Engineering Standard

SAES-Z-001 28 January, 2004

Process Control Systems

Process Control Standards Committee Members

Qaffas, Saleh A., Chairman
Assiry, Nasser Y., Vice Chairman
Awami, Luay H.
BenDuheash, Adel O.
Busbait, Abdulaziz M.
Dunn, Alan R.
ElBaradie, Mostafa M.
Esplin, Douglas S.
Fadley, Gary L.
Genta, Pablo D.
Ghamdi, Ahmed S.
Green, Charlie M.
Hazelwood, William P.
Hubail, Hussain M.
Jansen, Kevin P.
Khalifa, Ali H.
Khan, Mashkoor A.
Mubarak, Ahmed M.
ShaikhNasir, Mohammed A.
Trembley, Robert J.

Saudi Aramco DeskTop Standards

Table of Contents

Table of Contents (Cont'd)

1 Scope

This Standard prescribes the minimum mandatory requirements and guidelines governing the engineering, design and installation of Process Control Systems (PCS) in Saudi Aramco plants.

Systems such as Distributed Control Systems (DCS), Supervisory Control and Data Acquisition Systems (SCADA), PLC, and the interface with their subsystems are considered within the scope of this standard. The regulatory, sequential, advanced controls and optimization implemented in these systems are also included. The integrated system shall be referred to as the Process Control System (PCS).

The following systems are excluded from this standard except their interfaces to the PCS:

a) ESD (Emergency Shutdown) systems (covered by SAES-J-601)

b) Royalty and Custody Transfer Systems (covered by SAES-Y-101, SAES-Y-102, and SAES-Y-103)

c) Package Unit Instrumentation (covered by 34-SAMSS-831), for example, an air compressor skid、Licensor's specific technology package.

d) Automatic Tank Gauging System (covered by 34-SAMSS-318)

This entire standard may be attached to and made a part of purchase orders.

2 Conflicts and Deviations

2.1 Any conflicts between this standard and other applicable Saudi Aramco Engineering Standards (SAESs), related Materials System Specifications (SAMSSs), Standard Drawings (SASDs), or industry standards, codes, and forms shall be resolved in writing by the Company or Buyer Representative through the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

2.2 Direct all requests to deviate from this standard in writing to the Company or Buyer Representative, who shall follow internal company procedure SAEP-302 and forward such requests to the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

3 References

The selection of material and equipment, and the design, construction, maintenance, and repair of equipment and facilities covered by this standard shall comply with the latest edition of the references listed below, unless otherwise noted.

Saudi Aramco References

Saudi Aramco Engineering Procedures

SAEP-16	*Project Execution Requirements for Process Automation Systems*
SAEP-302	*Instructions for Obtaining a Waiver of a Mandatory Saudi Aramco Engineering Requirement*

Saudi Aramco Engineering Standards

SAES-J-003	*Basic Design Criteria*
SAES-J-601	*Emergency Shutdown Systems*
SAES-J-604	*Protective and Condition Monitoring Equipment for Rotating Machinery*
SAES-J-801	*Control Buildings*
SAES-J-902	*Electrical Systems for Instrumentation*
SAES-Y-101	*Custody Metering of Hydrocarbon Gases*
SAES-Y-102	*Royalty Metering of Hydrocarbon Liquids*
SAES-Y-103	*Custody Metering of Hydrocarbon Liquids*

Saudi Aramco Materials System Specifications

23-SAMSS-010	*Distributed Control Systems*
23-SAMSS-020	*Supervisory Control and Data Acquisition Systems*
23-SAMSS-030	*Remote Terminal Units*
34-SAMSS-318	*Automatic Tank Gauging Equipment*
34-SAMSS-820	*Instrument Control Cabinets - Indoors*
34-SAMSS-830	*Programmable Logic Controller*
34-SAMSS-831	*Package Unit Instrumentation*

Saudi Aramco Engineering Report

SAER-5895	*Alarm Management Guidelines for Process Automation Systems*

4 Definitions

4.1 Abbreviations

CCS	Compressor Control System
CWAN	Combined Wide Area Network
DCS	Distributed Control System
ESD	Emergency Shutdown Systems
FIFO	First-In, First Out
HMI	Human Machine Interface
HTML	Hyper Text Markup Language
OPC	OLE for Process Control
PCS	Process Control System
PDF	Portable Document Format
PLC	Programmable Logic Controller
RMPS	Rotating Machinery Protection System
RTPM	Real-Time Performance Management
RTU	Remote Terminal Unit
SAEP	Saudi Aramco Engineering Procedures
SAES	Saudi Aramco Engineering Standards
SAMSS	Saudi Aramco Material System Specifications
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol
TMS	Terminal Management System
UPS	Uninterruptible Power Supply

4.2 Definitions

Advanced Control: Multivariable, constraint and optimizing controls will be labeled advanced controls. Controls that fall into this category will be those that are supervisory in nature, i.e., they normally, but not always, output to the set points of other control loops rather than to the valves directly.

Algorithm: A prescribed set of well-defined rules or processes for the solution of a problem in a finite number of steps. (See also control algorithm).

Application: Application packages shall be vendor's standard off-the-shelf offering configurable to meet job-specific requirements. Modification of source codes unique for Saudi Aramco is not allowed.

Availability: The percent of time a system or component remains on line and performs as specified.

Cascade (Cascade Control): A control scheme composed of two loops where the setpoint of one loop (the inner loop) is the output of the controller of the other loop (the outer loop).

Control Algorithm: A mathematical representation of the control action to be performed.

Console: A collection of one or more workstations and associated equipment such as printers and communications devices used by an individual to interact with the PCS and perform other functions.

Critical services: A service which if lost would result in either a major process upset or loss of operation

Dead Band: The range through which an input signal may be varied without initiating an action or observable change in output signal.

Distributed Control System (DCS): A process control system that is composed of distinct modules. These modules may be physically and functionally distributed over the plant area. The distributed control system contains all the modules and associated software required to accomplish the regulatory control and monitoring of a process plant, excluding field instruments, remote terminal units, auxiliary control systems and Plant information systems.

Firmware: Firmware is a combination of both hardware and software. Hardware such as ROMs (Read Only Memory) or EPROMs that have software programs or data recorded on them is considered firmware.

Functional Specification Document (FSD): Written requirements of the functionality required for a piece of equipment or a system.

Hardware: Instrumentation and Control System Hardware consists of physical devices like transmitters, I/O cards, power supplies, control processors, disk drives, display screens, keyboards, printers, integrated circuit boards, and silicon chips.

OLE for Process Control (OPC): The objective of the OPC Foundation is to develop an open, flexible, plug-and-play standard that allows end users to enjoy a greater choice of solutions, as well as sharply reducing development and maintenance costs for hardware and software suppliers.

Operator Console: A console used by an operator to perform the functions required to monitor and control his assigned plant areas.

Point: A process variable derived from an input signal or calculated in a process calculation.

Portable Document Format (PDF): A file format developed by Adobe Systems. PDF captures formatting information from a variety of desktop publishing applications, making it possible to send formatted documents and have them appear on the recipient's monitor or printer as they were intended. To view a file in PDF format, you need Adobe Reader, a free application distributed by Adobe Systems.

Programmable Logic Controller (PLC): A stand-alone microprocessor-based control device used primarily to perform discrete or sequential control.

Real-Time Performance Management (RTPM): An integrated set of computing hardware, system software, networking, communication products, database management and applications which interfaces with the PCS to provide process data to a wide variety of users in an off-line office environment.

Redundant: A system and/or subsystem that provides for a standby module with automatic switchover from the active unit to the standby module, in the event of a failure, without loss of a system function. Both active and standby modules utilize diagnostics to assist in identifying and locating failures and to permit modules to be removed for repair and/or replacement.

Regulatory Control: The functions of process measurement, control algorithm execution, and final control device manipulation that provide closed loop control of a plant process.

Remote Terminal Unit (RTU): A device used for interfacing process I/O in a remote location with a central station. An Intelligent RTU includes discrete and regulatory control functions.

Software: Software shall be considered programming code, computer instructions or data that can be stored electronically. The storage devices and display devices are hardware. Software is often divided into two categories:

- **Systems Software:** Includes the operating system and all the utilities that enable the computer to function.
- **Applications Software:** Includes programs that do real work for users. For example, word processors, spreadsheets, and database management systems fall under the category of applications software.

Supervisory Control and Data Acquisition (SCADA): A system primarily intended for data acquisition and limited remote control over a wide geographically distributed area.

Tag: A collection of attributes that specify either a control loop or a process variable, or a measured input, or a calculated value, or some combination of these, and all associated control and output algorithms. Each tag is unique.

Terminal Management System (TMS): An integrated product receipt and distribution control management for terminal operations. Terminal facilities include bulk plants and air fueling terminals.

Transmission Control Protocol (TCP): Is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Workstation: A set of electronic equipment including a minimum of one monitor, keyboard(s) and associated pointing device(s).

5 System Selection

Depending on the particular control objectives to be accomplished within any given project, decisions need to be made regarding selection of the class of system(s) to be utilized.

This selection is specified by the Company's purchase orders, contracts or job specifications, including a project-specific FSD.

6 Standard Vendor Products

6.1 The process control system shall be composed of manufacturers' standard hardware, software, firmware and process control application packages.

6.2 A vendor's standard operating system software shall not be modified to meet any of Saudi Aramco's requirements.

All hardware, firmware, software and application that are supplied shall have been field proven prior to the hardware freeze date as defined in the contract or purchase order. Field proven is defined as successful operation at a field installation for six (6) or more months (excluding beta test period). It shall be possible for Saudi Aramco to verify the field proven status of the system.

6.3 Application packages shall be vendor's standard off-the-shelf offering configurable to meet job-specific requirements. Modification of source codes unique for Saudi Aramco is not allowed.

6.4 Third-party products incorporated as part of the vendor's systems must have been approved and certified by the specific vendor. Any substitute must be approved by Saudi Aramco in writing.

7 Segregation and Redundancy

7.1 The PCS shall be configured to segregate control functions for common or parallel plant equipment in order to provide a level of acceptable risk based on a risk area concept. The segregation, if required, shall be dictated by the project-specific FSD.

7.2 Each risk area shall comprise of one or more process units. This shall ensure that the failure of the control equipment in one risk area will not adversely affect the operation of any other areas.

7.3 Each risk area shall have its own process controllers with their own input, and output module(s). Each risk area shall also be provided with the designated amount of spare capacity as specified in the Company purchase document.

7.4 Multi-loop process controllers shall be provided in a redundant configuration. In critical services, output modules shall also be redundant.

7.5 All internal network communications required to support the operator's view and to manipulate the process, shall be provided in a redundant configuration.

7.6 A minimum of two electrically and electronically independent operator workstations shall be provided for each operator's console.

8 System Access & Security

This section details the requirements for restricting the access to process control system HMI functions. Five levels are required - Level 0 View Only and Levels 1 to 4. It shall be possible to configure these levels with selectable privileges. Each higher level shall include all the lower level privileges.

a) Level 0 (View Only)
b) Level 1 (Process Operator)
c) Level 2 (Process Operations Supervisor)
d) Level 3 (Engineer)
e) Level 4 (System Administrator)

8.1 Level 0 View Only

It shall be possible to configure any operator workstation for "View Only" access. This mode shall allow the viewing of all process values, configuration data, process displays, system status displays, trends, and reports configured in the system; but shall not allow the manipulation of any data or process parameters.

8.2 Level 1 Process Operator

This level shall allow normal operating functions to be performed. These include:

a) Changing of control setpoint
b) Changing of controller mode (auto/manual, etc.)

c) Changing of outputs
d) Acknowledgment of process alarms
e) Configuring and viewing trends
f) Viewing/Requesting reports
g) Viewing/Requesting logs
h) Acknowledgment of system alarms
i) Viewing of system diagnostic displays.

It is not mandatory that a password or key be provided for this level.

8.3 Level 2 (Process Operations Supervisor)

This level shall allow restricted functions to be performed. These include:

a) Modifying alarm parameters
b) Modifying tuning parameters
c) Alarm disable/enable
d) Assignment of plant areas to specific operator workstations
e) Assignment of view-only terminals
f) Manual override of process input values.

A hardware key and/or password shall be required. Configuration of reports and logs shall be allowed.

8.4 Level 3 (Engineer)

This level shall allow engineering functions to be performed. These include:

a) Alarm disable/enable
b) Modifying alarm parameters
c) Modifying tuning parameters
d) Building graphics
e) Software modification/development
f) Configuring password and key lock access
g) Database development/modification
h) Changing/assigning passwords.

8.5 Level 4 (System Administrator)

This is the highest level that has the privileges of all the above levels plus the following:

a) Set up and delete users
b) Control passwords
c) Restrict file accesses

d) Setting file attributes

e) Restricting any system resources

For systems that do not segregate levels 3 and 4, these two levels may be combined and labeled Level 3.

8.6 A hardware key or password shall be required to access Level 2 and above.

8.7 Keys

If keys are provided, they shall be of the type such that

a) Removal of the key shall prevent the access to any key protected functions.

b) Different keys for access to levels 2, 3 and 4.

8.8 Passwords

If passwords are used for access, it shall be possible for the user to configure different passwords for all levels.

8.9 Anti-virus protection shall be initially installed and update procedures clearly written in a manual.

9 Process Control & Equipment Protection

9.1 Regulatory Control Implementation

9.1.1 Control algorithms shall be executed at a rate based on process requirements as specified in the FSD. Consideration must be taken during design that the I/O scan rate is at least as fast as the required control algorithm execution rate. If not specified, all PID loops shall execute once per second.

9.1.2 Control loops shall be configured for bump-less transfer between manual, automatic, cascade and "computer" modes. Bumpless transfer shall be defined as less than 0.5% deviation when the transfer occurs.

9.1.3 Tracking - Control loops shall be configured to set the output of the controller equal to the downstream value during the initialization process. If the downstream value is an output to the field, the initial output of the controller will equal the position of the field device. For cascade controllers, the output of the primary controller shall equal the setpoint of the secondary controller.

9.1.4 Output - Output modules with failsafe functionality shall be configured to safely shutdown affected process equipment.

9.1.5 Composite tag - Where possible, multiple inputs and outputs for a single device, such as a pump or MOV, shall be combined into a single tag ID. Operation of the device shall be through this single tag ID.

9.2 Advanced Control Implementation

9.2.1 Advanced control shall be implemented in a hardware platform that is supported as a standard offering by each individual supplier.

9.2.2 Advanced control loops shall be of a supervisory nature and provide the set-points for regulatory control loops. Direct output to the output modules shall be by exception and clearly documented.

9.2.3 Startup and shutdown of the advanced control algorithms, whether by hardware failure or via operator command, shall be bumpless to the process.

9.2.4 If a critical input to an advanced control strategy or algorithm is out of service, the system will be automatically 'turned off' and the control will revert automatically to regulatory control, and the operator will be notified.

9.2.5 Graphical displays shall be provided for operators to monitor and manipulate advanced control strategies and/or algorithms. Where feasible, these displays shall be accessible through the operator's normal DCS workstation. Provide the following operator functions:

- Operator shall be able to acknowledge the APC alarms from the DCS station.
- Operator shall be able to bypass non critical APC control variables from his station.

9.2.6 Where an economic objective function is used, it shall be possible to change all economic parameters on-line.

9.2.7 Alarms shall be provided from the advanced process controller when it or its sub-controllers are turned off for any reason.

9.2.8 Graphical displays shall be provided for the operator to allow/disallow the advanced process controller to write to the DCS, SCADA or PLC systems.

9.2.9 Graphical displays shall be provided for the operator to change the limits of any process variables permitted.

9.3 Sequential Control

If a DCS is selected, and the sequence control is process related, it is preferred to be implemented in a process controller inside the DCS. If a PLC is selected, it shall be integrated as part of the PCS.

9.4 Equipment Protection

9.4.1 Equipment protection can be implemented either in the DCS, SCADA or the ESD layer, or other auxiliary systems such as RMPS and CCS as specified by the FSD in each project.

9.4.2 If implemented in the PCS layer, bypasses on both inputs and outputs shall be provided. Alarming and journaling of all bypasses are required.

9.4.3 Input, Output and Startup Bypasses

a) All shutdown inputs - sensing devices shall be installed or configured with a bypass switch to facilitate maintenance or testing. Bypass switches in electrical or electronic systems shall be either hardwired, or software-configured with a restrictive access mechanism such as a key-lock, a password protection scheme, or both.

b) Startup bypass systems shall be configured for devices which would prevent the normal startup of plant equipment, e.g., minimum flow, level, pressure or temperature interlocks. Startup bypasses shall be reset either by an operator or a computer program.

c) Activation of a bypass switch (i.e., to the bypass position) shall cause either a hard-wired status light or a 'soft light' in an operator graphical display.

d) Deactivation of a bypass switch shall also initiate either a hard-wired annunciation on an operator panel/display console, or software configured graphic display that emulates the same functions. A flashing or unique alarm display and an audible alert signal shall be used.

e) Activation or deactivation of a bypass switch in an electronic system shall initiate an entry in an event log which shall archive the change of state by tag number and by descriptor.

9.4.4 Logic for ESD input or startup bypass switches, and associated functionality (e.g., annunciation and event logging), shall be shown on separate logic or function block drawings, but not on P&IDs.

10 Consoles and Workstations

10.1 General

10.1.1 Consoles, including panel and CRT mounting structures shall be equipped with tabletop work surfaces.

10.1.2 Where required, telecommunication equipment (e.g., telephones, plant paging system, PA system) and emergency shutdown buttons shall be incorporated in separate bay within the same console furniture.

10.1.3 Each workstation shall have access to a printer which could be networked within the PCS network.

10.1.4 Printers shall be free standing, or tables shall be provided. Printers that utilize fanfold paper shall be equipped with pedestal (noise absorption enclosures) with paper stackers.

10.2 Operator Consoles

10.2.1 Each station in the operator console shall have access to printer(s) for alarm logging, reporting and graphical printing.

10.2.2 Consoles that are manned on a continuous basis shall be configured with a networked graphics printer for making hard copies of active displays.

10.2.3 Each Operator Console shall be equipped with a minimum of two workstations. (Section 7.6)

10.2.4 Shutdown buttons shall comply with SAES-J-601.

10.3 Engineering Workstation

10.3.1 Engineering consoles shall consist of a minimum of one workstation, each engineering workstation shall have access to a printer.

10.3.2 Each engineering workstation shall be capable of performing all operator workstation's functions.

11 Operator Graphical Displays

This section defines graphical displays primarily used by process operators to control and obtain information via the operator workstation.

11.1 Control functions

11.1.1 On systems where the dynamic update time of the operator displays can be configured, they shall be configured for updating at least once every four seconds.

11.1.2 For remote data acquisition, updating shall be within one second of the actual event received at the central station.

11.1.3 The operator shall be able to perform all the basic monitoring and control functions from graphic displays. These functions shall include, but not be limited to, changing process variables, alarm logs, setpoints, switching control modes, manually driving outputs, or initiating maintenance bypasses for input points.

11.1.4 Control Strategies

11.1.4.1 Control strategy information shall be displayed in such a way that the operator can determine what is being controlled, which control strategies are in service, which are out of service, and which are constrained or limited in some

way. Displayed control strategy information shall be dynamic, reflecting the actual current state of the strategy.

11.1.4.2 The operator shall be able to manipulate the state of the control strategy from the control graphics. Controller modes shall be indicated on primary operating display.

11.1.4.3 Where alternate control paths exist for advanced process controls, the graphical interconnecting line representation shall change to show the current control path.

11.2 Design Philosophy

11.2.1 Operator displays shall use only standard features provided by the selected product.

11.2.2 When designing operator displays, a consistent approach shall be used for the appearance (look-and-feel) and functionality. Avoid using highly animated objects that may inadvertently divert the operator from important process information.

11.2.3 The design approach shall include standardized approach for the entire process plant:

a. Layout - line sizes, equipment representation, orientation, fonts, titles, etc.

b. Data representation - process values and alarms

c. Color choices - process lines, control lines, process equipment, titles, etc.

d. Display access and navigation

e. How options are chosen via switches

f. How control strategies are commissioned and de-commissioned

g. How status pairs are defined (on/off, open/closed, start/stop, etc.)

h. Control modes (manual/auto/computer etc.), either by color or by a small text next to the controller

i. Data validity (invalid, out-or-range, unknown status), either by color or by a small text next to the controller

11.2.4 Wherever possible and practical, library elements, e.g., controller faceplate template, shall be used when assigning elements to a graphic. The template approach is preferred to ensure consistency between elements on graphics. Individual elements within a library element should be configured using agreed conventions. For example, if the background color of a process value indication in a controller element is specified to be flashing red for unacknowledged

alarm condition, solid red for acknowledged alarm condition, and flashing background color for unacknowledged return-to-normal alarms, this behavior should be specified in a display convention file and the element linked to the display convention. This approach is preferred to ensure consistency between elements on a graphic and to facilitate graphic maintenance in the future.

11.3 Navigation Through Displays

11.3.1 Any graphic display shall be accessible via no more than three operator actions.

11.3.2 When a graphic display has an associated primary control display, e.g., a group display, the graphic shall have a target that immediately calls up the associated control display. This target shall be located in the same location on every graphic that uses this feature.

11.3.3 When using a windows environment consideration must be given to prevent the Operator from opening too many windows and potentially masking important process information.

11.4 General Operator Graphics Requirements

11.4.1 All graphics shall include the following information in standard locations:

a) Title
b) Date and time
c) Display name

11.4.2 Colors

The following guidelines on color usage shall be applied unless it violates the standard conventions designed into the system.

a. Bright colors shall be used to convey key information such as process and control information.

b. Subdued (low intensity) colors shall be used for process vessels, process lines, and equipment labels.

c. Data representation of a specific type (alphanumeric, symbolic, etc.) shall be displayed with the same color sets for specific conditions on all graphic displays.

11.4.3 Process and Control Lines

11.4.3.1 Process and control line crossovers shall be minimized. Line breaks shall be used to indicate that crossing lines do not join. Main process lines for each graphic shall be bold with secondary lines being of finer width.

11.4.3.2 Process lines shall either be drawn horizontally or vertically.

12 Alarms and Messages

12.1 General

12.1.1 Alarm and messages shall be configured to perform the following:

a) To draw the operator's attention to abnormal conditions within his area of responsibility, both in the process (process alarms) under his control and in the control system equipment (system alarms).

b) To provide information to facilitate the operator's rapid understanding of the abnormal condition.

c) To provide rapid access to the tools needed by the operator to perform corrective action.

d) To provide a comprehensive historical record, accessible to the operator and other plant personnel, of the information needed to assess such abnormal conditions.

e) To prompt the operator or process engineer for feedback when approval for automated action or selection from among options is required.

f) To give operators and other users the ability to enter messages useful to other operators and users.

12.1.2 Alarms and messages shall be categorized as follows:

a) Process alarms & messages
b) System alarms & messages
c) Operator actions messages
d) Engineer actions messages

12.1.3 SAER-5895 or a similar design document shall be followed to provide the required consistency and avoid configuration of unnecessary alarms. Priority shall be established by severity of consequence and time to respond for each process variable, rather than a blanket policy such as setting alarms on all analog inputs at 80%.

12.2 Process and System Alarms

Any alarm used shall be informative and demands an operator action. Automatic alarm suppression shall be used to minimize nuisance alarms based on logic actions and/or events.

1 General

12.2.1.1 Process and System alarms shall include both audible and visual annunciation.

12.2.1.2 PCS modules shall provide identical alarm options.

12.2.2 Alarm Categories and Level Designations

12.2.2.1 Three alarm categories are required as a minimum:

a) PROCESS: abnormal condition that requires immediate operator action.

b) ESD: for notification that an automatic ESD trip action has taken place.

c) SAFETY: reserved for safety related alarms such as H_2S, combustible and fire alarms.

12.2.2.2 Four alarm levels shall be used as a minimum:

HH - high high

H - high

L - low

LL - low low

These levels may be used in association with any category. However, HH and LL in general indicate an automatic shutdown response or imminent shutdown condition.

The "pre-alarms" shall be designated H (High) or L (low).

12.2.2.3 All automatic trip setpoints or limits shall be pre-alarmed in the PCS, including auxiliary systems, regulatory controls, and ESD loops.

12.2.3 Visible Alarm Indication

12.2.3.1 Blinking Feature Blinking shall be reserved for unacknowledged alarm situations only. Blinking shall cease when the alarm is acknowledged.

12.2.3.2 Alarms - Alarms shall be invisible on the operator graphics, appearing only while an alarm is active.

12.2.3.3 All alarms shall be displayed with a small red square or rectangular with its background flashing. Blinking shall cease when the alarm is acknowledged. The color-coded background shall remain while the alarm is active.

12.2.3.4 Alarms shall be visually displayed and annunciated (blinking when unacknowledged) only on the workstation configured for those alarms.

12.2.3.5 A "Process Alarm Summary" display showing all active process alarms assigned to the workstation shall be provided. Accessing this alarm summary display from any other display shall require no more than one operator action. Alarms shall be grouped on this display to allow the operator to readily identify and respond to alarms and abnormal conditions in his area of responsibility (e.g., Sorted by priority, time).

12.2.3.6 A "System Alarm Summary" display showing all active system alarms shall be provided. Accessing this alarm summary display from any other display shall require no more than one operator action.

12.2.3.7 Each alarm indication shall be shown on one of the two alarm summary displays and on another display which conveys the significance of that alarm in relation to the process or to the control system. The alarm indication on this display shall be positioned and grouped, if necessary, to clearly identify the exact nature of the abnormal condition causing the alarm.

12.2.3.8 There shall be an indication of the overall process alarm status of the operator area assigned to each workstation regardless of which display is in use.

12.2.4 Audible alarm indication

12.2.4.1 Distinct audible tones shall be used to distinguish between the three required alarm categories, i.e., PROCESS, ESD and SAFETY.

12.2.4.2 A different audible tone shall be used to indicate system alarms.

12.2.4.3 Audible tone frequencies shall be between 500 Hz and 3000 Hz to ensure that alarms are heard by operators who might have relatively poor hearing.

12.2.4.4 Audible tone decibel levels shall be loud enough to be heard over normal control room background noise, but not so loud as to cause annoyance or discomfort to personnel. For these reasons, audible alarms should be approximately 25 to 30 dB above the normal "background" noise level.

12.2.4.5 A variable, "warbling" tone shall be considered to help recognize priorities, especially for the highest priorities.

12.2.4.6 The audible alarm signal for an operator console shall continue until either:

a) a "horn silence" is initiated at the operator console or

b) an active alarm is "selected" (on either alarm summary or other displays.)

12.2.4.7 Silencing the horn shall not constitute alarm acknowledgment.

12.2.5 Alarm Printing

The alarm configuration to be printed or not printed at time of alarm or event occurrence shall be decided on a per-project basis.

12.2.6 Alarm Acknowledgment

12.2.6.1 Alarms may be acknowledged only at consoles configured for those alarms.

12.2.6.2 It shall be possible for an operator to acknowledge any alarm configured at a workstation by no more than two actions.

12.2.6.3 An alarm shall be acknowledgeable only if it is shown on an active display.

12.2.7 First-Out

First-out alarms shall be used to pinpoint the origin of an automatic equipment trip.

12.2.8 Nuisance and Inhibited Alarms

12.2.8.1 Nuisance alarms may be caused by a monitored process variable continuously going into and out of alarm. This situation shall be minimized by setting appropriate alarm limits and alarm dead bands.

12.2.8.2 Nuisance alarms may be caused when a process is in a shutdown or out of service condition for an extended period. Alarm inhibition on a group basis shall be provided for use in such situations.

12.2.8.3 A list of inhibited alarms shall be provided and available for both display and printing. Other system processing functions, e.g., data acquisition, control and logging, shall continue for inhibited alarms.

12.2.9 The following PCS system alarms and messages shall be implemented but not limited to:

a) Failed modules,
b) Communication errors,
c) Power supply failures,
d) Cabinet fan failure,
e) Cabinet high temperature, smoke or incipient fire detection,
f) Diagnostic error detections and messages.

12.3 Process and System Messages

12.3.1 Process Messages

Process messages consist of normal process events that need not be brought to the immediate attention of the operator, although they are significant enough to be logged in history files (e.g., "Dehydrator bed regeneration cycle completed").

12.3.2 System Messages

System messages consist of normal system events that need not be brought to the immediate attention of the operator, although they are significant enough to be logged in history files (e.g., "Self-diagnostics program XYZ completed. No errors found").

12.4 Logging of Operation and Engineering Actions

12.4.1 A log shall be available for tracking operation and engineering actions or changes. Actions shall be further divided into "Operation" or "Engineering". Optionally this log should track user name, time of change and an abbreviated text of the change.

Items in the following shall be configured at different security levels depending on the operating organization's established procedures.

12.4.2 Operation actions include normal operator actions that are to be logged in history files including:

a) Change made to the mode of a controller,
b) Change made to the setpoint of a controller,
c) Change made to the output of a controller,
d) Responses to operator prompts,
e) Toggle of an alarm between inhibit and enable,
f) Change made to alarm limit,
g) Activating a soft-bypass of an ESD point accessed via the PCS.

12.4.3 Engineer Actions consist of normal engineer actions that are to be logged in history files, including:

a) Change made to tuning parameters,
b) Download or modification of tag or module configuration,
c) Modification to software used by the PCS,
d) Forcing member of a redundant pair on or off primary status,
e) Placing devices on-line or off-line,
f) Placing a tag on-scan or off-scan,
g) Responses to engineer prompts.

12.5 Operation and Engineering Prompts

12.5.1 Operator Prompts

12.5.1.1 Operator prompts include operator guidance messages which require a response. These may be provided by smart alarming techniques or be part of a semi-automatic sequence where each step requires operator approval before it is initiated (e.g., "Compressor K101 on minimum recycle. Proceed with compressor loading step?").

12.5.1.2 Audible annunciation shall be provided, typically with the tone of "PROCESS" priority level.

12.5.1.3 Operator prompt message shall also serve as the visual indication.

12.5.1.4 No password or key is required for this message.

12.5.2 Engineer Prompts

12.5.2.1 Engineer prompts include guidance messages which require a response from a user performing control system functions.

12.5.2.2 The prompt message shall also serve as the visual indication.

13 History

13.1 On-line History

13.1.1 All PCS configuration parameters, including tag data, workstation configurations and controller module configurations shall be stored on redundant on-line media.

13.1.2 On-line historical data shall be stored for access via history trends, displayed listings, and printed listings.

13.1.3 The collection rates, longevity, and scope for historical data are to be specified on a per project basis. The minimum allowable collection rates and longevity are listed in the following table:

Point type	Sampling Rate	Retention Time
Temperature	10 sec	4 days
Analytical	10 sec	4 days
Level	10 sec	4 days
Flow	4 sec	4 days
Pressure	4 sec	4 days
Discrete	4 sec	1 day

Circular files on a FIFO basis shall be implemented such that the latest records are retained when buffer or list overflow occurs.

13.2 Real-Time Performance Management (RTPM)[R]

13.2.1 Utilities shall be implemented to facilitate gathering, analysis, distribution and visualization of data through RTPM. This implemented capability shall allow the recall of the data to enable the use of all historical data analysis functions.

13.2.2 A method shall be provided to transfer and retrieve historical records from RTPM.

14 Integration & Interface

14.1 General Interface Requirement

14.1.1 Interfaces between the PCS and associated subsystems or auxiliary systems shall use standard hardware and software devices, which are compliant with industry standard protocol; or proprietary protocol, which is offered as a standard product by both the control system vendor and the subsystem vendor.

14.1.2 Redundant communication interfaces shall be supplied for:

a) Emergency Shutdown Systems,

b) Subsystems where loss of communication will result in the significant degradation of control functions.

14.1.3 Where redundant communications are specified, no single component failure shall result in the loss of communication to any subsystem.

14.2 Interface to ESD Systems

14.2.1 Emergency Shutdown Systems, interfaces, bypasses, shutdown and reset functions shall be engineered per Saudi Aramco SAES-J-601 requirements. Segregation of the ESD from the PCS is required.

14.2.2 The interface to ESD systems shall meet the following:

a) Clock to be synchronized with the PCS to within 100 milliseconds or better.

b) The PCS clock shall be the master.

c) "First out" ESD event status, if available, shall be passed via the communications link from the ESD logic solver to the PCS.

d) Peer-to-peer communication between the PCS and ESD is the preferred form of communication.

e) Synchronization shall be performed at least once every 24 hours.

14.3 Interface to Corporate Wide Area Networks (CWAN)

The control system communication to Corporate Wide Area Network and other non-control computer systems shall be designed to ensure that no failure, no request for information, or network loading problem will impact the performance or availability of the PCS. Use of standard software and hardware protocols for interfaces, such as TCP/IP and OPC, are preferred.

A fire-wall shall be installed and configured to allow only authorized users to access the PCS system.

14.4 Interplant Computer Communication

Plant to plant computer communications shall use industry standard protocols such as TCP/IP and OPC. If such standards are not available, then the vendor's standard communication package and protocol shall be used.

15 Units of Measurement

SAES-J-003 specifies the allowable units of measurement and shall apply.

16 Electrical

16.1 Electrical and wiring up to but excluding vendors' standard cabinets shall be designed in accordance with Saudi Aramco Engineering Standard SAES-J-902.

16.2 Marshaling cabinets shall be designed in accordance with Saudi Aramco specification 34-SAMSS-820.

16.3 Two separate, independent, electric circuits shall be supplied to power redundant modules.

16.3.1 If a simplex UPS is provided, one of the feed to system redundant power modules shall be supplied from a raw 120V power feed.

16.3.2 These circuits shall be clearly labeled. Branch circuits or power cords to redundant modules shall be clearly labeled identifying the circuit that they are connected to.

16.4 Redundant internal power supply modules shall be provided for the following:

a) Process controllers
b) Input and output modules
c) Communication modules

16.5 Redundant power supply modules shall be provided for field instrument SAES-J-902.

16.5 Grounding

Grounding design shall be per vendor standard recommendations and per SAES-J-902 whichever is more stringent. Conflicts in grounding design shall be resolved per the provisions of section 2.2.

17 Environmental Conditions

SAES-J-003 shall apply.

18 Control Rooms

Control room design shall be per SAES-J-801.

19 Documentation

Comprehensive documentation shall be provided as listed below to ensure that the PCS is engineered and configured in a consistent manner. It also ensures that a PCS project is executed properly, that operating personnel are provided with accurate drawings and manuals and that maintenance personnel will be able to trouble shoot and repair the PCS, post installation.

SAEP-16 identifies the minimum documentation requirements and guidelines for PCS systems, for other systems are not covered by SAEP-16, the following are required:

19.1 Standard vendor manuals and catalogs shall be provided in CD-ROM or other electronic media. Formats to be in PDF or HTML

19.2 Instrument and configuration data bases Microsoft Excel, Access or Intools.

3 Final project specific documents in two signed hard copies plus two (2) sets of CD-ROM in Microsoft Word.

Revision Summary

28 January, 2004 Major revision.