figure 5):

Figure 9-2 Level 1 Alarm Symbol

Level 2 alarm conditions represent high alarms that need rapid action. Level 2 alarm conditions are represented by a yellow up triangle with the number two inset (Figure 6):

Figure 9-3 Level 2 Alarm Symbol

Level 3 alarm conditions represent medium alarms that need operator action. Level 3 alarm conditions are represented by a magenta down triangle with the number three inset (Figure 7):

Figure 9-4 Level 3 Alarm Symbol

Level 4 alarm conditions represent low priority alarms that do not need immediate action. Level 4 alarm conditions are represented by a cyan square with the number four inset (Figure 8):

Figure 9-5 Level 4 Alarm Symbol

9.3 Navigation and Alarm Response

New systems or HMI upgrades will utilize a navigation banner either at the top or bottom of the HMI display. This navigation banner should organize the displays into a logical process flow of the plant. Each process area should have a navigation selection. When a during a critical alarm condition, the appropriate process navigation section containing the alarm will flash red. This ensures the operator will be notified of the alarm and will be able to easily navigate to the process display containing the alarm condition.

Figure 9-6 Alarm Navigation

9.4 External Annunciators

WIN-911 is the alarm and event notification software that connects to Wonderware. This software provides real-time alarm notification to numerous telecommunications devices. This software vocalizes alarms over intercom systems, radios and telephones and can send alphanumeric text messages and email.

Only Critical priority 1 alarms are configured in WIN-911. WIN-911 will be configured to provide notification when control room operators are not present.

10 ALARM SYSTEM IMPLEMENTATION, OPERATION, AND MAINTENANCE

The stages of implementation, operation, and maintenance cover the transition between alarm design and everyday use. The associated functions include training, testing, and control of the alarm suppression.

10.1 Alarm Commissioning Practices

During commissioning, the system designer (i.e. the Process Control System Engineer and/or the Design Engineer) shall ensure that alarm settings defined in the alarm database are implemented and that the design is consistent with the Alarm Standards document.

Prior to putting the alarm system into service, it shall be installed, inspected, and tested to ensure that it operates correctly. For new sites or systems, this should be performed during contract and site required commissioning. For new alarms added to existing facilities, the commissioning requirements shall be determined as part of the management of change process.

During commissioning, the response time of the operator shall be confirmed for all critical alarms and any process alarms that are deemed sufficiently significant.

10.2 Alarm System Testing

Routine testing of alarm detection (instruments) and presentation (annunciators and computer displays) shall be performed to assure the reliability of the alarm system. The testing frequency and requirements for alarms are dictated based on alarm criticality. Test criteria shall be clearly documented to show what is considered a passed test (with suitable tolerances). All test results shall be recorded, and all failures shall be explained with a documented strategy or plan for rectification and re-testing.

Alarm testing shall include:

- Verification of the alarm limit or logical condition
- Verification of the alarm priority
- Verification of the audible and visual indications for the alarm
- Verification of any other functional requirement for the alarm as specified
- Requirements based on alarm classification
- Requirements based on management of change policies
- Point-to-Point check (loop or function check) as required

During testing, alarm configuration (e.g., alarm setpoint and priority) should be verified against the MADB.

Testing should be performed by driving the alarmed process variable into the alarm state. This is especially appropriate for flow and level alarms. Alarms shall not be tested by altering the alarm setting; this does not confirm that the instrument can achieve the appropriate output. Smart devices shall also not be tested by artificially overwriting the instrument output.

Any modifications to the alarm as a result of successful or unsuccessful testing shall be performed in accordance with the appropriate change management and updated in the MADB.

All overrides (bypasses) put in place to maintain or test alarms shall be suitably controlled and removed as soon as servicing or testing is complete.

The testing of the overall alarm system in SCADA shall be performed yearly. High sump alarms will be tested semi-annually. Alarm system testing should include:

- The audible and visual indications for each alarm priority
- The HMI features, such as alarm messages displayed in the alarm summary
- The methods for removing an alarm from service
- The methods of alarm filtering, sorting, linking of alarms to process displays
- Requirements based on management of change policy

10.3 Maintenance

Regular maintenance is vital to ensure the performance of the alarm system does not degrade throughout the life of the equipment, building or system. Routine maintenance of all alarms shall be performed to ensure that they will activate as and when required.

Maintenance activities shall be determined by the maintenance. Maintenance activities will follow organizational goals and strategies, as well as, regulatory and compliance requirements.

10.4 Alarm Out-of-Service Procedure

If supported by the HMI and PLC, the operator may take an alarm out of service or suppress the alarm for an extended period using an authorization process. Alarms are typically taken out of service for repair. Out-of-service requirements for alarms shall be determined by the classification of the alarm and the class (or group) requirements as specified in this alarm management standard.

Alarms that will be compromised for extended durations shall be examined to determine whether an alternative alarm is necessary. If an interim alarm is necessary, it shall adhere to the alarm class and Maintenance of change (MOC) requirements.

Maintenance personnel will notify operators before taking the equipment out of service. This procedure will be documented in the Lock-Out-Tag-Out form. Before returning out-of-service alarms to the operational state, operators shall be notified to ensure they are aware of the returning alarm and the removal of the interim methods.

A list of all out-of-service alarms should be readily available to the operator at all times. The operator should review the list at shift handover.

10.5 Alarm System Training

An effective alarm system requires that the operator know the correct action to take in response to each alarm. Training should cover all realistic operational usage of the alarm system and address not only the system functionality and features but also the principles of the process to ensure a full understanding of 'why' as well as 'what' may happen. Initial training should be conducted prior to placing the alarm in service. Regular refresher training and re-assessment shall be conducted on an appropriate frequency (depending on the alarm's classification).

Operator training on the alarm system shall include the following at a minimum:

- the audible and visual indications for alarms,
- the distinction of alarm priorities,
- the use of the alarm HMI features (e.g., alarm summary sorting and filtering),
- the use of alarm response procedures (if available),
- the approved methods for shelving and suppression,
- the use of advanced alarming applications,
- the approved methods for removing an alarm from service,
- the approved methods for returning an alarm to service,
- the approved procedure for management of change.

For a new, or modified, alarm the operator shall be trained on the following items as documented in the MADB:

- Likely causes of the alarm
- Worst credible consequences of not responding to the alarm
- Time to respond to the alarm (e.g. time available to respond and time required to respond)
- Recommended actions to take in response to the alarm
- Information used to confirm the alarm is valid
- Alarm setpoint
- Alarm priority
- Any advanced alarm handling performed on the alarm

Where the responses to alarms are unfamiliar to the operators, then these shall be practiced (wherever practical) before the alarm system is put into service.

10.6 Alarm Response Procedures

For critical alarms, an alarm response procedure shall be developed. Use of alarm response procedures can reduce the time it takes the operator to diagnose the problem and determine the appropriate corrective action, as well as, promote consistency between operators. Responses shall be clear and concise and should reflect the operator's perspective of the process, and not use technical jargon. These procedures will highlight the following information:

- the alarm type,
- alarm setpoint,
- potential causes,
- consequence(s) of inaction,
- corrective action(s),
- method of confirmation that the alarm is genuine,

- allowable response time,
- alarm priority.

Operators shall participate in developing responses to alarms to ensure that the responses are understandable and achievable within the physical and time constraints of the process.

11 ALARM SYSTEM PERFORMANCE MONITORING, ASSESSMENT, AND AUDITS

The inclusion of monitoring, assessment, and audits in the alarm standard is a requirement of ISA 18.2. They are essential to achieving and maintaining the stated objectives of the alarm system. These overall activities will identify areas of improvement in the alarm management lifecycle, as well as, the process control and water system.

11.1 Alarm System Key Performance Indicators (KPIs)

Alarm system key performance indicators (KPIs) are the few metrics that indicate overall performance of the alarm system. These document the broad indicators of alarm system performance to management, which can be compared to operational performance goals.

Diagnostic metrics should be utilized as an assessment tool to pinpoint problem alarms for further rationalization, and/or modification. The following diagnostic metrics will be used for analysis:

- Listing and quantity of the most frequent alarms
- Listing and quantity of fleeting alarms
- Listing of standing alarms
- Other reports as necessary

11.2 Alarm Performance Reporting

Alarm reporting provides the feedback mechanism for continuous monitoring and assessment that leads to overall system improvement. This should not be considered an ad-hoc process. In order for the alarm management program to be successful, these activities must be performed regularly to baseline, track, and improve.

11.2.1 Average Alarm Rate Per 10 Minutes

The alarm rate per 10-minute interval, measured for each operator position, provides a reasonable measure of alarm rate relative to operator capability. It also provides some detail regarding time periods where the operator may be overloaded.

The average alarm rate per 10 minutes is a general measure of performance. Additional measures are generated from this calculation.

11.2.2 Alarm Flood Analysis

The rate of handling 10 or more alarms in 10 minutes cannot generally be sustained by an operator for long periods of time. This condition is considered an alarm flood. In a flood period the alarm system can become a hindrance or a distraction, rather than acting as a useful tool to assist the operator. During such floods, alarms are likely to be missed.

For calculations, a single alarm flood event is defined as beginning when the alarm rate exceeds 10 or more alarms occurring in 10 minutes and ending when the rate drops below 5 alarms in 10 minutes. Flood events should be analyzed for the following:

- Total percentage of time the alarm system spends in a flood condition (KPI).

- Overall number of floods per day and week.
- Total duration of each flood event.
- Flood severity, by measuring the average and peak alarm rate during the flood event.

11.2.3 Alarm Out-of-Service

If available, placing an alarm out-of-service is useful during known process states to prevent nuisance alarms from shutdown, or non-operational equipment. It is important for Operations to regularly review out-of-service alarms to ensure that alarms are not disabled once the equipment is returned to service.

The alarm out-of-service report shall provide a listing of all alarms that have been disabled. This information shall be available as a summary display for operators in the SCADA system.

11.2.4 Alarm Priority Distribution

The purpose of alarm priority is to help the operator quickly differentiate the relative importance of alarms. For higher priorities to be effective, their occurrence count should be small compared to the lowest given priority.

The alarm priority distribution report shall provide a percentage breakdown of annunciated alarms by priority.

11.2.5 Standing Alarms

Standing, or stale, alarms are annunciated to the operator and remain in the alarm state continuously for a substantial time period, such as several days or weeks. Following their initial appearance, such alarms provide little valuable information to the operators.

Standing alarm reports shall consist of a list of all alarms that have been in constant alarm for more than 5 days. The report shall include the alarm duration.

11.2.6 Frequently Occurring Alarms

A relative few alarms often produce a large percentage of the total system alarm load. Given a time period of several weeks, the alarms shall be ranked from the most frequent to the least frequent. Often, the top 10 alarms represent 20% to 80% of the alarms. Substantial improvement can be realized by addressing most frequent alarms.

Frequent alarms reports shall include a list of the top 10 alarms ranked from the most frequent to the least frequent with an associated percentage.

11.2.7 Fleeting Alarms List

Fleeting alarms transition into and out of the alarm state in a short amount of time. The time and rate of transition are too fast to result from operator corrective action, thus violating a fundamental principle of proper alarm management. Review of basic alarm design principles are generally required to fix chattering alarms.

The fleeting alarms reports shall include a listing of the top 10 fleeting alarms ranked from the most frequent to the least frequent.

11.3 Record / History Preservation

Alarm and Events records are stored with process data in SCADA using History Blocks and/or SQL tables. This data shall be stored for a minimum of 24 months in the online Historian. Additional History Blocks can be stored offline and recalled as necessary for further analysis.

11.4 Alarm Audits

Audits of the alarm system shall be conducted annually. The audit shall cover a review of the documentation that demonstrates the work processes in the alarm standard have been followed and that the objectives of the alarm standard have been met.

The alarm audit shall be conducted by an audit team, including:

- Alarm System Owner (Operations)
- SCADA Analyst (Support Services)
- Operations Superintendent (As applicable for Operations, Treatment, etc.)

During an alarm audit, the following materials shall be available:

- Alarm Standard
- MADB
- Alarm monitoring reports
- Alarm and Events history
- MOC documents
- Test records for alarms requiring periodic testing
- Training records for operators
- Any relevant incident investigation forms

The following checklist items shall be covered in the audit:

- ✓ Alarms occur only for conditions requiring operator action
- ✓ Alarm attributes match the MADB
- ✓ Alarms are documented, and the documentation is available
- ✓ Alarm priority is consistently applied
- ✓ Alarms allow sufficient time for the operator to respond
- ✓ Alarm attribute changes are authorized through the MOC process
- ✓ Alarm performance is being monitored
- ✓ Training is provided on the alarm system and standard
- ✓ Practices are compared to industry guidelines
- ✓ Action items and lessons learned from past audits are reviewed and addressed

The audit team may additionally utilize an interview process to assess audit items with key individuals.

Audit findings should be documented as a summary report with action items.

12 ALARM SYSTEM MANAGEMENT OF CHANGE (MOC)

Management of change is a separate stage of the lifecycle covered in Clause 17 of ISA-18.2. Within the MOC process, changes relating to: new alarms, removal of alarms, alarm attribute modifications, alarm system functions, authorization procedures, and documentation are covered. The purpose of MOC is to ensure that changes are authorized and subjected to evaluation criteria described in the alarm standard.

Quarterly Alarm Management Meetings will occur. These meetings will be held to discuss the alarm audit findings and procedures, temporary changes to alarms, permanent changes to alarms, and changes to the master alarm database. Any changes in alarm management will be documented and recorded in the Master Alarm Database. This database shall be maintained by Support Services. Notification of changes will be distributed to operations, maintenance, and support staff after each meeting.

12.1 MOC Applicability

The MOC procedure will be broken into three applicable levels based on the alarm class and scope of the change.

Table 12-1 MOC Types

MOC Level	Description
Formal MOC	• Full review team • Complete MOC documentation • Log of Change • Training (as determined with Operations) • E-mail notification to all parties
Informal MOC	• Smaller review team • Complete MOC documentation • Log of Change • Informal training (e.g. e-mail, conversation) • E-mail notification to affected parties
Change Log	• Minimal review required • Log of Change • Training not required • Notification not required

12.2 MOC Methodology

The MOC procedure has multiple levels to enable an efficient process for both minor and major changes, while maintaining authorization levels that are appropriate to the requested change.

12.2.1 Formal MOC

A Formal MOC is required for:

- New alarms
- Removed alarms
- Alarms part of a class that require a Formal MOC (e.g. Safety)
- For specific changes that relate to rationalization criteria
  The Formal MOC requires complete documentation of the MOC form with full review and authorization.

  The following individuals must provide authorization for a Formal MOC:

- Sr Operator or Planner/Scheduler (Review)
- Process Control System Engineer, or SCADA Analyst (Review)
- ME Automation Supervisor (Authorizer)
- Operations Superintendent (Authorizer)
- Maintenance Supervisor (Authorizer)
- EH&S Representative (Authorizer for Safety/Environmental Classes)

12.2.2 Informal MOC

An Informal MOC is required for:

- Setpoint changes

- On/Off – Delay changes
- Deadband changes
- Advanced alarming changes

The Informal MOC requires complete documentation of the Lockout Tagout form with review and authorization.

The following individuals must provide authorization for an Informal MOC:

- Sr Operator or Planner/Scheduler (Review)
- Process Control System Engineer, or SCADA Analyst (Review)
- ME Automation Supervisor (Authorizer)
- Operations Superintendent (Authorizer)

12.3 MOC Requirements

A Formal or Informal MOC requires the following information:

- The technical basis for the proposed change
- The impact of the change on safety, compliance, and the environment
- The modifications are in accordance with the alarm standard
- The requirements for modifying operating procedures
- The time period for which the change is valid (e.g. temporary or permanent)
- Other authorization requirements above those required by the MOC (i.e. required by PSM, NDEP)
- Changes to the alarm system in SCADA (e.g. display or indication changes)
- Implementation testing and training requirements
- The reference documentation required for review (e.g. manuals, displays, logic, P&IDs)

APPENDIX A ALARM RATIONALIZATION PROCESS

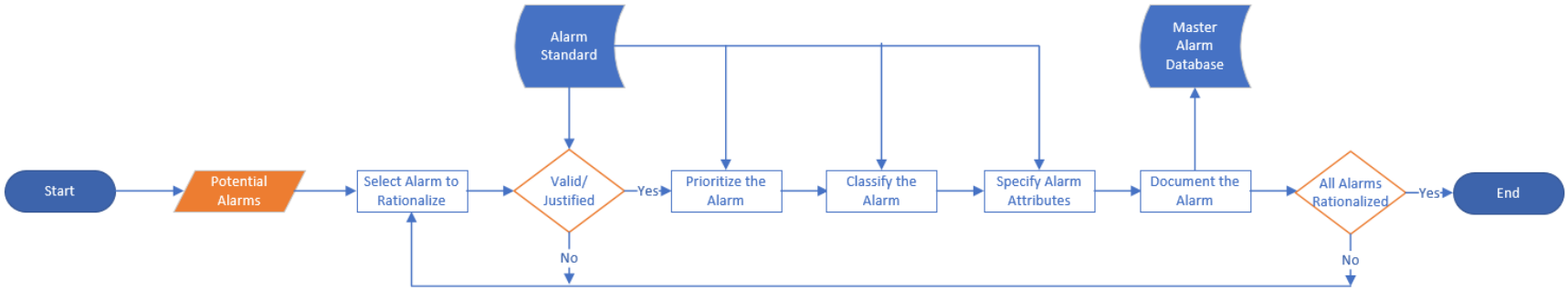

Figure A-1 Rationalization Process

APPENDIX B ALARM STANDARDS

B1 ACTUATOR (ISOLATING)

B1.1 Introduction

The City of Tulsa wastewater treatment process uses Isolating (Open/Close) valve/gate actuators. Isolating valves are designed to operate in either Full Open or Full Closed position. The actuators are typically electrically motorized but can be pneumatically powered as well. The actuator unit is coupled to the valve or gate via a stem that can vary in length. The type of coupling results in two basic types of valve/gate movement: Quarter-turn (90 deg.) or multiturn. Either style can be isolating or modulating and depends on the application. However, multiturn is commonly used for gates in open channel flow applications, while quarter-turn is used for valves (e.g. butterfly) for in-line piping applications.

The actuator is self-contained and comes with the required electrical motor and controls housed in a NEMA rated enclosure. The NEMA rating is determined by the application and the engineer should determine this during the design. The motorized actuator uses a reversing motor starter (FVR) and has all other electronic components to operate in the isolating mode. The actuator has limit switches (dry-contact) that are setup to indicate the valve/gate is either Full Open or Full Closed and these are wired to the SCADA system to provide position feedback. A separate set of limit switches are also interlocked internally with the motor starter to de-energize it once the Full Open or Full Closed position is reached.

The actuator has a local control station integral to the actuator as standard, but the control station can be ordered for remote mounting from the manufacturer when the actuator is not readily accessible. The engineer should determine this during design and specify it accordingly. These controls allow selection between Local or Remote control via the SCADA system. Local mode allows manual control to Open/Close/Stop the valve/gate using the pushbuttons or switches on the control station. Additionally, most actuators come with a mechanical override lever and handwheel. The mechanical override lever disengages the motor and allows the operator to use the handwheel to turn the stem directly to position the valve/gate. When the size/weight of the valve/gate is large as with some gates, a separate handheld motorized device is used to turn the valve stem. This is typically used on multiturn actuators where a handwheel would have to be turned many, many times to position the valve/gate.

Based on these differing installation types, there are several decisions that a designer will need to make in determining how to protect this equipment. Several of these decisions involve field instrumentation and if/when to provide specific wiring in the starter controls to monitor and act based on the imbedded instruments.

B1.2 Standard Actuator Alarm Design

An engineer shall design an alarm system that will protect the actuator and valve/gate. This alarm system shall contain, at a minimum, the alarms listed below in Table B1-1. The alarm system consists of hardwired actuator controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B1.3 Hardwire Alarms

In lieu of discrete hardwired alarms, actuators today use network connections (Ethernet, Profibus, etc.) to communicate status to the PLC. The first is the “Valve Torque Overload” alarm which senses the torque as the valve/gate is moved. Torque values can be high during seating the valve when closing or unseating the valve when opening. The torque alarm limit value is typically recommended by the manufacturer to prevent over-torque from damaging the seat and other components.

Second, the actuator monitors itself for motor and internal faults and generates an “Actuator Failure” alarm. This is a common alarm that will as a minimum include any internal alarms that shut down the actuator or is deemed critical to the operation of it outside of the Torque alarm. This monitoring shall include motor current overloads, motor winding temperature and internal electronics failure. Refer to the manufacturer’s information for details on what is included in the Fault Alarm.

Another alarm is the “Valve Not in Remote”. Since the valve/gate is normally controlled via the PLC, if the switch at the actuator local control station is not in the Remote position this alarm is generated.

B1.4 Software Alarms

There are alarms associated with the operational sequence of the actuator. A “Valve Fail to Open” alarm is generated when a valve/gate is commanded to move via the SCADA system and the valve/gate does not reach that position within the specified time period. Similarly, a “Fail to Close” alarm is generated when a valve/gate is commanded to close via the SCADA system, and it does not reach that position within the specified time period.

Another software alarm is “Valve Limit Fail”. It is generated if both the Full Open and the Full Closed limit switch inputs are received at the PLC simultaneously for a set time period. This alarm indicates a potential wiring problem or malfunction with the actuator.

The actuator communication connection is monitored and a “Communications Failure “alarm is generated when network communications (e.g. Ethernet) is disrupted for a short time period between the actuator and the PLC. Typically, a “Watch-dog” timer is programmed in the PLC which the equipment periodically resets to ensure that communications is operational. If the comms link is down and the watch-dog timer times out an alarm is generated.

Also, operators have the option via the HMI graphic to place a valve/gate “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the valve icon and the valve does not operate in remote modes. Furthermore, putting a valve out of service disables all alarms associated with that valve. Putting a valve out of service does not issue an alarm.

Table B1-2 Actuator Minimum Alarms

IO Type	Description	Delay	Priority
Ethernet	Valve Torque Overload	5 seconds	300
Ethernet	Actuator Failure	5 seconds	300
Ethernet	Valve Not in Remote	5 seconds	400
PLC	Valve Fail to Open	90 seconds	300
PLC	Valve Fail to Close	90 seconds	300
PLC	Valve Limit Fail	90 seconds	300
Ethernet	Communications Failure	5 seconds	200

B1.5 Specialty Actuator Alarm Design

None

B2 ACTUATOR (THROTTLING)

B2.1 Introduction

The City of Tulsa wastewater treatment process uses Throttling (Modulating) the valve/gate actuators. Throttling actuators are designed to operate valve/gates from 0 to 100% open. The actuators are typically electrically motorized but can be pneumatically powered as well. The actuator unit is coupled to the valve or gate via a stem that can vary in length. The type of coupling results in two basic types of valve/gate movement: Quarter-turn (90 deg.) or multiturn. Either style can be isolating or modulating and depends on the application. However, multiturn is commonly used for gates in open channel flow applications, while quarter-turn is used for valves (e.g. butterfly) for in-line piping applications.

The actuator is self-contained and comes with the required electrical motor and controls housed in a NEMA rated enclosure. The NEMA rating is determined by the application and the engineer should determine this during the design. A motorized actuator contains a reversing variable frequency drive and all other electronic components to operate in the modulating mode. Each actuator has limit switches (dry-contact) and/or position feedback system (analog – 4-20mA) that are wired to the SCADA system to provide position feedback of the gate/valve.

The actuator has a local control station integral to the actuator as standard, but the control station can be ordered for remote mounting from the manufacturer when the actuator is not readily accessible. The engineer should determine this during design and specify it accordingly. These controls allow selection between Local or Remote control via the SCADA system. Local mode allows manual control to Open/Close/Stop the valve/gate using the pushbuttons or switches on the control station. Additionally, most actuators come with a mechanical override lever and handwheel. The mechanical override lever disengages the motor and allows the operator to use the handwheel to turn the stem directly to position the valve/gate. When the size/weight of the valve/gate is large as with some gates, a separate handheld motorized device is used to turn the valve stem. This is typically used on multiturn actuators where a handwheel would have to be turned many, many times to position the valve/gate.

Based on these differing installation types, there are several decisions that a designer will need to make in determining how to protect this equipment. Several of these decisions involve field instrumentation and if/when to provide specific wiring in the starter controls to monitor and act based on the imbedded instruments.

B2.2 Standard Actuator Alarm Design

An engineer shall design an alarm system that will protect the actuator and valve/gate. This alarm system shall contain, at a minimum, the alarms listed below in Table B2-1. The alarm system consists of hardwired actuator controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B2.2.1 Hardwire Alarms

In lieu of discrete hardwired alarms, actuators today use network connections (Ethernet, Profibus, etc.) to communicate status to the PLC. The first is the “Valve Torque Overload” alarm which senses the torque as the valve/gate is moved. Torque values can be high during seating the valve when closing or unseating the valve when opening. The torque alarm limit value is typically recommended by the manufacturer to prevent over-torque from damaging the seat and other components.

Second, the actuator monitors itself for motor and internal faults and generates an “Valve Failure” alarm. This is a common alarm that will as a minimum include any internal alarms that shut down the actuator or is deemed critical to the operation of it outside of the Torque alarm. This monitoring shall include motor

current overloads, motor winding temperature and internal electronics failure. Refer to the manufacturer's information for details on what is included in the Fault Alarm.

Another valve alarm is the "Valve Not in Remote". Since the valve/gate is normally controlled via the PLC, if the switch at the actuator local control station is not in the Remote position this alarm is generated.

B2.2.2 Software Alarms

There are alarms associated with the operational sequence of the actuator. A "Valve Position Fail" alarm is generated when a valve/gate is commanded to move via the SCADA system and the valve/gate does not reach that position within a specified time period. For modulating valve/gates the commanded % Open (0-100%) is not reached within a Deadband limit (default is 5%) within the time period.

A second software alarm is "Valve Limit Fail". It is generated if both the Full Open and the Full Closed limit switch inputs are received at the PLC simultaneously. This alarm indicates a potential wiring problem or malfunction with the actuator.

Also, operators have the option via the HMI graphic to place a valve/gate "Out-of-Service". A visual "OOS" tag appears on the HMI graphic next to the valve icon and the valve does not operate in remote modes. Furthermore, putting a valve out of service disables all alarms associated with that valve. Putting a valve out of service does not issue an alarm.

Table B2-3 Actuator Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Valve Torque Overload	5 seconds	300
IO Discrete	Valve Failure	5 seconds	300
IO Discrete	Valve Not in Remote	5 seconds	400
PLC	Valve Position Fail	60 seconds	400
PLC	Valve Limit Fail	90 seconds	300
Ethernet	Communications Failure	5 seconds	200

B2.3 Specialty Actuator Alarm Design

None

B3 CLARIFIER

B3.1 Introduction

For the City of Tulsa wastewater treatment process, each clarifier (Primary or Secondary) is designed to run continuously unless placed Out-of-Service. The clarifier separates the clean (clarified) water from sludge. The heavier sludge material collects on the bottom of the unit while the clarified water is separated and passed through using weirs that ring the clarifier along the water surface. Each clarifier has a drive/motor combination used to rotate the skimmer arm on the surface of the process liquid. The mechanical skimmer arm skims the surface of the process liquid to remove scum and other material from the surface and direct them into a scum pit sump. The sump level is monitored and is pumped down on high level. The drive/motor along with the local control panel are located on a walkway platform in the center of the unit. The skimmer arm's drive/motor is monitored for torque and alarms and is to shut down the clarifier on High Torque

B3.2 Standard Clarifier Alarm Design

An engineer shall design an alarm system that will protect the clarifier drive/motor combination. This alarm system shall contain, at a minimum the alarms listed below in Table B3-1 and include any other alarms as recommended by the manufacturer. The alarm system consists of hardwired starter controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B3.2.1 Hardwire Alarms

An Across-the-Line (ACL) motor starter is provided to turn on/off the clarifier as needed. Internal to the starter are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. A “Clarifier Overload Trip” input to the PLC from the overloads will turn off the clarifier and lock it out from starting and requires a manual Reset.

The Clarifier is also monitored for high torque loading with a couple of separate inputs. The first is the “Clarifier Torque Warning” which is a warning alarm that the torque level is exceeding the normal range and is typically set to 110% of rated torque. The second is the “Clarifier Torque Shutdown” which is a shutdown alarm that is wired to the motor starter and is set to 140% of rated torque. These torque ratings are adjustable and typically specified by the manufacturer.

Another clarifier alarm is the “Clarifier Not in Remote”. Since the clarifier is normally controlled via the PLC, if the Local-Off-Remote switch at the local control station is not in the Remote position this alarm is generated.

B3.2.2 Software Alarms

There are alarms associated with the operational sequence of the clarifier and are generated in the PLC. The positive running feedback is a contact from the associated starter for the motor. Since the clarifier is designed to run continuously, a “Clarifier Not Running” alarm is generated if the running status is not detected.

The “Clarifier Run Disable” alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

A “Clarifier Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. The designer must coordinate with the motor manufacturer to determine what maximum value this can be.

Another sequential alarm is issued when the clarifier does not start or stop based on commands from the SCADA system. If the SCADA systems requests the clarifier to either Start or Stop and a feedback input is not received, a “Clarifier Start-Stop Fail” alarm is generated.

Also, operators have the option via the HMI graphic to place a clarifier “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the clarifier icon and the clarifier does not operate in remote modes. Furthermore, putting a clarifier out of service disables all alarms associated with it. Putting a clarifier out of service does not issue an alarm.

Table B3-4 Clarifier Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Clarifier Overload Trip	5 seconds	300
IO Discrete	Clarifier Torque Warning	5 seconds	400

IO Discrete	Clarifier Torque Shutdown	5 seconds	300
IO Discrete	Clarifier Not in Remote	5 seconds	400
PLC	Clarifier Not Running	5 seconds	400
PLC	Clarifier Run Disable	0 seconds	200
PLC	Clarifier Starts Exceeded	5 seconds	300
PLC	Clarifier Start-Stop Fail	15 seconds	200

B3.3 Special Clarifier Alarm Design

Some Clarifiers have a mechanical Shear Pin protective device to protect against destructive high torque. The Shear Pin is designed to break if the torque exceeds a very high limit and will mechanically disengage the skimmer arm from the drive/motor. The Shear Pin is monitored and if it breaks an alarm contact closes which is wired to the SCADA system.

Load Monitors provide continuous monitoring of the clarifier motor current. If a jam occurs on the skimmer arm, the load monitor will detect a rise in current draw to the motor and provide dry-contact outputs to the SCADA system, if the current rise exceeds a preset value for more than an adjustable time delay period. There are two alarms associated with the Load Monitoring – “Load Monitoring Warning” which is a warning alarm and a “Load Monitoring Shutdown” alarm which is wired to the motor starter circuit to shut down the clarifier. The Load Monitor is typically installed in the clarifier control panel

This instrumentation is may or may not be required by the clarifier manufacturer to safely operate their product along with maintaining warranties. As the designer discusses the operation of the clarifying system, protective items must be discussed with the manufacturer and process engineer. Some commonly manufacturer requested instruments are listed in Table B3-2 below.

Table B3-5 Clarifier Specialty Clarifier Alarms

IO Type	Description	Delay	Priority
IO Discrete	Shear Pin Alarm	5 seconds	300
IO Discrete	Load Monitoring Warning	5 seconds	300
IO Discrete	Load Monitoring Shutdown	5 seconds	200

B4 CONTINUOUS INSTRUMENT

B4.1 Introduction

The City of Tulsa wastewater treatment process uses Continuous Instruments to measure various process parameters throughout the plant and display these readings on the SCDADA system. Continuous Instruments as the name implies continuously measure the process parameter in real-time across the full range of expected values. These parameters include but are not limited to:

- Flow
- Level
- Pressure
- Analytical measurements (e.g.: pH, ORP, DO, CL2, etc.)

For example, a magnetic flowmeter measures flow from 0 to the Full-Scale value in engineering units (e.g. GPM) that the meter is designed for. There are many continuous instruments available from manufacturers to measure these and many other parameters needed at a wastewater treatment facility.

The Continuous Instruments are self-contained and have all the required detection, electrical and mechanical components to sense the measured parameter, display it locally (if necessary) and transmit it to the SCADA system as required. Each instrument is comprised of a sensor and a transmitter. The sensor can either be integral to the transmitter or mounted remotely. If mounted remotely then wiring is required to connected them. This wiring can be either provided by the manufacturer (typical of magmeters) or by the electrical contractor. The transmitter contains the electrical components and is housed in a NEMA enclosure rated for the process area/application. Using the local controls, personnel can setup, calibrate and service the unit. Most instruments are solid state electronic based and include sophisticated electronics to monitor the instrument for health and predictive maintenance such as the Sensor Calibration Needed or sensor End-of-Life conditions. The measured parameter is transmitted as an analog signal (e.g. 4-20mA) calibrated in engineering units to the SCADA system. In addition to the hardwired analog signal, many manufacturers now offer communications networks such as HART (Highly Addressable Remote Transducer) protocol that allow multiple instruments to be connected together and provide the measured parameter value along with a myriad of diagnostic data about the instrument.

Based on differing instrument types, there are several decisions that a designer will need to make in determining how to protect both the instrument and the related process equipment. Several of these decisions involve the field instrumentation and if/when to provide specific wiring in the starter controls to monitor and act based on the imbedded instruments. All Instruments are to be installed and wired per the manufacturer's recommendations.

B4.2 Standard Continuous Instrument Alarm Design

An engineer shall design an alarm system that will protect the Continuous Instrument and related process equipment. This alarm system shall contain, at a minimum, the alarms listed below in Table B4-1. The alarm system consists of hardwired Continuous Instrument controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay,

programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B4.2.1 Hardwire Alarms

Some Continuous Instrument may have hardwired alarms associated with them. The Designer must consult with the specific manufacturer to determine which are available and if they are to be used. For example, magnetic flow meters have an “Empty Pipe” alarm, ultrasonic level instruments have a “Loss of Echo” and gas detectors have a “Trouble” alarm that indicates the unit may not be functioning.

B4.2.2 Software Alarms

The software alarms associated with Continuous Instruments are directly related to the measured process parameter value. The first of these is the Instrument “Value Fault” alarm. This alarm is generated when the PLC detects that the analog input signal is not within the prescribed range. For example, a 4-20mA signal is not within these limits whether it is above (>20mA) or below (<4mA) for a time period. Some PLC manufacturers provide for this type of alarm detection within the analog input module itself otherwise it must be programmed separately.

Each of the High-High, High, Low and Low-Low alarms are separately generated when the measured process parameter exceeds (High-High and High) the setpoint alarm value or falls below it (Low-Low and Low) for a specified time period. The alarm setpoints can be entered via the SCADA system HMI software via a password protected screen. The alarm setpoints must be provided by the alarm system designer working with process engineers to determine the initial alarm value. These must be easily adjustable and can be changed during startup and commissioning.

Note: Not all four of these alarms may be required. The engineer must decide which ones apply and design the system accordingly.

Additionally, an Alarm Reset Setpoint is required to prevent rapid toggling of the alarm if the value hovers around the setpoint value. This is the value that the process parameter must increase or decrease to before the alarm is declared as having returned to Normal state and can reset.

The following example is provided:

A Wet Well Level with a maximum fill level of 20 feet, the alarm setpoints:

Alarm	Alarm Setpoint	Alarm Reset Setpoint
High-High	18.0 (rising)	17.5 ft (falling)
High	16.5 ft. (rising)	16.0 ft (falling)
Low	4.0 ft (falling)	4.5 ft. (rising)
Low-Low	2.0 ft (falling)	2.5 ft. (rising)

Note: Where possible alarm values shall be Real numbers

Table B4-6 Continuous Instrument Minimum Alarms

IO Type	Description	Delay	Priority
PLC	Instrument – Valve Fault	5 seconds	400
PLC	Instrument – High-High Alarm	5 seconds	200

B4.3 Specialty Continuous Instrument Alarm Design

Some Continuous Instrument types use communication networks in lieu of or in addition to the hardwired analog input signal. These networks vary depending on the manufacturer but one of the most commonly used as previously mentioned is the HART protocol. These networks can provide additional diagnostic data about the instrument that can be used to provide alarm conditions for display at SCADA. Refer to the manufacturer's information for details.

If such a communications network is designed, regardless of the exact type used the network needs to be monitored for any interruption of the communication connection and alarm at the SCADA system.

B5 CONTROL PANELS

B5.1 Introduction

The City of Tulsa wastewater treatment plants use control panels throughout the plant to monitor and control the process. These panels are supplied by different equipment manufacturers and also from a System Integrator (SI) and come in a variety of sizes and complexities depending on the specific function they serve. This section focuses on those control panels that contain Programmable Logic Controllers (PLCs) but can also apply to non-PLC panels as applicable.

Control panels with PLCs require power conditioning equipment such as Uninterruptable Power Supplies (UPS) and DC Power Supplies. Additionally, PLC panels also contain other non-process related equipment such as communications equipment (Ethernet switches, radio equipment, etc.), control panel temperature switches and intrusion detection switches.

The SCADA systems monitor these panels for these ancillary alarms that aren't directly related to the treatment process but do provide information to maintenance personnel about the health of this equipment.

B5.2 Standard Control Panel Alarm Design

An engineer shall design an alarm system that will monitor and protect a control panel's critical components and alarm if any abnormal condition is detected.

Since it is the Owner's preference a PLC be provided in all manufacturer's control systems, monitoring of the equipment shall be via an Ethernet connection to the plant SCADA system. If a PLC is not provided, coordination meetings between Engineer, Owner, and Manufacturer will be held during design to iron out a full list of alarms desired. This alarm system shall contain the, alarms listed in Table B5-1 as applicable and other alarms recommended by the manufacturer. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B5.2.1 Hardwire Alarms

Control panels should monitor the incoming 120VAC Utility power feed. A control relay connected directly to this incoming power can be used. The relay is energized when Utility power is present and de-energized when power fails. Contacts from the relay are wired to the PLC so that If the utility power source goes down a "Control Panel Utility Power Fail" is generated.

A UPS is required for panels with a PLC to help ensure a clean power source and backup power if the Utility power is lost. Additionally, UPS's should be specified to include a Bypass Switch or other means by which the UPS can be removed for maintenance (such as replacing the batteries) and quickly allow switching the control panel power with minimal interruption of power to the control panel. Since UPS's use batteries to provide backup power, consideration should be given during design to the "back-up" time batteries should provide power before the panel shuts down.

Each UPS typically has several preconfigured, dry-contact alarm outputs provided by the manufacturer that are wired to the PLC. These alarms are “UPS Fail” – any internal fault within the UPS (consult manufacturer for details), “UPS On Battery” – utility power has been interrupted and the UPS has switched to its backup battery power, and “UPS Low Battery” – this indicates that the UPS batteries are no longer reaching the full charge voltage and could need to be replaced.

If DC power supplies are included in the control panel, they should also be monitored to ensure that they are operational. Typically for large PLC panels, redundant DC power supplies are required that include the manufacturers' redundancy module or other means to switch between them if one of them fails. In order to detect a DC power supply failure, a relay for each supply can be directly wired to the output of it. The relay contacts are wired to the PLC. As long as the power supply output voltage is within limits, the relay is energized. If the power supply voltage drops significantly or stops altogether, the relay de-energizes and a “Control Panel DC Power Supply Fail” alarm is generated.

B5.2.2 Software Alarms

There are software alarms associated with the operational sequence of the equipment.

Most PLCs monitor themselves for a variety of internal statuses and faults. Within the Allen Bradley family of PLCs, faults are classified as either a Major or Minor. Furthermore, they are designated as either Recoverable or Non-Recoverable. There are many types of faults that are monitored for and each one has a specific code. A Non-Recoverable fault is one that cannot be corrected and may require replacement of the PLC hardware. Consult with the client to determine which specific faults and/or statuses should be monitored for operational and maintenance purposes.

The PLC has internal status bits that indicate its operational status: Running, Program Mode, or Faulted. Of critical importance is the PLC Running mode status. The Running mode is the normal operating mode for the PLC. The Run mode should be monitored by the SCADA system and a “PLC not in Run Mode” alarm generated if the PLC is not in this mode.

Another important alarm is the “PLC Communications Failure” alarm. This alarm is generated when network communication (e.g. Ethernet) is disrupted for a short time between the PLC and the higher-level SCADA servers. Typically, a “Watch-dog” timer is programmed in the PLC which the equipment periodically resets to ensure that communication is operational. If the comms link is down and the watch-dog timer times out, an alarm is generated.

The designer should consider which faults should be monitored and alarmed at the SCADA system.

Table B5-7 Equipment Generic Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Control Panel Utility Power Fail	5 seconds	200
IO Discrete	Control Panel UPS Fail	5 seconds	200
IO Discrete	Control Panel UPS on Battery	5 seconds	200
IO Discrete	Control Panel UPS Low Battery	5 seconds	300
IO Discrete	Control Panel DC Power Supply Fail	5 seconds	200
PLC	Control Panel PLC Not in Run Mode	5 seconds	100
PLC	Control Panel PLC Fault	5 seconds	100

PLC	Control Panel PLC Communications Failure	5 seconds	100

B5.3 Specialty Control Panel Alarm Design

Control panels may require additional protective instrumentation. This additional instrumentation is usually provided by the control panel manufacturer to safely operate their product along with maintaining warranties. As the designer discusses the operation of the control panel, protective items must be discussed with the manufacturer. Some common manufacturer-requested instruments are listed in Table B5-2 below. Also refer to other Alarm Sections as applicable. For instance, Continuous Instruments for details on alarm requirements of instrumentation and/or equipment related to the manufacturer's package.

B5.3.1 Temperature Monitoring

Control panels contain components that both generate heat and are susceptible to temperatures that are outside the operating range. For Control panels that are located outdoors in warm or cold climates this is of particular concern.

Typically, a temperature switch such as a thermostat is used to detect temperature above a certain high or low level to start a cooling or heating system. The thermostat is also wired to the PLC to generate a temperature alarm.

B5.3.2 Panel Intrusion Alarm

For security purposes, control panels are often monitored for entry access in order to alert operators that unauthorized access has occurred. This is especially important for panels located outdoors at unmanned sites. Typically, a switch is installed on each control panel door that is wired to the PLC and generates a "Control Panel Intrusion" alarm each time the door is opened. If maintenance personnel are scheduled to access the panel then the alarm can be ignored or suppressed.

Table B5-8 Specialty Alarms for Control Panels

IO Type	Description	Delay	Priority
IO Discrete	Control Panel High/Low Temp.	10 seconds	200
IO Discrete	Control Panel Intrusion Alarm	5 seconds	200

B6 MANUFACTURER SUPPLIED CONTROL SYSTEMS

B6.1 Introduction

The City of Tulsa wastewater treatment plants use a variety of process equipment that comes with prepackage controls systems. Examples of such process equipment includes but is not limited to: Ultraviolet (UV) Disinfection, Barscreens, Grit Removal and Compaction, Incinerators, Chemical Feed systems, etc. This equipment serves a specialized function in the treatment process and may include complex, proprietary control information specific to the manufacturer. It is common that these systems include a Programmable Logic Controller (PLC) that is programmed by them as well.

The purpose of this section along with the individual equipment specification sections is to provide standards for the control systems components and alarm requirements. By standardizing the major control system components, such as the PLC, on a single manufacturer simplifies troubleshooting and maintenance and reduces the Owner's overall maintenance costs. The Owner has selected Allen Bradley

as their preferred PLC manufacturer. The exact model of PLC will depend upon a variety of factors including number of IO points, the need for redundancy, and other factors. This and other related equipment including Ethernet switches, Operator Interface Terminals (OITs) are specified elsewhere.

If the manufacturer's control system does not contain a PLC then hardwire alarms will be required. This section provides examples of alarm signals from both the equipment and associated field instrumentation sensors. Refer to the specific equipment specification section for additional details.

B6.2 Standard Manufacturer's Equipment Alarm Design

An engineer shall design an alarm system that will protect the equipment and monitor the immediate process area associated with it and alarm if any abnormal condition is detected. For example, in addition to monitoring the equipment, monitoring the atmosphere for combustible gas around equipment in a classified area. The gas detection equipment may not be provided by the equipment manufacturer but needs to be included as part of the overall design.

Since it is the Owner's preference that a PLC be provided in all manufacturer's control systems, monitoring of the equipment shall be via an Ethernet connection to the plant SCADA system without any hardwired alarms wired to the PLC. If a PLC is not provided, coordination meetings between Engineer, Owner, and Manufacturer will be held during design to iron out a full list of alarms desired. This alarm system shall contain the sample generic alarms listed in Table B6-1 as applicable and other alarms recommended by the manufacturer. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B6.2.1 Hardwire Alarms (if a PLC is not provided)

A motor starter (ACL, VFD, or RVSS) is provided to turn on/off, and/or provide speed control as needed by the process. Internal to a starter are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. This input shall be monitored by both the starter and the PLC. If an "Equipment Overload Trip" input is received, both the starter and the PLC will immediately call for the unit to stop and lock out the equipment. A local manual reset will be required before restarting the equipment.

Note: If a VFD or RVSS is used in lieu of an across the line starter (ACL) to control the equipment, additional alarms specific to those controllers are not discussed here. Refer to the VFD and RVSS sections for a detailed discussion of these additional alarms.

The motor has integral thermo-switches that provide feedback for winding temperature. This input shall be monitored by both the starter and the PLC. If an "Equipment Hot Motor High Winding" alarm is received, both the starter and the PLC will immediately call for the unit to stop and lock out the equipment. The thermo-switches open on high temperature and will automatically close again when the motor cools below the switch setpoint thus allowing the equipment to be restarted.

The ability to quickly stop the equipment under an emergency is needed to protect the asset and personnel. The use of an Emergency Stop provides this quick stop capability immediately next to or on the equipment where a full disconnect may not fit. The E-Stop can be a pushbutton, pull-string, limit switch (on protective equipment covers) or other such means. It is hardwired to the starter and the PLC. Both the starter and the PLC will call for the equipment to stop immediately and be locked out until the is the condition is cleared and a manual reset.

A motor protection relay device is incorporated with medium voltage equipment to monitor the incoming power feed to the equipment. This device will monitor for over and under-voltage, phase-loss and other abnormal electrical conditions. This input shall be monitored by both the starter and the PLC. If a "Equipment Protection Relay Fault" input is received, both the starter and the PLC will immediately call for

the unit to stop and lock out the equipment. A local manual reset will be required before restarting the equipment.

The equipment is also equipped with a Hand-Off-Remote (HOR) or a Hand-Off-Auto (HOA) switch. If an HOR switch is used and the switch is in “REMOTE” position, this indicates to operators that the equipment is controllable remotely from the plant SCADA PLC. If the PLC sees that the HOR switch is not in “REMOTE”, an alarm signal is generated and is sent to the SCADA network. If an HOA switch is used and the switch is in “AUTO” position, this indicates to operators that the equipment is controlled locally by the equipment PLC and not the plant SCADA PLC. If the PLC sees that the HOA switch is not in “AUTO”, an alarm signal is generated and is sent to the SCADA network.

Also, operators have the option via the HMI graphic to place equipment “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the equipment icon and doing so disables it from operating in remote modes. Furthermore, putting equipment out of service disables all alarms associated with it. Putting equipment out of service does not issue an alarm.

B6.2.2 Software Alarms

There are software alarms associated with the operational sequence of the equipment.

The “Equipment Run Disable” alarm is generated when there is one or more another alarms that shut down and lock out the equipment and notifies the operator that a manual Reset is required before the motor can be restarted.

When a motor starts, excess heat is generated internally. Subsequent starts within a short time period (typically an hour) that occur without a cool down period between starts can lead to winding temperature trips and life span shortening from insulation decay. A “Equipment Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE/AUTO mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. The designer must coordinate with the motor manufacturer to determine what maximum value this can be. The default setting in the Table B6-1 below is five starts per hour.

A second sequential alarm is issued when the equipment does not start or stop based on commands from the SCADA system. If the SCADA systems requests the equipment to start and a positive running feedback is not received, a “Equipment Fail to Start” alarm is generated. If the SCADA system requests the equipment to stop and the positive running feedback does not go away, a “Equipment Fail to Stop” alarm is generated. The positive running feedback is usually a contact from the associated starter for the motor; however, other options could be used such as the presence of flow on a flow meter, rise in pressure on discharge line, etc.

A third alarm is the “Equipment Communications Failure” alarm. This alarm is generated within the PLC when network communications (e.g. Ethernet) is disrupted for a short time period between the equipment and the PLC. Typically, a “Watch-dog” timer is programmed in the PLC which the equipment periodically resets to ensure that communications is operational. If the comms link is down and the watch-dog timer times out an alarm is generated.

Equipment is monitored for excessive temperature. Typically, Resistance Temperature Detectors (RTD) are used for temperature monitoring. These are provided by the equipment manufacturer and are embedded in the equipment housing at the bearing(s) and other temperature sensitive components. Each RTD is labeled to its location and is wired to a specialty PLC module specifically for the type of RTD used. The RTD provides an analog signal to the PLC which converts it to a scaled value in engineering units (^{o}C or ^{o}F). The PLC in turn monitors each RTD for both a “Equipment High Temp Warning” and a “Equipment High Temp Alarm”. The Equipment High Temp Warning alerts the operator that the temperature has exceeded the norm temperature at that location but does not shutdown the equipment. The Equipment

High Temp Alarm alerts the operator and does shutdown the equipment. For RTDs and other similar Continuous Instruments refer to that section for details.

Table B6-9 Equipment Generic Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Equipment Overload Trip	5 seconds	300
IO Discrete	Equipment Hot Motor Winding	5 seconds	300
IO Discrete	Equipment E-Stop Activated	5 seconds	300
IO Discrete	Equipment Protection Relay Fault	5 seconds	300
IO Discrete	Equipment Not in Remote	5 seconds	400
PLC	Clarifier Run Disable	5 seconds	200
PLC	Equipment Starts Exceeded	5 seconds	300
PLC	Equipment Start-Stop Fail	seconds	200
Ethernet/PLC	Equipment Communications Fault	5 seconds	300
PLC	Equipment Bearing High Temp Warning	15 seconds	400
PLC	Equipment Bearing High Temp Shutdown	30 seconds	300

B6.3 Specialty Manufacturer's Equipment Alarm Design

Equipment motor combinations may require additional protective instrumentation. This additional instrumentation is usually required by the Equipment manufacturer (but not provided by them) to safely operate their product along with maintaining warranties. As the designer discusses the operation of the equipment, protective items must be discussed with the manufacturer and process engineer. Some commonly manufacturer requested instruments are listed in Table B6-2 below. Also refer to other Alarm Sections as applicable. For instance, Continuous Instruments for details on alarm requirements of instrumentation and/or equipment related to the manufacturer's package.

B6.3.1 Environmental Monitoring

As part of the overall alarm system design for process equipment, the environment in which it is located must be taken into consideration. This includes but is not limited to monitoring for ambient temperature, combustible gas detection, fire/smoke detection, spill/flood detection etc. Each of these are discussed below.

B6.3.2 Ambient Temperature Monitoring

Consideration should be given to monitoring room/area/panel temperature where high temperatures may affect equipment operation. This monitoring is vital to rooms that are temperature controlled in order to keep equipment with its 'operating range. This is particularly true for electronic equipment such as PLCs that are located in control panels in process areas.

B6.3.3 Combustible Gas Detection

Of critical importance is the monitoring of Combustible Gas in classified areas. Equipment that is located in Classified areas (C1D1 or C1D2) will need to be monitored for combustible gas. This is a Life-Safety issue and provides alarming to personnel that the area is ***NOT*** safe to enter. Combustible gas detection systems consist of one or more sensors designed to detect a specific combustible gas (H2, CH4,

hydrocarbons) that wire a transmitter. The transmitter converts the sensor signal into an analog signal(4-20mA) that wires to the PLC. a transmitter

B6.3.4 Fire/Smoke Detection

Fire/smoke detection is usually a standalone subsystem with its' own specification that may or may not directly wire to the PLC. However, as a minimum fire/smoke detector(s) may be required in the process area (consult the NFPA, NEC and local authority having jurisdiction (AHJ)). Fire/smoke detectors should be specified that provide a dry-contact output when wired directly to the PLC.

B6.3.5 Spill/Flood Detection

This applies to a variety of systems including chemical storage facilities, dry-pit areas and any other area where a spill or flood may cause damage or injury. Typically, for bulk chemical storage a containment area surrounds the storage vessels in order to contain a leak or spill. The containment area has a sump with float switches to detect the accumulation of liquid. Also, for dry-pit pumping area the pump deck will include a sump or if not, a level detection probe system may be used to detect a flood condition on the floor as little at 1". In either case these devices are wired to the PLC and/or local alarm displays.

B6.3.6 Vibration Monitoring

Equipment motor vibration would become an issue if it is neglected. Small vibrations can quickly resonate and lead to shaft bending or bearing destruction. The designer shall specify vibration sensors in locations recommended by the equipment manufacturer. These sensors can either connect to the PLC or be part of a separately specified vibration monitoring system that in turn provides dry-contact outputs to the PLC when a high vibration is detected. Maximum vibration levels shall be provided by the manufacturer and PLC logic implemented to issue warnings and alarms. If there is a high probability of excessive equipment vibration, sensors on the equipment casing may be used to provide early warning. Consult the manufacturer.

B6.3.7 Seal Water or Cooling Water Flow Monitoring

Some equipment requires water for cooling and/or lubrication of seals. In either case water flow and/or pressure should be monitored. Seal Water is required to both lubricate the seal and prevent the shaft and seal from overheating. If the water flow is interrupted for even just a short period of time (seconds), heat can build up causing deformation or seal failure. The use of flow switch and pressure switch are two common alarm signals to monitor seal water system on the seal water system. For the system where the seal water is only turned on when the Equipment is in operation, a flow switch between shutoff solenoid and the equipment location monitors water flow to the seal. The pressure/flow switch is hardwired to the starter and the PLC. Both the starter and the PLC will call for the equipment to stop if the pressure/flow switch drops out.

B6.3.8 Pressure Sensing

A major destructive force to equipment is operating outside the recommended pressure range. Pressure sensors can be installed on the suction and discharge lines of the equipment or on the equipment itself. These sensors can be either pressure switches and/or pressure transmitters. The pressure sensors would be connected back to the PLC. PLC logic is implemented to issue pressure warning alarms along with shutting the Equipment down if necessary. Consult the manufacturer for specific pressure ranges. For pressure transmitter and other analog instruments, Refer to the Continuous Instrument section for details on alarms.

Table B6-10 Specialty Equipment Alarms

IO Type	Description	Delay	Priority

IO Real	Combustible Gas Monitoring	15 seconds	100
IO Discrete	Ambient/Room High Temperature	30 seconds	400
IO Discrete	Fire/Smoke Detection	15 seconds	200
IO Discrete	Spill Flood Detection	30 seconds	300
IO Discrete	Equipment High Vibration Warning	5 seconds	400
IO Discrete	Equipment High Vibration Shutdown	5 seconds	200
IO Discrete	Equipment Seal Water Low Flow	5 seconds	100
IO Discrete	Equipment Seal Water Low Pressure	5 seconds	100
IO Discrete/PLC	Equipment Low Pressure	5 seconds	200
IO Discrete/PLC	Equipment High Pressure	5 seconds	200

B7 MEDIUM-VOLTAGE BLOWER

B7.1 Introduction

The City of Tulsa wastewater treatment plants use blowers to provide required air flow to treatment process throughout the plant. When a design has a process application that requires a high-capacity, large horsepower (300 horsepower and above) blower, a medium-voltage (4160V) should be considered instead of a low-voltage (480V) one. A medium-voltage motor demands lower inrush current than a low-voltage motor, approximately nine times lower. The reduced inrush current provides economic benefits in both construction costs and operational costs. Construction costs savings are realized, since the lower inrush allows for substantially smaller gauge power feed conductors, potentially fewer parallel runs of conductors and smaller conduit size. Additionally, the low inrush current applies less stress on electrical utility grid and wastewater treatment plant itself. Also, medium-voltage motors would require smaller capacity (current) motor starter whether an ACL, VFD, or RVSS, when compared to a low-voltage one for the same horsepower motor and thus additional cost savings. There are a variety of different technologies that blowers use to generate and control air flow. Each type has its own unique set of instrumentation to monitor the operation of the blower. The engineer must take this into consideration and refer to the manufacturers' specific requirements when designing the alarm system. This section describes alarm signals from field instrumentation sensors and alarm signals embedded in the starter.

B7.2 Standard Blower Alarm Design

An engineer shall design an alarm system that will protect the blower and motor combination. This alarm system shall contain, at a minimum, the alarms listed in Table B7-1. The alarm system consists of hardwired starter controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B7.2.1 Hardwire Alarms

A motor starter (ACL, VFD, or RVSS) is provided to turn on/off, and/or provide speed control as needed by the process. For medium voltage motors a Motor Protection Relay (MPR) is used instead of a simple motor overload device for monitor and protect the motor. An MPR is a sophisticated device that can monitor multiple electrical anomalies including motor overload, phase-loss, power-loss, thermal overload and other electrical abnormalities. A variety of sensors can be wired to the MPR including Current Transformers (CT), Resistance Temperature Devices (RTDs) and others depending on the electrical and other parameters to be monitored. The MPR continuously monitors the sensors for any abnormalities and

generates a supervisory alarm "Blower Motor Fault" output that is wired to the motor control circuit and the PLC that will immediately call for the unit to stop and lock out the blower. A local manual reset will be required before restarting the blower. The MPR monitors for the blower for Phase-loss and Loss of Power. These inputs can also be monitored by both the starter and the PLC to shut down the blower. Additionally, RTDs re wired to the MPR to monitor blower motor windings and bearing temperature. The PLC in turn monitors each RTD for both a "Blower Motor Hot Winding" and a "Blower High Temp Shutdown". The Blower High Temp Warning alerts the operator that the temperature has exceeded the normal temperature at that location but does not shutdown the blower. The Blower High Temp Shutdown alerts the operator and does shutdown the blower.

The ability to quickly stop the blower under an emergency is needed to protect the asset and personnel. The use of an Emergency Stop Pushbutton provides this quick stop capability immediately next to the equipment where a full disconnect may not fit. The pushbutton is hardwired to the starter and the PLC. Both the starter and the PLC will call for the blower to stop immediately and be locked out until the pushbutton is reset.

The blower is also equipped with a Hand-Off-Remote (HOR) switch, and when the switch is in "REMOTE" position, this indicates to operators that the RVSS is controllable remotely from the PLC. If the PLC sees that the HOR switch is not in "REMOTE", an alarm signal is generated and is sent to the SCADA network.

Note: If a VFD or RVSS is used in lieu of an across the line starter to control the pump, additional alarms specific to those controllers are not discussed here. Refer to the VFD and RVSS sections for a detailed discussion of these additional alarms.

B7.2.2 Software Alarms

There are alarms associated with the operational sequence of the pump and are generated in the PLC.

The "Blower Run Disable" alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

When a motor starts, excess heat is generated internally. Subsequent starts within a short time period (typically an hour) that occur without a cool down period between starts can lead to winding temperature trips and life span shortening from insulation decay. A "Blower Starts Exceeded" alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. The designer must coordinate with the motor manufacturer to determine what maximum value this can be. The default setting in the Table B7-1 below is five starts per hour.

Another sequential alarm is issued when the blower does not start or stop based on commands from the SCADA system. If the SCADA systems requests the blower to either Start or Stop and a feedback input is not received, a "Blower Start-Stop Fail" alarm is generated. The positive running feedback is usually a contact from the associated starter for the motor; however, other options could be used such as the presence of flow on a flow meter, rise in pressure on discharge line, etc.

A third alarm is the "Blower Communications Failure" alarm. This alarm is generated within the PLC when network communications (e.g. Ethernet) is disrupted for a short time period between the blower PLC and the SCADA system. Typically, a "Watch-dog" timer is programmed in the PLC which the blower periodically resets to ensure that communications is operational. If the communications link is down and the watch-dog timer times out an alarm is generated.

Also, operators have the option via the HMI graphic to place a blower "Out-of-Service". A visual "OOS" tag appears on the HMI graphic next to the blower icon and it does not operate in remote modes. Furthermore, putting a blower out of service disables all alarms associated with it. Putting a blower out of service does not issue an alarm.

Table B7-11 Medium Voltage Blower Minimum Alarms

IO Type	Description	Delay	Priority
MPR/IO Discrete	Blower Motor Fault	5 seconds	300
MPR/IO Discrete	Blower Motor Hot Winding	5 seconds	300
MPR/IO Discrete	Blower Phase Loss	5 seconds	300
MPR/IO Discrete	Blower Power Loss	5 seconds	300
MPR/IO Discrete	Blower Bearing High Temp Warning	5 seconds	400
MPR/IO Discrete	Blower Bearing High Temp Shutdown	5 seconds	300
IO Discrete	Blower E-Stop Activated	5 seconds	300
IO Discrete	Blower Not in Remote	5 seconds	400
PLC	Pump Run Disable	0 seconds	200
PLC	Blower Starts Exceeded	5 starts/hour	300
PLC	Blower Start-Stop Fail	15 seconds	200
Ethernet/PLC	Blower Communications Fault	5 seconds	200

B7.3 Specialty Blower Alarm Design

Large horsepower blower motor combinations require additional protective instrumentation. This additional instrumentation is usually required by the blower manufacturer (but may not be provided) to safely operate their product along with maintaining warranties. As the designer discusses the operation of the blower system, protective items must be discussed with the manufacturer and process engineer. Some commonly manufacturer requested instruments are listed in Table B7-2 below. For analog transmitters, refer to the Continuous Instrument section for details on alarms.

B7.3.1 Vibration Monitoring

Blower motor vibration would become an issue if it is neglected. Small vibrations can quickly resonate and lead to shaft bending or bearing destruction. The designer shall specify vibration sensors in locations recommended by the pump manufacturer. These sensors can either connect shall connect back to the PLC or be part of a separately specified vibration monitoring system that in turn provides dry-contact outputs to the PLC when a high vibration is detected. Maximum vibration levels shall be provided by the manufacturer and PLC logic implemented to issue warnings and alarms. If there is a high probability of excessive impeller wear, vibration sensors on the blower casing may be used to provide early warning of impeller decay. Unless it is a large blower, usually in 600 HP and larger arena, the cost of operating and maintaining this sensor does not equate to the benefit of early warning.

B7.3.2 Pressure Sensing

A potential problem with blowers is surge. The onset of surge can be monitored using pressure sensors on the suction and discharge lines of the blower. If the net blower suction head is too low, surge can occur. The pressure sensors would be connected back to the PLC. Utilizing the minimum pressure levels provided by the blower manufacturer, PLC logic is implemented to issue low suction pressure warning alarms along with shutting the blower down if necessary. The discharge pressure sensor reading can be used to show there is a plug in the line or a closed valve.

Table B7-12 Specialty Blower Alarms

IO Type	Description	Delay	Priority
IO Discrete	Blower High Vibration Warning	5 seconds	200
IO Discrete	Blower High Vibration Shutdown	0 seconds	100
PLC	Blower Low Suction Pressure	5 seconds	300
PLC	Blower High Discharge Pressure	5 seconds	300

B8 MIXER

B8.1 Introduction

The City of Tulsa wastewater treatment process uses motorized Mixers in a variety of process areas to achieve mechanical mixing of process liquids or to prevent settling of solids in process tanks throughout the plant. They are designed to run continuously unless placed Out-of-Service. The Mixer can be either constant-speed or variable-speed driven by a VFD.

Mixers are relatively simple devices consisting of a motor, drive train, shaft and mixing blades. They have a drive/motor combination used to rotate a shaft that has the mixing blades submerged in the process liquid. The Mixer controls are either located at the mixer or at the MCC.

B8.2 Standard Mixer Alarm Design

An engineer shall design an alarm system that will protect the Mixer drive/motor combination. This alarm system shall contain, at a minimum the alarms listed below in Table B8-1 and include any other alarms as recommended by the manufacturer. The alarm system consists of hardwired starter controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B8.2.1 Hardwire Alarms

A motor starter (ACL, RVSS or VFD) is provided to turn on/off the mixer and/or control the speed as needed by the process. Internal to a starter are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. A “Mixer Overload Trip” input to the PLC from the overloads will turn off the clarifier and lock it out from starting and requires a manual Reset.

The Mixer is also monitored for high torque loading with a couple of separate inputs. The first is the “Mixer Torque Warning” which is a warning alarm that the torque level is exceeding the normal range and is typically set to 110% of rated torque. The second is the Mixer Torque Shutdown” which is a shutdown alarm that is wired to the motor starter and the PLC and is set to 140% of rated torque. These torque ratings are adjustable and typically specified by the manufacturer.

An “Emergency Stop Activated” alarm is generated when the emergency stop pushbutton is pressed. This button is typically located at the mixer for life-safety reasons. The button is maintained such that it must be pulled out (reset) to allow the mixer to be restarted.

The mixer is also equipped with a Hand-Off-Remote (HOR) switch, and when the switch is in “REMOTE” position, this indicates to operators that the mixer is controllable remotely from the PLC. If the PLC sees that the HOR switch is not in “REMOTE”, an alarm signal is generated and is sent to the SCADA network.

Note: If a VFD or RVSS is used in lieu of an across the line starter to control the pump, additional alarms specific to those controllers are not discussed here. Refer to the VFD and RVSS sections for a detailed discussion of these additional alarms.

B8.2.2 Software Alarms

There are alarms associated with the operational sequence of the Mixer. A sequential alarm is a “Mixer Fail to Start/Stop”. This alarm is generated when the mixer does not start or stop based on commands from the SCADA system. If the SCADA system requests the mixer to start and a positive running feedback is not received within the designated time period, an alarm is generated. If the SCADA system requests the mixer to stop and the positive running feedback does not go away, an alarm is generated. The positive running feedback is a contact from the motor starter.

The “Mixer Run Disable” alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

A “Mixer Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. The designer must coordinate with the motor manufacturer to determine what maximum value this can be.

Also, operators have the option via the HMI graphic to place a mixer “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the mixer icon and it does not operate in remote modes. Furthermore, putting a mixer out of service disables all alarms associated with it. Putting a mixer out of service does not issue an alarm.

Table B8-13 Mixer Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Mixer Overload Trip	5 seconds	300
IO Discrete	Mixer Torque Warning	5 seconds	400
IO Discrete	Mixer Torque Shutdown	5 seconds	300
IO Discrete	Mixer Emergency Stop Activated	5 seconds	300
IO Discrete	Mixer Not in Remote	5 seconds	400
PLC	Mixer Run Disable	0 seconds	200
PLC	Mixer Starts Exceeded	5 starts/hour	300
PLC	Mixer Fail to Start/Stop	15 seconds	200

B8.3 Specialty Mixer Alarm Design

If the mixer is variable-speed (VFD) or an RVSS is used to control it, then see those respective sections for additional alarms.

B9 PUMP (NON-SUBMERSIBLE)

B9.1 Introduction

The majority of motor/pump combinations, for the City of Tulsa wastewater treatment process, units are not submerged directly in the process liquid. The motor and pump are located on concrete pads physically attached to piping that interconnects one hydraulic zone to another. This combination connects the pump to the motor via a shaft. Depending on the distance between the pump and motor, there may

one to several bearings and/or seals allowing for the support of the spinning shaft. In some instances, the pump is directly attached to an electric motor. Based on these differing installation types, there are several decisions that a designer will need to make in determining how to protect this equipment. Several of these decisions involve field instrumentation and if/when to provide specific wiring in the starter controls to monitor and act based on the imbedded instruments. Some examples of field instrumentation are vibration sensors, thermo-switches in the motor windings, pressure sensors, flow sensors, etc.

B9.2 Standard Pump Alarm Design

An engineer shall design an alarm system that will protect the pump and motor combination. This alarm system shall contain, at a minimum, the alarms listed below in Table B9-1. The alarm system consists of hardwired starter controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where.

B9.2.1 Hardwire Alarms

A motor starter (ACL, RVSS or VFD) is provided to turn on/off the pump, and/or control the speed as needed by the process. Internal to a starter are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. A “Pump Overload Trip” input to the PLC from the overloads will turn off the pump and lock it out from starting and requires a manual Reset.

The motor has integral thermo-switches that provide feedback for motor winding temperature. This input shall be monitored by both the starter and the PLC. If a “Pump Motor Hot Winding” alarm is received, both the starter and the PLC will immediately call for the unit to stop and lock out the pump. The thermo-switches open on high temperature and will automatically close again when the motor cools below the switch setpoint thus allowing the pump to be restarted.

The ability to quickly stop the pump under an emergency is needed to protect the asset and personnel. The use of an Emergency Stop Pushbutton provides this quick stop capability located immediately next to the equipment where a full disconnect may not fit. An “Emergency Stop Activated” alarm is generated when the emergency stop pushbutton is pressed. The pushbutton is hardwired to the starter and the PLC. Both the starter and the PLC will call for the pump to stop immediately and be locked out until the pushbutton is reset.

Another pump alarm is the “Pump Not in Remote”. Since the pump is normally controlled via the PLC, if the Local-Off-Remote switch at the local control station is not in the Remote position this alarm is generated.

Note: If a VFD or RVSS is used in lieu of an across the line starter to control the pump, additional alarms specific to those controllers are not discussed here. Refer to the VFD and RVSS sections for a detailed discussion of these additional alarms.

B9.2.2 Software Alarms

There are alarms associated with the operational sequence of the pump and are generated in the PLC.

The “Pump Run Disable” alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

A “Pump Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. Subsequent starts that occur prior to a cool off period can lead to winding temperature trips and life span shortening from insulation

decay. The designer must coordinate with the motor manufacturer to determine what maximum value this can be.

Another sequential alarm is issued when the pump does not start or stop based on commands from the SCADA system. If the SCADA systems requests the pump to either Start or Stop and a feedback input is not received, a “Pump Start-Stop Fail” alarm is generated. The positive running feedback is usually a contact from the associated starter for the motor; however, other options could be used such as the presence of flow on a flow meter, rise in pressure on discharge line, etc.

Also, operators have the option via the HMI graphic to place a pump “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the pump icon and it does not operate in remote modes. Furthermore, putting a pump out of service disables all alarms associated with it. Putting a pump out of service does not issue an alarm.

Table B9-14 Pump Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Pump Overload Trip	5 seconds	300
IO Discrete	Pump Motor Hot Winding	5 seconds	300
IO Discrete	Pump Emergency Stop Activated	5 seconds	300
IO Discrete	Pump Not in Remote	5 seconds	400
PLC	Pump Run Disable	0 seconds	200
PLC	Pump Starts Exceeded	5 seconds	300
PLC	Pump Start-Stop Fail	15 seconds	200

B9.3 Specialty Pump Alarm Design

Some pump types and motor connections require additional protective instrumentation. This additional instrumentation is usually required by the pump manufacturer to safely operate their product along with maintaining warranties. As the designer discusses the operation of the pumping system, protective items must be discussed with the manufacturer and process engineer. Some commonly manufacturer requested instruments are listed in Table B9-2 below. For analog transmitters, refer to the Continuous Instrument section for details on alarms.

B9.3.1 Vibration Monitoring

Pumps with long shaft connections to the motor (e.g. Vertical Turbine), vibration becomes an issue. Small vibrations can quickly resonate and lead to shaft bending or bearing destruction. The designer shall specify vibration sensors in locations recommended by the pump manufacturer. These sensors shall connect back to the PLC. Maximum vibration levels shall be provided by the manufacturer and PLC logic implemented to issue warning alarms. If there is a high probability of excessive impeller wear, vibration sensors on the pump casing may be used to provide early warning of impeller decay. Unless it is a large pump, usually in 600 HP and larger arena, the cost of operating and maintaining this sensor does not equate to the benefit of early warning.

B9.3.2 Bearing Temperature

Pumps with longer shafts, bearings are required to hold the shaft in place. If the shaft becomes bent, out of alignment, or the bearing starts to fail; the temperature of the bearing will rise. The use of bearing temperature RTDs allows Operations and Maintenance to see a failure coming and provide preventative remedies prior to a catastrophic failure. The RTDs would be connected back to the PLC using a specialty

module, refer to PLC Equipment Standard. Using the maximum temperature levels provided by the bearing manufacturer, PLC logic is implemented to issue warning alarms.

B9.3.3 Pressure Sensing

A major destructive force to pumps is cavitation. The onset of cavitation can be monitored using pressure sensors on the suction and discharge lines of the pump. If the net pump suction head is too low, cavitation can occur. Utilizing the minimum NPSH levels provided by the pump manufacturer, PLC logic is implemented to issue low suction pressure warning alarms along with shutting the pump down if necessary. The discharge pressure sensor reading can be used to show there is a plug in the line or a closed valve. For positive displacement pumps, High Discharge pressure should be monitored since these types of pumps can continue pumping and damage piping if not shutdown on high pressure. Consult the manufacturer for specific pressure ranges.

These sensors can be either pressure switches and/or pressure transmitters. The pressure sensors are connected back to the motor starter and the PLC. PLC logic is implemented to issue pressure warning alarms along with shutting the pump down if necessary.

B9.3.4 Seal Water Monitoring

Some pumps require Seal water for their seals. The seal water is required to prevent the shaft and seal from overheating and for lubrication. Without the seal water, the shaft can heat up causing deformation or seal failure. There are two common ways to monitor the seal water system on a pump; flow switch, pressure switch. For systems that have continuous seal water flow, a pressure switch is used to monitor the presence of water at the pump location. For systems where the seal water is only turned on when the pump is in operation, a flow switch between the shutoff solenoid and the pump location monitors water flow to the seal. The pressure/flow switch is hardwired to the starter and the PLC. Both the starter and the PLC will call for the pump to stop if the pressure/flow switch drops out.

Table B9-15 Specialty Pump Alarms

IO Type	Description	Delay	Priority
IO Discrete	Pump High Vibration Warning	5 seconds	200
IO Discrete	Pump High Vibration Shutdown	0 seconds	100
IO Discrete	Pump Seal Water Low Flow	0 seconds	100
IO Discrete	Pump Seal Water Low Pressure	5 seconds	300
IO REAL	Pump Bearing Temperature	5 seconds	300
IO REAL	Pump Suction Pressure Low	5 seconds	300
IO REAL	Pump Discharge Pressure High	5 seconds	300

B10 PUMP (SUBMERSIBLE)

B10.1 Introduction

City of Tulsa wastewater treatment process uses submersible pumps in different applications: in transferring raw wastewater, in primary and secondary sludge processes, in effluent pumping application, in grinding solid wastes, or in sump to handle discharge, etc. Submersible pumps are not amenable to frequent visual inspection; therefore, pump and motor alarms are essential. Besides field instrumentation sensors that input alarm signals to protect the pump and motor, submersible pump manufacturers suggest alarms that the design engineer must consider. These include moisture detection, pump internal heat monitoring, etc.

B10.2 Standard Pump Alarm Design

An engineer shall design an alarm system that will protect the pump and motor combination. For the drive motor, this alarm system shall contain, at a minimum, the alarms listed below in Table B10-1. The alarm system consists of hardwired starter controls, hardwired inputs to the PLC and PLC logically generated alarms. The alarm notifications to Operations will occur after a desired delay, programmed in the PLC, based on priority and possible damage to equipment or personnel. The alarm priority will determine how the HMI displays and where. See sections for other Process Equipment (i.e. Non-Submersible Pump Alarm Design). Due to the submersed installation, the pump normally has sealed in oil-filled cavities that are protected from contact with the transfer process liquids. These submersible pumps are not intended for frequent visual inspection; thus, they are normally built with typical sensors/signals within such as moisture sensor, internal heat monitoring, and seal leakage monitoring.

B10.2.1 Hardwire Alarms

A motor starter (ACL, RVSS or VFD) is provided to turn on/off the pump, and/or control the speed as needed by the process. Internal to a starter are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. A “Pump Overload Trip” input to the PLC from the overloads will turn off the pump and lock it out from starting and requires a manual Reset.

The motor has integral thermo-switches that provide feedback for winding temperature. This input shall be monitored by both the starter and the PLC. If a “Pump Motor Hot Winding” alarm is received, both the starter and the PLC will immediately call for the unit to stop and lock out the blower. The thermo-switches open on high temperature and will automatically close again when the motor cools below the switch setpoint thus allowing the blower to be restarted.

Moisture sensors are used to detect water in the sealed oil chamber. A probe type sensor is typically used for oil-filled seal chambers and is located in the seal chamber and electrically insulated from the pump housing. The resistance between two probes or between the probe and pump housing is being monitored. A “Pump Seal Leak Detection” alarm is generated when the probe detects a change in resistance caused by differing liquids entering the seal cavity and diluting the oil. The sensor is connected back to the PLC and SCADA system, and the alarm allows operations or maintenance to provide the necessary maintenance.

The ability to quickly stop the pump under an emergency is needed to protect the asset and personnel. The use of an Emergency Stop Pushbutton provides this quick stop capability immediately next to the equipment where a full disconnect may not fit. An “Emergency Stop Activated” alarm is generated when the emergency stop pushbutton is pressed. The pushbutton is hardwired to the starter and the PLC. Both the starter and the PLC will call for the pump to stop immediately and be locked out until the pushbutton is reset.

Another pump alarm is the “Pump Not in Remote”. Since the pump is normally controlled via the PLC, if the Local-Off-Remote switch at the local control station is not in the Remote position this alarm is generated.

Note: If a VFD or RVSS is used in lieu of an across the line starter to control the pump, additional alarms specific to those controllers are not discussed here. Refer to the VFD and RVSS sections for a detailed discussion of these additional alarms.

B10.2.2 Software Alarms

There are alarms associated with the operational sequence of the pump and are generated in the PLC.

The “Pump Run Disable” alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

A “Pump Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. Subsequent starts that occur prior to a cool off period can lead to winding temperature trips and life span shortening from insulation decay. The designer must coordinate with the motor manufacturer to determine what maximum value this can be.

Another sequential alarm is issued when the pump does not start or stop based on commands from the SCADA system. If the SCADA systems requests the pump to either Start or Stop and a feedback input is not received, a “Pump Start-Stop Fail” alarm is generated. The positive running feedback is usually a contact from the associated starter for the motor; however, other options could be used such as the presence of flow on a flow meter, rise in pressure on discharge line, etc.

Also, operators have the option via the HMI graphic to place a pump “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the pump icon and it does not operate in remote modes. Furthermore, putting a pump out of service disables all alarms associated with it. Putting a pump out of service does not issue an alarm.

Table B10-16 Pump Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Pump Overload Trip	5 seconds	300
IO Discrete	Pump Hot Motor Winding	5 seconds	300
IO Discrete	Pump Seal Leak Detection	5 seconds	300
IO Discrete	Emergency Stop Activated	5 seconds	300
IO Discrete	Pump Not in Remote	5 seconds	400
PLC	Pump Run Disabled	0 seconds	200
PLC	Pump Starts Exceeded	5 starts/hour	300
PLC	Pump Start-Stop Fail	15 seconds	200

B10.3 Specialty Pump Alarm Design

Submersible pumps may require additional protective instrumentation. These additional instruments are usually required by the pump manufacturer to safely operate their product along with maintaining warranties. As the designer discusses the operation of the pumping system, protective items must be discussed with the manufacturer and process engineer. Some commonly manufacturer requested instruments are listed in Table B10-2 below.

B10.3.1 Pressure Sensing

A major destructive force to pumps is cavitation. The onset of cavitation can be monitored using pressure sensors on the discharge lines of the pump and the pressure of the liquid submersed in. If the net pump suction head is too low, cavitation can occur. The pressure sensor would be connected back to the PLC. Utilizing the minimum NPSH levels provided by the pump manufacturer, PLC logic is implemented to issue low suction pressure warning alarms along with shutting the pump down if necessary. The discharge pressure sensor reading can be used to show there is a plug in the line or a closed valve. PLC logic would take the pressure reading and issue an alarm of high pressure. Refer to the Continuous Instrument section for details on the alarms associated with analog instruments.

Table B10-17 Specialty Pump Alarms

IO Type	Description	Delay	Priority
IO REAL	Suction Pressure Low	5 seconds	300
IO REAL	Discharge Pressure High	5 seconds	300

B11 REDUCED-VOLTAGE SOFT STARTERS

B11.1 Introduction

The City of Tulsa wastewater treatment process uses motors to drive blowers, pumps, compressors, conveyors, etc. Where process applications don't need variable speed control, plant power has limitations on its line power, or the process does not like large changes; the use of a Reduced-Voltage Soft Starter (RVSS) is a solution to the motor and its driven equipment. A Reduced Voltage Soft Starter is a motor controller which reduces the voltage to limit the current inrush on startup. Its capability is not only to turn on/off the motor, but also provide smooth of the process. Besides field instrumentation sensors that input alarm signals to protect the motor, the RVSS has its own alarm signals and the design engineer should include these alarms. Alarm signals are varying between RVSS manufacturers, this section describes typical RVSS alarm signals.

B11.2 Standard Reduced-Voltage Soft Starter Alarm Design

The engineer shall design an alarm system that will protect the motor, the process equipment, motor and starter/controller. The design engineer should design two distinct alarm systems: (1) Alarms associated with the RVSS, which are provided by soft starter manufacturer. This alarm system shall contain, at a minimum, the alarms listed in Table B11-1. The alarm system consists of a combination of hardwired RVSS controls, hardwired inputs to the PLC, PLC logically generated alarms, and ethernet communication. (2) Alarms associated with the motor and process equipment driven by motor. See sections for other Process Equipment (i.e. Non-Submersible Pump Alarm Design).

B11.2.1 Hardwire Alarms

In most applications, the RVSS interacts with process control signals through the PLC and is monitored on the SCADA graphical interface.

Internal to a RVSS are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. An "Overload Trip" input to the PLC from the overloads will turn off the motor and lock it out from starting and requires a manual Reset.

The RVSS monitors its internal electronics for any abnormalities. If it detects any malfunction a "RVSS Fault" alarm is generated. This alarm is wired to the PLC and requires a manual Reset at the RVSS before the motor can be restarted.

RVSSes equipped with a Hand-Off-Remote (HOR) switch, and the switch is in "REMOTE" position, this indicates to operators that the RVSS is controllable remotely from the PLC. If the PLC sees that the HOR switch is not in "REMOTE", an alarm signal is generated and is sent to the SCADA network.

B11.2.2 Software Alarms

There are alarms associated with the operational sequence of the pump and are generated in the PLC.

RVSSes equipped with a Hand-Off-Remote (HOR) switch, and the switch is in "REMOTE" position, this indicates to operators that the RVSS is controllable remotely from the PLC. If the PLC sees that the HOR switch is not in "REMOTE", an alarm signal is generated and is sent to the SCADA network.

The “Motor Run Disable” alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

A “Motor Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. Subsequent starts that occur prior to a cool off period can lead to winding temperature trips and life span shortening from insulation decay. The designer must coordinate with the motor manufacturer to determine what maximum value this can be.

Another sequential alarm is issued when the pump does not start or stop based on commands from the SCADA system. If the SCADA systems requests the pump to either Start or Stop and a feedback input is not received, a “RVSS Start-Stop Fail” alarm is generated. The positive running feedback is usually a contact from the associated starter for the motor; however, other options could be used such as the presence of flow on a flow meter, rise in pressure on discharge line, etc.

Also, operators have the option via the HMI graphic to place a pump or other equipment driven by an RVSS “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the equipment icon and it does not operate in remote modes. Furthermore, putting the equipment out of service disables all alarms associated with it. Putting an equipment out of service does not issue an alarm.

Table B11-18 RVSS Minimum Alarms

IO Type	Description	Delay	Priority
IO Discrete	Overload Trip	5 seconds	300
IO Discrete	RVSS Fault	5 seconds	300
IO Discrete	RVSS Trouble	5 seconds	300
IO Discrete	RVSS Not in Remote	5 seconds	400
PLC	Motor Run Disable	0 seconds	200
PLC	Motor Starts Exceeded	5 starts/hour	300
PLC	RVSS Start-Stop Fail	12 seconds	200

B11.3 Specialty Reduced-Voltage Soft Starter Alarm Design

The use of Ethernet communication and hardwired I/O gives the operator a convenient way of to obtain information about the RVSS, such as drive full load amps, drive torque values, drive energy consumption, etc. When these parameters are out of their set ranges, alarms are generated.

B11.3.1 RVSS Communications Failure

If the RVSS uses a network communications connection such as Ethernet, then this link should be monitored. A “RVSS Communications Fail “alarm is generated when network communications (e.g. Ethernet) is disrupted for a short time period between the RVSS and the PLC. Typically, a “Watch-dog” timer is programmed in the PLC which the equipment periodically resets to ensure that communications is operational. If the comms link is down and the watch-dog timer times out an alarm is generated.

B11.3.2 Ground Fault

Ground fault common causes are motor power cables shorted to ground and/or motor windings shorted to ground. Over time motor power cable insulation can breakdown causing the cable to short to ground. Similarly, when motor winding insulation degrades enough that the windings short to the motor ground.

When either of these conditions occur a “RVSS Ground Fault” alarm is generated. The alarm is wired to the PLC and displayed at the SCADA system.

B11.3.3 Torque Out of Range

The soft starter is not a speed controller, it only controls the torque. By reducing starting voltage and current during startup, sufficient torque is provided to get the motor in operation and then accelerate to desirable speed or decelerate speed to stop. When drive torque values are out of set ranges, a “RVSS alarm is generated. The alarm is wired to the PLC and displayed at the SCADA system.

B11.3.4 Input Phase Loss

The 3-phase input power is monitored by the RVSS. If a phase is completely lost due to a loose connection or a fuse is blown, or a significant current imbalance occurs between phases, a “RVSS Input Phase Loss” alarm is generated. The alarm is wired to the PLC and displayed at the SCADA system.

Table B11-19 Specialty RVSS Alarms

IO Type	Description	Delay	Priority
Ethernet	RVSS Communication Fail	5 seconds	200
IO Discrete/Ethernet	RVSS Ground Fault	0 seconds	300
IO Discrete/Ethernet	RVSS Torque Out of Range	0 seconds	200
IO Discrete/Ethernet	RVSS Input Phase Loss	0 seconds	100

B12 VARIABLE-FREQUENCY DRIVES

B12.1 Introduction

The City of Tulsa wastewater treatment process uses motors to drive blowers, pumps, mixers, etc. The speeds of these equipment, as designed per process, may be varied. Starting, stopping, ramping up or down a motor too frequently subjects the motor to high mechanical and electrical stresses, shock damage, stress on the insulation, and long-term wear on the motor. The use of variable-frequency drives (VFD) provide a gradual smooth ramping up of the motor instead of instant energization by full voltage starters reducing mechanical stresses, prolonging the motor’s lifespan. Besides field instrumentation sensors that input alarm signals to protect the motor, VFDs have their own alarm signals the design engineer should include in their alarm and protective scheme. Alarm signals vary between VFD manufacturers, this section describes typical VFD alarm signals.

B12.2 Standard Variable-Frequency Drive Alarm Design

An engineer shall design a VFD alarm system that will protect the VFD, the motor, and the process equipment that are driven by the motor-VFD combination. The design engineer should design two distinct alarm systems: (1) Alarms associated with VFD, provided by drive manufacturer. This alarm system shall contain, at a minimum, the alarms listed in Table B12-1. The alarm system consists of a combination of hardwired VFD controls, hardwired inputs to the PLC, PLC logically generated alarms, and ethernet communication. (2) Alarms associated with the motor and its driven process equipment. See sections for other Process Equipment (ex. Non-Submersible Pump Alarm Design).

B12.2.1 Hardwire Alarms

The variable frequency drive acts as a motor starter. Its capability is not only to turn on/off the motor, but also control the speed of the motor as desired by the process. In most applications, the VFD interacts

with process control signals through the PLC, is monitored on the SCADA graphical interface, and these signals may be shown on the VFD control human machine interface (HMI) displaying its status.

Internal to a VFD are current overloads. These overloads protect the motor from sustained over current, not including a short circuit. An “Overload Trip” input to the PLC from the overloads will turn off the motor and lock it out from starting and requires a manual Reset.

The VFD monitors its’ internal electronics for any abnormalities. If it detects any malfunction a “VFD Fault” alarm is generated. This alarm is wired to the PLC and requires a manual Reset at the VFD before the motor can be restarted.

Process loads are typically equipped with a Hand-Off-Auto (HOA) switch that is used to determine the equipment operation location. When switch is in “HAND” position, the VFD is controlled by an operator input, bypassing the control of the SCADA network. When the switch is in “OFF” position, the VFD is still energized but control is disabled. When the switch is in “AUTO” position, the VFD is controlled based on a set of process conditions. A “VFD Starter Trouble” alarm is generated when the switch is not in the “AUTO” position or the drive “Ready” is not present.

B12.2.2 Software Alarms

There are alarms associated with the operational sequence of the pump and are generated in the PLC.

In a process where precision motor speed is important, the VFD can monitor speed. The VFD measures the speed of the motor and sends the signal to the PLC for proportional-integral-derivative (PID) loop controls to maintain motor speed per process requirements. If VFD speed feedback is not within an operator set deadband around the desired speed a “VFD Speed Feedback Fail” alarm is generated.

VFDs equipped with a Hand-Off-Remote (HOR) switch, and the switch is in “REMOTE” position, this indicates to operators that the VFD is controllable remotely from the PLC. If the PLC sees that the HOR switch is not in “REMOTE”, an alarm signal is generated and is sent to the SCADA network.

The “Motor Run Disable” alarm is generated when there is an alarm that shuts down and locks out the motor and notifies the operator that a manual Reset is required before the motor can be restarted.

A “Motor Starts Exceeded” alarm is generated when the number of starts a motor can perform within an hour is exceeded. These starts can either be in HAND mode or REMOTE mode. The higher the horsepower, the less starts per hour allowed before heat damage can occur. Subsequent starts that occur prior to a cool off period can lead to winding temperature trips and life span shortening from insulation decay. The designer must coordinate with the motor manufacturer to determine what maximum value this can be.

Another sequential alarm is issued when the motor does not start or stop based on commands from the SCADA system. If the SCADA systems requests the motor to either Start or Stop and a feedback input is not received, a “VFD Start-Stop Fail” alarm is generated. The positive running feedback is usually a contact from the associated VFD for the motor; however, other options could be used such as the presence of flow on a flow meter, rise in pressure on discharge line, etc.

Also, operators have the option via the HMI graphic to place a pump or other equipment driven by an VFD “Out-of-Service”. A visual “OOS” tag appears on the HMI graphic next to the equipment icon and it does not operate in remote modes. Furthermore, putting the equipment out of service disables all alarms associated with it. Putting an equipment out of service does not issue an alarm.

Table B12-20 VFD Minimum Alarms

IO Type	Description	Delay	Priority

IO Discrete	Overload Trip	5 seconds	300
IO Discrete	VFD Fault	5 seconds	300
IO Discrete	VFD Trouble	5 seconds	300
PLC	VFD Speed Feedback Fail	60 seconds	400
PLC	VFD Not in Remote	5 seconds	400
PLC	Motor Run Disable	0 seconds	200
PLC	Motor Starts Exceeded	5 starts/hour	300
PLC	VFD Start-Stop Fail	15 seconds	200

B12.3 Specialty Variable-Frequency Drive Alarm Design

The use of Ethernet communication and hardwired I/O give the operator a convenient way of obtaining additional information about the VFD, such as the drive full load amps, the drive torque values, the drive energy consumption, the drive speed, etc. When these parameters are out of their set ranges, alarms are generated.

B12.3.1 VFD Communications Failure

If the VFD uses a network communications connection such as Ethernet, then this link should be monitored. A “VFD Communications Fail “alarm is generated when network communications (e.g. Ethernet) is disrupted for a short time period between the VFD and the PLC. Typically, a “Watch-dog” timer is programmed in the PLC which the equipment periodically resets to ensure that communications is operational. If the comms link is down and the watch-dog timer times out an alarm is generated.

B12.3.2 Ground Fault

Common causes for Ground fault are motor power cables shorted to ground and/or motor windings shorted to ground. When motor power cables’ insulation breaks down, eventually that cable will short to ground, and an alarm generated. Similarly, when motor winding insulation degrades enough that the windings short to the motor ground, an alarm is generated. The alarms are acknowledged and shown on VFD’s HIM.

B12.3.3 Overvoltage

The most common time a VFD overvoltage fault occurs is during deceleration. When a process requires VFD and motor to decelerate rapidly, the motor operates as a generator. The motor regenerates power, which feeds back into the drive and stored on the DC bus. This fault should generate an alarm. During normal operation, VFD overvoltage faults occur when the output load has a clutch that could cause a sudden drop in load, the motor speed may increase quickly, causing a regenerative load. This fault should generate an alarm. In both cases, the alarms are acknowledged and shown in VFD’s HIM.

B12.3.4 Input Phase Loss

Input phase loss is also known as undervoltage. When power line voltages are imbalanced because one phase is lost by a loose connection, a fuse blown, or more seriously a line-to-line or line-to-ground faults. In all cases, an alarm is generated. Current on input power lines should also be monitored. Should an imbalance in current between the three input lines while the VFD is running, an alarm is generated. These two fault alarms could be combined in one alarm signal and sent to the plant PLC.

Table B12-21 Specialty VFD Alarms

IO Type	Description	Delay	Priority
Ethernet	VFD Communications Fail	5 seconds	200
IO Discrete/Ethernet	Ground Fault	0 seconds	300
IO Discrete/Ethernet	Overvoltage	0 seconds	300
IO Discrete/Ethernet	Input Phase Loss Fault	0 seconds	300