.2 Clear English language description of the control philosophy (final PLD).

.3 Details describing how the control philosophy has been implemented in the programming. This shall take the form of detailed control descriptions combining both text and detailed flow charts in order to clearly define how each device is controlled.

.4 Each manual shall include an index listing its contents.

.5 Cross referencing shall be provided between code and the control description such that a reasonable knowledgeable programmer shall be able to quickly refer to the documentation and complete whatever revisions the plant staff requests.

.6 Clear identification of all configuration information that is different from the default values set by the manufacturer in order to allow staff to quickly reconfigure the system.

.7 Details describing how all functionality described within the documents has been implemented.

.8 A description of the system physical layout (System Architecture).

.9 Network Diagrams.

.10 Database Schematic Diagrams.

.11 A description of the systems standards and procedures (System Conventions).

.12 A description of the systems links to other systems and links between applications forming part of the primary system (System Links).

.13 A summary of the steps necessary to maintain the system describing all regular routines such as adding a new operator, checking the system, routine system maintenance, disk management, data management, checking back-ups, monitoring resources, etc.(System Administrative Checklists).

.14 A list of tools required to reorganize, optimize, restore and maintain the system, component parts thereof, and application data stored on the system.

.7 Mission Critical Plan:

.1 The Mission Critical Plan shall provide detailed information regarding how to recover the system after a catastrophic failure. As a minimum, the plant shall provide a list of steps necessary to recover from possible disasters including, but not limited to, OIS failure, power interruptions, data corruption, data loss, communication link outages and data server destruction.

1.5 Programming Documentation

.1 All programming shall be internally documented with every block of code commented, describing the function of the block. In addition, PLC programming shall make effective use of nicknames for every data point used in the program and shall provide detailed descriptions of the significance of each point. Nicknames shall be consistent with the tag naming convention. The description shall include the associate device field identification code where applicable and description as to the significance of the value.

.2 Every section of the control logic shall contain a reference to the control philosophy. Sequential function charts will be generated for each system. An abbreviated control philosophy shall be included in the header comment of each program function block/ladder function block.

1.6 Electronic Documentation

.1 The final application, along with all documentation, shall be provided on CD-ROM for archival purposes.

PART 2 - PRODUCTS

2.1 Target Architecture

.1 Performance:

.1 The performance requirements of the control system are:

Item	Minimum Response
Graphic Screen Updates	Graphics, with all dynamic data, must be displayed within 3 seconds after request is issued; Display update response must be under 2 seconds; Field response to operator commands must be under 2 seconds.
Alarm Response	Local alarms must be reported within 2 seconds.

.2 SCADA Functions:

.1 The primary operator window for viewing and controlling processes will be the SCADA operator computers. A view node is to be provided.

.3 Data Historian:

.1 Historical alarm logs, trend data, operator actions, etc., will be recorded in a database. This information will be used to generate scheduled and ad-hoc reports and will be available to a wide spectrum of users.

.4 PLC Functions:

.1 The PLC shall perform the following functions:

.1 Accept and store field data from field devices.

.2 Control operation of all equipment (for example, pumps, valves).

.3 Run-time accumulation for equipment with periodic runtimes such as: motors, generators, pumps and filters.

.4 Start/stop frequency counts for equipment with intermittent duty cycles such as: motors, generators and pumps.

.5 Flow and chemical use accumulators.

.6 Critical alarm detection and annunciation (Plant Alarm Horn).

.7 Equipment sequencing based on duty cycle, failure, operator request, time of day, etc.

.8 Monitor and report field conditions.

.9 Provide automated control for systems (e.g., D.O. based Blower Control).

.10 Monitor breakers (where provision for mechanical lockouts are required at the field device).

.11 Provide equipment control interlocks.

.12 Interface plant to SCADA operator interface.

.5 PLC/SCADA Communication:

.1 The communication between the PLC and the SCADA operator interface shall utilize a Data Highway Plus communication link.

.2 All writes to the PLC shall be directly from corresponding control coils and/or registers. Writes shall not be made to the same registers as values are read from.

.3 Tags for totalizers and other fields that change on an infrequent basis may be scanned at slower rates to optimize performance.

.4 The communications link shall be monitored by a loop back heartbeat. The SCADA system shall increment a register in the PLC, the PLC shall move the value to a second register, the SCADA system shall read the value back, and then in turn increment the value. Communications shall be verified by confirming the entire process is fully functional.

2.2 Design Guidelines

.1 Engineering Units:

.1 Standard Engineering units are to be metric. Unless otherwise specified, the following guidelines shall be used:

Unit	Description of Use
mL/d	Plant Flow/Plant Capacity
L/s	Chemical Feed Rates
mg/L	Chemical Dosage/Residual Analysis
kg/d	Chemical Usage (Dry Compounds Dry Equivalent)
kPa	Pressure

m^3	Volume
kV	Voltage
A	Amperage
kW	Power

.2 If additional units are required, the System Integrator shall request in writing that the Engineer add additional units to the list, otherwise all units shall comply with the guidelines.

.2 Security:

.1 System security shall be implemented using individual user passwords for access to the operating system and to the SCADA system control functions.

.2 Unless the user has appropriate security clearance for access to the operating system, the graphical environments control bar and menu box shall be disabled.

.3 Passwords shall be entered by the user calling up a pop-up window by pressing a function key.

.4 Each user shall be provided with an individual unique password.

.5 It shall not be possible to modify the systems configuration without being logged with sufficient security clearance.

.6 Five distinct system security levels shall be provided as follows:

.1 Developer/System Administrator - has authority to modify the system, change security, etc.

.2 Manager/Supervisor - highest level of operating control. Has control of all operating parameters plus the ability to add operators and change passwords.

.3 Sr. Operator - has a more limited access to control functions. Has ability to change setpoints and alarms within span of control.

.4 Operator - has limited span of control. Can change only a specific group of setpoints and alarms in addition to starting and stopping of equipment, changing duty queues and other routine operational activities.

.5 Guest - View Only. No control of the process or access to the operating system. Access to view certain control screens may be restricted.

.7 Users shall be able to change their own passwords at any time by entering their current password followed by the new password they wish to use. The system shall not display the password when typed, but shall require the user to re-enter the new password to confirm that a typing error did not occur before accepting the change. The change in password shall be replicated to all nodes on the network.

.S If an operator incorrectly enters their password more than 3 times in a five minute period, the system shall lock the account for a period of 30 minutes before allowing another attempt at logging in to that account and generate an alarm.

.9 If a node is not used for a pre-specified period of time, it shall automatically drop to guest level security and remain there until an individual logs on with a password providing additional privileges. A warning message will be posted before the system logs a user out providing a five-minute warning. The user will be provided the option to log in as a new user or delay log out for 15 minutes. The time-out period shall be definable on a node by node basis by Developers/System Administrators and

Managers/Supervisors without access to development tools. In addition, the system will log staff out at the end of shift.

.10 Only Developers/System Administrators and Managers/Supervisors shall be able to change the control functions, time outs and disable passwords.

2.3 Standard Device Control

.1 Standard Devices:

.1 Device control pop-up windows shall be used to display and maintain the following:

.1 Status.
.2 Mode.
.3 Number of running hours.
.4 Number of cycles (start/stop,open/close).
.5 Standard alarms and alarm state.

.2 Each device will have two registers - an equipment status register and an equipment alarm register. This approach minimizes the tag count required in the SCADA system and simplifies generation of the standard device library and simplifies generation of the generation and maintenance of the standard device library. The format of each register is as follows:

Equipment Status Register		Equipment Alarm Register	
Bit	Description	Bit	Description
0	Stopped/Closed	0	Failed to Start/Open
1	Running/Open	1	Failed to Stop/Close
2	Stopped/Closing	2	Over Current
3	Starting/Opening	3	Excessive Vibration
4	Alarm while running	4	Bearings Over Temperature
5	Alarm while stopped	5	Motor Over Temperature
6	Alarm while Unknown	6	High Pressure
7		7	Low Pressure
8	SCADA - Automatic	8	High Flow
9	SCADA - Semi-automatic	9	Low Flow
10	SCADA - Manual	10	High Level
11	Local - Automatic	11	Low Level
12	Local - Manual	12	High Temperature
13	Local - Maintenance	13	Low Temperature
14	Local - Lockout	14	
15		15	

.2 Operating Modes:

.1 If additional modes other than those listed are required for a specific process, the integrator shall request in writing a new mode and will describe why the new mode is required. If the Engineer agrees that the new mode is justified, the mode will be added, otherwise the integrator shall follow these guidelines.

.1 Modes:

.1 The following operating modes shall be supported at the SCADA level:

.1 SCADA - Automatic: In automatic mode, the PLC shall control the process and advise the operators of any deviations by way of alarms. Operator action will only be required to react to critical alarms or to clear warning alarms that require operator acknowledgement.

.2 SCADA - Semi-Automatic: In semi-automatic mode, the PLC shall control the sequence of operations but the operator is required to acknowledge each process step.

.3 SCADA - Manual: In manual mode, the operator has complete control over the system and will be able to start and stop individual pumps, open and close valves, etc. Normal interlocks shall apply.

.2 The following modes shall be supported at the device level:

.1 Local - Automatic: In automatic mode, the device is controlled by the PLC system.

.2 Local - Manual: In manual mode, the device is controlled locally using a manual (pushbutton) or local operator interface (HMI). In Local Mode, PLC interlocks are enabled. When a device or group of devices which are part of a process are in Local Mode, the system mode will revert to manual.

.3 Local - Maintenance: In Maintenance Mode, the device is controlled manually with interlocks disabled. When a device is in maintenance mode, system will not support automatic operation.

.4 Local - Lockout: When a device is in lockout mode, all system modes will be available. However, the specific piece of equipment will be disabled. If the system is in Automatic or Semi-automatic, the backup or alternate equipment will be automatically selected for use.

.3 Start-up and Power Failure:

.1 The system will not attempt to restore the plant to a state of operation until after power has been restored for a minimum of 5 minutes without operator intervention.

.2 The SCADA system will boot up and automatically initialize itself at a guest security level to represent the current state of the plant after any system interruption. It will be performed without the intervention of an operator.

.3 The PLC system will reset upon power failure to represent the current state of the plant after any system interruption. However, the PLC will not restart the plant without operator intervention (either local or remote).

.4 The control system will be maintained on-line during short-term power outages by the UPS. If the UPS has drained to below 25% capacity, the system will automatically shut down in an orderly fashion. All data in memory will be saved to disk, and all open files will be closed.

.4 Fault Tolerance and Recovery - SCADA:

.1 The failure of any portion of the system shall result in the posting of an alarm identifying the malfunctioning unit. If a Programmable Logic Controller fails, an alarm shall be sounded to warn operators of a potential for serious problems.

.2 In order to simplify the process of reinitializing the system upon replacement of failed hardware, a "boot disk" shall be provided that when loaded shall automatically reformat the hard drive, load appropriate restore software and reload the most recent system backup from tape, restoring the system should a failure occur. Before commencing on the reformatting, a warning message shall be posted and confirmation required by the operator. The operator shall be prompted to perform all actions that are not automated. The prompt shall describe the exact steps to be followed such that an individual with only limited computer knowledge can perform the restoration.

.3 The data collection nodes shall function in a redundant configuration such that the failure of a single unit will not result in the total system failing.

.4 Supervisory and operator interface nodes that are acquiring data from the SCADA data collection node that fails will automatically switch to acquiring data from the operational node once an operator acknowledges the failure at the interface node.

.5 The backup process will be server based and will be fully automatic requiring the system administrator to perform no action other than load the corresponding data cartridge(s). In addition to backing up all data for all nodes in the system, the backup process shall include backing up of all configuration information for the server and the database. The system shall automatically back up all information both on the server and all nodes on the network. The tape backup system shall be sized such that all data can be backed up on a daily basis to a single tape cartridge. The backup software shall automatically back up on-line databases in their entirety without interruption to the logging of new data into the database. The backup process will include backing up of all information to allow any node in the system (including all data on any node) to be recovered as easily as possible.

.6 Failure of either SCADA server or the network shall result in a message indicating "Out of Service" being displayed on all nodes which are unable to display accurate information.

.7 If the local network should fail, the SCADA system shall continue to function without interruption and without any loss of monitoring and control functions. On large projects, the database server will collect data via a direct connection to the control network.

.8 The SCADA software package will record key PLC information into a recipe archive upon senior operator request. Each "recipe" shall be named by the operator and shall be accessible by name. The operator shall be able to attach a user-defined description of up to 255 characters to each "recipe". On demand, an operator can restore these values to the PLC (i.e., setpoints, startup values, runtimes, number of starts, alarm setpoints, etc.). Thus, after failure and replacement of a PLC or under different operational conditions these values can be restores.

2.4 Operator Interface

.1 Graphical User Interfaces:

.1 Wherever appropriate, process graphics will be used to provide the operator with a window to view the status of the overall process and each piece of equipment. Overview graphics will be developed for each facility as well as detail process graphics for each major process.

.2 In general, screens shall be categorized as follows:

Category	Content
Overview	Overview of the entire system or map of the area
Area/Process Overview	Overview of an independent facility, area or process
Process Detail	Detail of a process or equipment grouping
Electrical/Power Overview	Overview schematic showing status of major breakers, etc.
Control Setpoints	Listing of all control setpoints and recipe control
Alarm Setpoints	Listing of all alarm setpoints and alarm control
Pop-up	Device settings

.3 On overview screens, details of process piping will only be displayed if it is critical to controlling the operation of the system. Detail screens will display all process piping and control devices.

.4 Clicking on a device will bring up a device pop-up window. This window will be used to control the device (start, stop), change operating parameters (Hi - Lo alarm setpoints), change status, etc. All control functions shall be initiated and confirmed using pop-ups.

.2 Configuration:

.1 All screen development shall be fully Windows compliant and make optimal use of pop up windows, scroll bars and push buttons.

.2 Dynamic dialogue box overlay pop-ups shall be used to allow operators to make changes to devices shown on the underlying screen. The pop-up box shall support keyboard data entry, mouse

pick boxes, and dynamic mouse scroll bars for selection of analog input values.

.3 Screens shall be configures such that analog values change colour to yellow to indicate that the value may no longer represent the value at the field device and a caution symbol shall appear beside devices automatically upon failure of communications with the Programmable Logic Controller. The quality of the signal shall be monitored using the software packages built in quality monitoring and a heartbeat between the PLC and the SCADA system. The heartbeat shall consist of a register in the PLC being incremented by the SCADA software package, moved by the PLC to another register, and then read back by the SCADA software. If the value fails to change for a period of 30 seconds, a communications failure will be assumed.

.4 The system shall define maximum and minimum allowable values for analog operator input as specified by the Engineer in consultation with the Systems Integrator.

.5 All field devices (e.g., motors, pumps), for which the display of run-times is deemed to be desirable by the Engineer, shall display run-times on the start-stop or sequencing pop-up control window used to control the device.

.3 Size and Resolution:

.1 All operator interface screens will be designed for 1024 x 768 resolution and shall exclusively incorporate scalable true-fonts for all text and numbers displayed.

.4 Screen Format:

.1 All screens will follow the following format:

PASTE UP SCADA MMI SCREEN LAYOUT

$end

.2 The screen display shall consist of three tiled windows. The top being reserved for controls (common), the centre being specific information (specific) and the bottom being the alarm banner (common). By designing the screen to consist of three tiled windows, it is subsequently possible to modify the common aspects by modifying a single window rather than having to modify each and every window.

.3 The top of the screen shall be used for common screen controls to toggle between functions and for status information (i.e., Alarm Acknowledgement with PLC).

.4 The bottom of each graphic screen shall display a four-line alarm banner and PLC communication status that displays the system's four most recent alarm condition occurrences. The alarms banner shall also be replaced with a pop-up for navigation by using a toggle switch in the controls segment of the screen.

.5 Device Symbols:

.1 All graphics will incorporate standard process graphic symbols (ISA) for common devices. The symbols will be drawn to be consistent with those found in the Process and Instrumentation Drawings. However, on screens they will be displayed as 3-D objects. This is not to be read as implying that the items are to be 3-D pictorials, but simply aesthetically enhanced ISA symbols.

.2 All objects shall be created in the form of graphic wizards. The library shall include all objects required to build the system described in the design documents. It shall be possible to build screens by inserting wizards from the library and specifying which tags to attach to each animation link. All wizards created shall become the property of the Engineer.

.6 Colour Coding:

.1 Devices or device indicators, as specified by the Engineer in consultation with the Systems Integrator, shall display:

.1 Slow flashing green when starting or opening.
.2 Green when running or open.

.3 Slow flashing red when stopping or closing.

.4 Red when closed or stopped.
.5 Rapid flashing when in alarm state.
.6 Dark gray until initial value is known.

.2 Transition states (starting and stopping) shall only be displayed if the transient condition exists for more than 2 seconds.

.3 The colour of all pipes shown on screens shall conform, where possible, to the fluid being transported. A table of colours will be provided by the Engineer during construction. Where deemed feasible and desirable by the Engineer, flow shall be indicated in pipes and conduits by a change in pipe colour from grey to the colour for the fluid being transported. Text stating pipe contents are to be shown adjacent to pipes along with arrows indicating the direction of flow.

.4 Where bar graphs are specified, the bar graph shall change colour based upon whether the associated analog value is in alarm state. Alarm levels shall be clearly indicated on the screen at all times, irrespective of whether or not the device is in alarm state. The colour of the bar while in the normal operating range shall be the colour described for the liquid being monitored, as per MOE Standards for pipe colours. While in alarm state, the bar graph shall flash.

.7 Settings:

.1 Screens shall be provided to facilitate the maintenance of major groups of setpoints. These will be accessed by the use of a "settings" button on device pop-ups and from the menus screen.

.8 Online Documentation:

.1 Context sensitive help text will be provided where appropriate. The operator will be provided online access to all the information contained within the Operations Manual. The Operations Manual will be written to facilitate context sensitive help. The manual will be written as a hypertext online document accessible from the SCADA system.

2.5 Alarm/Event Management

.1 Presentation:

.1 Alarms will be displayed in the alarm banner that comprises the bottom section of operator's screen. The four most recent alarms will be displayed at all times. The alarm banner shall record active alarms requiring acknowledgement in yellow, acknowledged alarms in red and unacknowledged alarms no longer in alarm state in blue. All alarms shall be displayed on a black background. The alarm banner shall indicate the date, time and description of the alarm condition. Acknowledgements shall indicate the name of the individual who acknowledged the alarm and time acknowledged.

.2 In addition, a separate full screen historical alarm window with scroll bars shall be provided. The historical alarm screen will display:

.1 Unacknowledged alarms in red.

.2 Acknowledged alarms in blue.

.3 Events in white.

.3 Critical alarms hall use the soundboard on the SCADA Operator Interface to annunciate the occurrence of an alarm. If acknowledgement is required, the alarm shall continue to sound until it is acknowledged.

.4 Critical alarms shall result in a pop-up window being displayed

describing the alarm condition and the significance of the alarm. To clear the pop-up window, an operator must click on an acknowledge button on the pop-up. In addition, a prerecorded message clearly stating in English the alarm condition shall sound until acknowledged.

.2 Classes:

.1 Alarms will be divided into the following classes:

.1 Critical Alarms: Critical Alarms are generated in situations where equipment or system failure will potentially impact safety or result in damage to the environment, property or equipment without immediate intervention.

.1 Class 1 - Plant Wide Alarms: Class 1 Alarms will be displayed immediately on the operator's display and will trigger a plant wide audible and visual alarm and dial up off site maintenance personnel. Class 1 Alarms must be acknowledged by the operator either via the SCADA system or via hardwired "PLC" acknowledge. Both methods of acknowledgement shall be provided. The alarm condition must be corrected and cleared before normal operation resumes. Critical Class 1 alarms cannot be disabled by an operator. True Class 1 alarms will function irrespective as to the status of the SCADA system.

.2 Class 2 - Local Alarms: Critical Class 2 Alarms are similar to Class 1 but the impact is localized and not relevant when the SCADA system is not operational. Critical Class 2 Alarms will display immediately on the operator's display and will trigger a local visual alarm. Critical Class 2 Alarms that are not cleared within 15 minutes are automatically elevated to Pseudo Class 1 (plant wide) status. Class 2 Alarms must be acknowledged by the operator. Certain Critical Class 2 alarms may be disabled by an operator. The Engineer shall decide which Critical Class 2 Alarms can be disabled.

.2 Warning Alarms: Warning alarms do not stop operations. There is no audible annunciation for warning alarms. Warning alarms notify the operator of non-critical situations (i.e., warning the operator that a low or high level tank limit has been exceeded and action may be required). All warning alarms will be displayed.

.1 Acknowledgement Required: Operator acknowledgement is required to clear this class of alarm.

.2 Self-Clearing: Self-clearing warning alarms may be acknowledged. However, they will clear automatically once the alarming condition ceases to exist.

.3 Events (Information Only): Event alarms issued to record useful information about the normal operation of the system (i.e., the start and completion of a filter backwash). Events will be logged but will not appear in the alarm banner. Events are subdivided into two classes: Compliance events that record data necessary to comply with Health and Safety or environmental issues associated with the site's operating license, and all other.

.2 When an alarm is acknowledged on one system, the alarm will be acknowledged on all systems.

.3 Communication alarms and any remote alarms that may be attributed to communications failure shall be masked for 2 minutes to allow the system to attempt to re-establish communications before sounding the alarm. However, loss of communication will immediately display on the communications monitor.

.3 Sources:

.1 PLC:

.1 All critical alarm conditions shall originate in the PLC control systems.

.2 Discrete Alarms:

.1 These digital alarms are generated in the Programmable Logic Controller and remain in alarm state in the SCADA system until acknowledged. If self-clearing, it is critical that the alarm condition is held in alarm state long enough for the SCADA system to log the alarm.

.2 Alarms generated by the PLC will be determined using the following guidelines:

.1 All devices with output and input status will generate a device alarm when there is conflict between the output and the input status. For example, if a valve is closed, the limit switch on the valve must indicate closed, otherwise a "valve fault" alarm will be issued.

.2 Any abnormal, hazardous or undesirable condition must generate an alarm identifying the condition.

.3 PLC operation and communications will be alarmed to detect:

.1 Rack faults
.2 Low battery
.3 Loss of communications.

.3 Analog Alarms:

.1 All Hi-Hi - Lo-Lo analog alarms shall originate from the PLC.

.2 Trigger levels/dead shall be generated either from the device controller or derived in the PLC for all analog alarms that can be configured. Configuration of PLC alarms shall be from the SCADA and shall only be possible when someone with Developer/System Administrator clearance is logged in. Discrete alarm points will exist in the PLC for all PLC based analog alarms.

.2 SCADA:

.1 Logical Alarms:

.1 Logical Alarms shall be generated by the SCADA system based upon the described logical conditions. The alarms shall remain on the screen until the actual alarm condition is cleared in the field. Typical SCADA Logical Alarms include:

.1 SCADA System disconnected from PLC
.2 Network not working.

.2 SPC alarms shall also originate in the SCADA system.

.2 Analog Alarms:

.1 Hi and Lo operator status alarms shall be programmed in the SCADA system. These alarms require Hi-Hi and Lo-Lo alarms to exist in the PLC. In order to change the alarm limits and deadbands a user must be logged into the system with operator level or higher security clearance. The system shall restrict the level at which these alarms can be set to within the range defined by the Hi-Hi and Lo-Lo alarm limits. These alarms are intended to allow

operators to fine tune processes and are not to be used for alarm limits which warn against possible equipment damage or unsafe operating conditions.

.4 Run Time Alarm Control:

.1 Supervisors/Administrators will, at any time, be able to enable/disable the sound on their local node without affecting other nodes on the network. this must be accomplished without stopping the operation of the SCADA software or affecting any other node on the network. This functionality will not be accessible to individuals with lower level security clearances.

.2 Operators will be able to adjust volume levels for alarms separately for both for the control nodes and the plant wide alarm horns from the SCADA system to one of three predefined levels (quiet, normal and loud). These levels shall be defined and adjustable at any time by persons with Supervisory/Administrator security clearance.

.3 Operators will be able to lock in alarm state alarms specified to have "lock" functionality by the Engineer, at run-time from an "Alarm Control" screen such that the alarm continues to display on the screen as active, irrespective of the actual alarm condition in the field. When alarms have been locked, all screens shall display a warning that alarms have been locked.

.4 Operators shall be able to change alarm high/low limits for alarms specified to have this functionality by the Engineer. Alarm limits are adjusted at runtime from an "Alarm Control" screen such that the alarm continues to display on the screen as active irrespective of the actual alarm condition in the field.

.5 Operators will be able to disable alarms specified to have "disable" functionality by the Engineer. Alarms are disabled at run-time from the "Alarm Control" screen such that the alarm will not be triggered irrespective of the actual alarm condition in the field. When alarms have been disabled, all screens shall display a warning that alarms have been disabled.

.6 Operators will be able to lock alarms specified to have "lock" functionality by the Engineer. Alarms are held at run-time in alarm state from the "Alarm Control" screen such that the alarm will remain in alarm state irrespective of the actual alarm condition in the field. When alarms have been locked, the alarm banner and alarm screen shall display a warning that alarms have been locked.

.7 Certain alarms will be logged to the database historian. The historian will allow the alarm history to be queried to locate all occurrences of the alarm, the time duration the alarm was in alarm state over any operator definable period, and the number of times the alarm entered alarm state over any given alarm period. Operators will be able to disable the logging of alarms specified to have the alarm log disable functionality by the Engineer.

.8 The definition for each alarm shall be as per the "Alarm Data" table in Section 2 of the Process Logic Description.

.5 Logging:

.1 The local alarm log shall be maintained for a period of 45 days. The system shall automatically erase historical alarm data older than 45 days.

.2 In addition to alarms, the system logger shall also be configured to log status events. Their occurrence shall not require acknowledgement nor shall the events sound an audible alarm. In addition, these events shall not display on the alarm banner. However, shall be viewable on the historical alarm log in white. The alarm log shall indicate the date, time and description of the status event.

.3 In addition to alarms and events, the system logger shall also be configured to log operator inputs. Their occurrence shall not require acknowledgement nor shall the input sound an audible alarm. In addition, these events shall not display on the alarm banner. However, shall be viewable on the dedicated historical alarm log screen in cyan. The inputs shall not log when the trigger returns to the off state. The alarm log shall indicate the date, time and description of the operator input, including analog setpoint if applicable. The ability to search for operator inputs and specific alarm occurrences shall be provided.

.4 The definition for each event shall be as per the "Historical Logged Data" table in Section 2 of the Process Logic Description.

.6 Printing:

.1 Alarm printer control shall be provided as a pop-up accessible from the "Alarm" screen. Operators shall be able to select any portion of the historical alarm log for printing by specifying the start and end time. For example, 10:00 11-23-93 through 14:00 11-24-93. Operators shall be able to specify Alarms, Logged Events, Operator Inputs, Alarms and Logged Event, or Alarms, Logged Events and Operator Inputs for inclusion in the alarm print out, those not specified shall not print.

2.6 Trends

.1 The system shall be configured to allow the operator to recall and simultaneously graph eight or more analog trends per chart over any specified time base.

.2 The trend data shall be logged by the data collection nodes and the database. All other nodes shall access the information from these systems over the network.

.3 The operator shall be able to select the trend they wish to view by tag name, select the individual Y scales (both upper and lower limit) for each individual trend line.

.4 Each trend and scale shall be displayed in a different colour and the legend shall be clearly displayed.

.5 Data missing as a result of a power failure or system failure will not prevent trending. The trend line will not display for time periods where data is missing (it will not display as zero).

.6 Operators shall be able to define common trend groups along with all associated configuration information such as scales, time base, etc., by user defined name and load these trend groups simply by selecting the corresponding group from a list.

.7 Full network printing support shall be provided. The colour printer shall be connected directly to the network and shall be accessible by all computers on the network.

.8 It shall be possible for an operator to plot a trend in colour to the colour printer by hitting a single key to print the trends.

.9 The operator shall be able to select the size of the plot as any size supported by the operating system driver for the printer selected up to and including the largest size supported by the printer selected.

.10 The trend types to be supported are as follows:

.1 Short-Term Trends: Short-term trends will be accessible from the local trend task for a period of not less than 30 days. The sample interval shall be 2 seconds.

.2 Historical Analog Trends: The information shall be logged to the database. The actual sample interval shall not exceed 15 seconds. The developer shall be able to disable at runtime the logging of data on a trend by trend basis during predefined periods by changing a single data point in the control logic for each trend to be disabled. The value recorded in the historian shall be the maximum, minimum, total and/or average as specified by the Engineer in consultation with the Systems Integrator.

.3 Event Trends: In addition to supporting time base driven trending, event driven trending will also be provided. Event driven trends will be stored in the database and will be used for information such as sludge wasting statistics (runtime, flow, etc.), daily operational summary information (daily flow, max flow, etc.), etc.

.11 It shall be possible to add not less than 25 additional trends to each trend type without disabling the collection of data for trends already defined or suspending trending for any interval longer than 1 minute. The addition of new trends shall in no way place any restrictions on the accessibility of the information (including, but not necessarily restricted to, trend data) previously stored on the system.

.12 It shall be possible to remove individual trends from each trend type without disabling the collection of data for other trends already defined or suspending trending for an interval longer than 1 minute. The removal of trends shall in no way place any restrictions on the accessibility of information (including but not necessarily limited to trend data) previously stored on the system.

2.7 Keyboard Usage

.1 The following key assignments shall be used:

F1 - Help
F2 - Main Overview Graphic
F3 - Alarm Screen
F4 - "Toggle" for screen control pop-up

F5 - Toggle keyboards - Actual/Virtual
F6 - Sign On
F7 - Sign Off
F8 - Acknowledge
F9 - Show

2.8 Mouse/Trackball Usage

.1 The system shall be able to operate strictly from a pointing device without need for a keyboard. A user toggle shall be used to switch between "keyboard" and "virtual keyboard" using F5. Popup keyboards to allow the system to function without the use of a keyboard will only be displayed when "virtual keyboard" mode has been selected, otherwise an input box will be displayed echoing keyboard input.

.2 Mouse and Trackball button usage will follow the Microsoft Windows conventions.

2.9 System Configuration/Programming

.1 General Guidelines:

.1 Where possible, all programs shall be protected by the use of passwords to ensure unauthorized individuals are unable to modify existing programs and/or configurations. If the system allows multiple level passwords allowing separate passwords for view and edit capabilities, multiple passwords shall be implemented. All passwords shall be provided to the Engineer such that the Engineer staff will have full access to all programs, documentation, etc.

.2 Computers:

.1 Development Tools and Programming Languages:

.1 All systems development for PC applications must be performed using approved languages or development tools. These include:

.1 Operating systems
.2 Database management systems
.3 SCADA Systems
.4 Programming Languages
.5 Report Generators.

.2 Approved languages and development tools are listed in Section 13200.