DISTRIBUTION SHEET

To Distribution	From Tank Farm Projects	Page 1 of 1
		Date <u>04/27/95</u>
Project Title/Work Order Process Control Computer Software Requirements and Specifications for the 241-AY and 241-AZ Tank Farm MICON Automation System		EDT No. 607937
		ECN No. --

Name	MSIN	Text With All Attach.	Text Only	Attach./ Appendix Only	EDT/ECN Only
<u>U.S. Department of Energy,</u> <u>Richland Operations Office</u>					
C. R. Pacheco	S7-52	X			
<u>ICF Kaiser Hanford Company</u>					
J. L. Henderson	E6-22				X
<u>Westinghouse Hanford Company</u>					
R. L. Brown	B4-08	X			
H. M. Chafin	G6-07	X			
F. T. Clifton	G6-06	X			
K. A. Colosi	R3-27	X			
R. A. Dodd	S5-05	X			
M. D. Harding	S5-07	X			
L. F. Hill	S4-58	X			
M. N. Islam	R3-08				X
S. R. Nelson	G6-14	X			
S. R. Pierce	S5-05	X			
M. C. Teats	R1-43	X			
Project Database	B3-65	X			
Project Files	G6-51	X			
Central Files (orig. +2)	L8-04	X			
OSTI (2)	L8-07	X			

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

APR 28 1995
35 Station 21

ENGINEERING DATA TRANSMITTAL

Page 1 of 1
1. EDT 607937

2. To: (Receiving Organization) Distribution	3. From: (Originating Organization) Waste Treatment Systems Engineering	4. Related EDT No.: NA
5. Proj./Prog./Dept./Div.: W-030	6. Cog. Engr.: M. C. Teats	7. Purchase Order No.: NA
8. Originator Remarks: Approval and release of the attached software specs and requirements for the Aging Waste Vent System MICON automation system.		9. Equip./Component No.: NA
		10. System/Bldg./Facility: MICON / AY-AZ Tank Farms
		11. Receiver Remarks:
		12. Major Assm. Dwg. No.: NA
		13. Permit/Permit Application No.: NA
		14. Required Response Date: ASAP

15. DATA TRANSMITTED					(F)	(G)	(H)	(I)
(A) Item No.	(B) Document/Drawing No.	(C) Sheet No.	(D) Rev. No.	(E) Title or Description of Data Transmitted	Approval Designator	Reason for Transmittal	Originator Disposition	Receiver Disposition
1	WHC-SD-WM-CSRS-025		0	COMPUTER SOFTWARE REQUIREMENTS AND SPECS FOR THE AY/AZ TANK FARM MICON AUTOMATION SYSTEM	Q	1,2		

16. KEY					
Approval Designator (F)		Reason for Transmittal (G)			Disposition (H) & (I)
E, S, Q, D or N/A (see WHC-CM-3-5, Sec.12.7)		1. Approval	4. Review	1. Approved	4. Reviewed no/comment
		2. Release	5. Post-Review	2. Approved w/comment	5. Reviewed w/comment
		3. Information	6. Dist. (Receipt Acknow. Required)	3. Disapproved w/comment	6. Receipt acknowledged

17. SIGNATURE/DISTRIBUTION (See Approval Designator for required signatures)											
(G)	(H)	(J) Name	(K) Signature	(L) Date	(M) MSIN	(J) Name	(K) Signature	(L) Date	(M) MSIN	Reason	Disp.
1	2	Cog.Eng. F.T. CLIFTON	<i>[Signature]</i>	3/16/95	G6-06	M.C. TEATS	<i>[Signature]</i>	see below	R1-43	3	1,2
1	2	Cog. Mgr. K.A. COLOSI	<i>[Signature]</i>	3/14/95	R3-27						
1	2	QA H.M. CHAFIN	<i>[Signature]</i>	3/13/95	G6-07						
1	2	QA M.L. HERMANSON	<i>[Signature]</i>	3/13/95	A4-79						
		Safety									
		Env.									

18. <i>M.C. Teats</i> 3/8/95 Signature of EDT Originator	19. <i>[Signature]</i> 3/15/95 Authorized Representative for Receiving Organization	20. <i>[Signature]</i> 3/14/95 Cognizant Manager	21. DOE APPROVAL (if required) Ctrl. No. ☐ Approved ☐ Approved w/comments ☐ Disapproved w/comments
--	---	--	---

RELEASE AUTHORIZATION

Document Number: WHC-SD-WM-CSRS-025, Rev.0

Document Title: Process Control Computer Software Requirements and Specifications for the 241-AY and 241-AZ Tank Farm Micon Automation System

Release Date: April 27, 1995

**This document was reviewed following the
procedures described in WHC-CM-3-4 and is:**

APPROVED FOR PUBLIC RELEASE

WHC Information Release Administration Specialist:

V.L. Birkland

April 27, 1995

TRADEMARK DISCLAIMER. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors.

This report has been reproduced from the best available copy. Available in paper copy and microfiche. Printed in the United States of America. Available to the U.S. Department of Energy and its contractors from:

U.S. Department of Energy
Office of Scientific and Technical Information (OSTI)
P.O. Box 62
Oak Ridge, TN 37831
Telephone: (615) 576-8401

Available to the public from: U.S. Department of Commerce
National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161
Telephone: (703) 487-4650

SUPPORTING DOCUMENT		1. Total Pages 27
2. Title Process Control Computer Software Requirements and Specifications for the 241-AY and 241-AZ Tank Farm MICON Automation System	3. Number WHC-SD-WM-CSRS-025	4. Rev No. 0
5. Key Words W-030, MICON, software, specifications	6. Author Name: M. C. Teats <i>M.C. Teats</i> 4-26-95 Signature Organization/Charge Code 71730/NB103	
7. Abstract Software requirements and specifications for the AY/AZ MICON distributed control system are provided.		

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

8. RELEASE STAMP

**PROCESS CONTROL COMPUTER
SOFTWARE REQUIREMENTS AND SPECIFICATIONS
FOR THE
241-AY AND 241-AZ TANK FARM
MICON AUTOMATION SYSTEM**

This page intentionally left blank.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
1.0 INTRODUCTION	1
1.1 PURPOSE	1
1.2 SCOPE	1
1.3 OVERVIEW	2
1.4 DEFINITIONS	2
2.0 GENERAL DESCRIPTION	5
2.1 PRODUCT PERSPECTIVE	5
2.1.1 COMMUNICATION INTERFACES	7
2.2 PRODUCT FUNCTIONS	7
2.3 USER CHARACTERISTICS	8
2.4 GENERAL CONSTRAINTS	8
2.5 ASSUMPTIONS AND DEPENDENCIES	8
2.6 CONTROL SOFTWARE RATIONALE	9
2.7 WATCHDOG CIRCUIT RATIONALE	9
3.0 SOFTWARE REQUIREMENTS AND SPECIFICATIONS	10
3.1 DATABASE & CONTROLLER SOFTWARE REQUIREMENTS & SPECS	10
3.2 OPERATOR INTERFACE SOFTWARE REQUIREMENTS & SPECS	10
3.2.1 LOOP AND ANALOG DETAIL DISPLAYS	11
3.2.2 GROUP DISPLAYS	11
3.2.3 OVERVIEW DISPLAYS	11
3.2.4 TREND AND HISTORY DISPLAYS	12
3.2.5 ANNUNCIATOR DISPLAYS	12
3.2.6 GRAPHIC DISPLAYS	13
3.2.7 ALARM COLORS	16
3.2.8 GRAPHIC DISPLAY COLOR USAGE	19
3.2.9 LOCAL OPERATOR INTERFACE	19
4.0 REFERENCES	20

LIST OF FIGURES

<u>Section</u>	<u>Page</u>
Figure 1. W-030 DCS Hardware Configuration	5

LIST OF TABLES

<u>Section</u>	<u>Page</u>
Table 1. Alarm Color Usage	16
Table 2. Graphic Display Color Assignments	19
Table 3. LOI Definition	19

LIST OF TERMS

CRT	Cathode Ray Tube
DCS	Distributed Control System
GPLI	General Purpose LAN Interface
ICF-KH	ICF Kaiser Hanford
IOK	Industrial Operator Keyboard
LAN	Local Area Network
LOI	Local Operator Interface
LCU	Local Control Unit
OCS	Operator Control Station
P&ID	Piping and Instrument Diagram
RCM ¹	Remote Control Module
TCP/IP	Transmission Control Protocol / Internet Protocol
U-32 ¹	Universal Communication Interface and Supervisory Controller
UPS	Uninterruptable Power Supply
WHC	Westinghouse Hanford Company

1. U-32 and RCM are a trademarks of MICON-Powell Process Systems, Inc.

This page intentionally left blank.

1.0 INTRODUCTION

1.1 PURPOSE

The AY/AZ Ventilation control system shall provide uninterrupted operation of the tank ventilation system, maintain a negative differential pressure with respect to atmospheric conditions to contain radioactive and non-radioactive gases, vapors, liquids and airborne particulate within the system until appropriately treated and discharged. The closed loop cooling system shall remove heat generated by the in-tank steam coil and the waste itself.

Rather than control the new ventilation and cooling system with panel boards, control will be performed by a computer process control system purchased from Micon-Powell Process Systems. This system will allow combine control functions with graphics, alarm management and data acquisition. Logic and instrumentation for this system will be provided by ICF-KH. However, control system software will then be implemented by WHC personnel with prior experience in the configurations of Distributed Control Systems.

The purpose of this document is to identify the necessary software requirements for creating and operating this computer system.

1.2 SCOPE

Software designed by ICF-KH and implemented by WHC will control the new ventilation and cooling equipment. In performing this task, the DCS will display the status of all instruments, controls, and alarms to the operator using easy to understand process graphics, display alarms and their origins in a quick and efficient manner, keep record of all alarms and system status changes, trend certain key analog and discrete signal values and display them to the operator on demand, and provide sufficient redundancy to provide a backup for Safety Class 2 systems. Software will identify all failures within the computer itself and switch-over to backup components when needed and available. Software will provide several layers of password protection to prevent the unauthorized use or modification of this software.

Instrument and controls for this system lack redundancy with the exception of Safety Class 2 systems such as the heater, damper and MOV controls on the K1 primary tank ventilation system. In this case, the systems one LCU is redundant to another so bumpless transfer of the process control to a backup unit can be provided. However, this provides redundancy to those signals only and not all signals in the LCUs.

1.3 OVERVIEW

The 241-AY and 241-AZ Tank Farms are the site of four double shell tanks containing high level radioactive liquid wastes from fuel reprocessing operations at Hanford's PUREX plant. These tanks have been serviced by a ventilation and cooling system to prevent boiling. However, this system has been shown to be in need of replacement and will not last into the next decade. Current Hanford Waste Volume Projections identify a need to use these Tanks through the year 2000. The purpose of the W-030 project is to upgrade some of the Tank Farm subsystems including the ventilation and cooling system components and extend the tank's useful life. The upgrade will additionally bring the tank farm into compliance with the current codes. As part of this upgrade, the current panel board system will be replaced with a Supervisory Control and Data Acquisition (SCADA) system to perform all local control, alert the operator to any abnormal conditions, and perform a modest amount of documentation and trending of data.

1.4 DEFINITIONS

A/S OPEN²

The brand name of a Distributed Control System supplied by the MICON Company (Powell Process Systems) of Houston, Texas.

A/S VIEW²

The proprietary operation and configuration software provided by the MICON Company for the MICON A/S OPEN Distributed Control System. This is the user interface software on a SPARC 2 workstation.

DCS

Distributed Control System. Computer system that divides responsibilities up between several types of computers. This type of system allows one computer to perform control at a local level while networked to others that provide display and control to the operator.

GPLI

General Purpose LAN Interface. The GPLI serves as a universal communications interface between the token data highway LAN and the OCS.

-
2. A/S OPEN and A/S VIEW are a trademarks of MICON-Powell Process Systems, Inc.

IOK

Industrial Operator Keyboard. A dedicated, non-QWERTY keyboard used to access displays on an OCS and control plant processes.

LAN

Local Area Network. On the Micon A/S Open system, the LAN passes information between LCUs and the GPLIs. It uses a token-passing carrier-based protocol.

LCU

Local Control Unit. A process control cabinet including signal terminations, several RCMs, one pair of U-32s, a communications bus, an LOI, and miscellaneous hardware (racks, cooling fans, power supplies).

LOI

Local Operator Interface. 80386 SX computer with electroluminescent touchscreen resident in each LCU cabinet door. LOIs provide group and alarm displays for signals residing in the LCU. LOIs cannot display graphics. Group displays are different than those on the operator console.

OCS

Operator Control Station. A Sun Microsystems SPARC 2 operator console including one 19-inch CRT, one QWERTY keyboard, one IOK and one trackball.

P&ID

Pipe and Instrument Diagram. A schematic of a manufacturing process. These drawings show the major equipment components, the connecting piping and services, and the instrumentation. These drawings are traditionally used as a design guide and reference for process control.

RCM

Remote Control Module. A multi-loop programmable controller with I/O terminations capable of processing data, performing process control, logic control, and limited batch control.

TCP/IP

Transmission Control Protocol / Internet Protocol. Universal transmission protocol used to pass information between OCSs.

U-32

Universal Communication Interface and Supervisory Controller. A multi-loop programmable controller with dual network communications capability which passes communications from RCMs and the field bus to the token data highway. Like the RCM, the U-32 is capable of processing data, performing continuous process control, logic, and limited batch control. Unlike the RCMs, U-32s contain no inputs or outputs.

UPS

Uninterruptable Power Supply. Provides battery power to the DCS for brief periods during a power outage.

2.0 GENERAL DESCRIPTION

2.1 PRODUCT PERSPECTIVE

Figure 1 W-030 DCS HARDWARE CONFIGURATION

The computers of this control system are divided into five tasks and four computer networks (see Figure 1).

The Remote Control Module (RCM) are small non-redundant computers that perform the bulk of the process control. Application software is downloaded to the RCMs where it is compiled and executed. All analog and digital inputs and outputs terminate in the back of the RCMs. Controllers may handle analog, digital or a combination of digital and analog I/O depending on the RCM type. Controller memory is limited to 25 Kbyte. Micon approximates the number of loops per controller as 15. RCMs are linked to all other RCMs within an LCU and to a pair of U-32s via a redundant field bus.

U-32s represent the next level of control. U-32s have 1 Mbyte of memory allowing 128 control loops. U-32s are the only redundant controller on this project. U-32s have no terminations but can access I/O or logic in other controllers via export and import statements. U-32s program, compile and execute application software identical to the RCMs. RCM communication is passed through the U-32s. Each U-32 is linked to the other three U-32 pairs and the GPLIs via a redundant token data highway.

General Purpose LAN Interface (GPLI) are IBM PCs that provide an interface between the token data highway and the thin wire ethernet³ of the Operator Control Stations (OCS). GPLIs have no control function. The GPLIs are redundant.

The OCSs are four Sun Microsystems SPARC 2s. The OCSs use the UNIX⁴ operating system. This allows the execution of many tasks at the same time (multitasking). The SPARC 2s display X-Windows⁵ which allows opening of multiple windows and the scaling of windows and text anywhere on the 19-inch CRT. Micon displays may be placed in any of four quadrants of the screen. Access to displays and controls are via an Industrial Operator Keyboard (IOK) or a three button track ball. Pop-up control windows appear in the lower left hand corner of the screen on controllable points. The operator console is used to configure and download the system, display all alarms, statuses, and trends as well as allow the operator to make modifications to the process. Alarms produce the same audible sound for all alarms. The most recent alarms are displayed at the bottom of all screens.

Control functions are organized into Local Control Units (LCUs). Each LCU consists of a two redundant U-32s, and several RCMs with their I/O terminations within one cabinet. The U-32s and RCMs are linked via a non-redundant field bus to a Local Operator Interface (LOI). The LOIs are IBM PC clones with an amber electroluminescent touch screen display. One LOI is mounted in each LCU cabinet door. The LOI can monitor signals and alarms originating within it's LCU. The LOIs are a backup operator interface which allows control of the process in case the operator consoles, thinwire ethernet, or token data highway fail. However, the LOIs are not capable of displaying graphic or group displays as found on the operator consoles.

This system is not related to any other project at Hanford at the present time. However, there are four other Micon systems on the Hanford site.

3. Ethernet is a trademark of the Xerox Corporation.

4. UNIX is a trademark of the American Telephone and Telegraph Company.

5. X-Window is a trademark of Massachusetts Institute of Technology.

2.1.1 COMMUNICATION INTERFACES

The four operator consoles are linked via a 10 Mbyte/sec thick wire ethernet running the TCP/IP network protocol. The thick wire ethernet is used to pass configuration files between OCSs. However, communications between the GPLIs and the consoles is via a non-redundant thinwire ethernet. The LCU field bus, token data highway, and thin wire ethernet communications are via a Micon proprietary protocol. Communications between the SPARC stations are via standard TCP/IP.

There are no current plans to connect this distributed control system with any other computer system on site via a Local Area Network (LAN).

2.2 PRODUCT FUNCTIONS

WHC will supply the application software for the control system. The P&IDs, logic diagrams, and tag list developed by ICF-Kaiser Hanford (ICF-KH) defines the basis for the control logic and other applications software.

Applications software will be created principally using fill-in-the-blank software. The control database is created at the OCS as three files: the scroll list which is displayed and edited at the operator console, a text file which is the compilable code and not seen by the engineer, and the linked list in binary. Creation of the scroll list produces hash tables that define the process control variables and alarms. The text file is what is actually downloaded and compiled in the RCMs and U-32s. This differs from most DCS where one file creates the entire database and is compiled at the OCS before downloading to the controller.

The primary means of displaying the created database is via 'group' displays created by the engineer on the OCS using fill-in-the-blank type software. Group displays are also linked to graphic, trends and alarm summaries.

Graphic displays will be created to mimic in flowsheet-like fashion format, the equipment within the cooling and ventilation system. Graphic displays will be built in-house by WHC process engineers in compliance with ANSI/ISA S5.5 Standard (ANSI/ISA 1985).

Trend displays will show the values of analog and digital signals over time. Key variables will be stored on the computer then archived on magnetic media for later recall.

All process status changes and alarms will print out on printers, in alarm summary files, and alarm summary displays.

Each OCS has a process system status annunciator display with 40 windows. Select windows will be linked by software to multiple alarms and events to handle deterministic alarm processing that will allow a single keystroke on the annunciator display to bring up the

proper graphic display on the associated CRT. Thus, the alarm can be viewed in relationship to the surrounding process environment for enhanced recognition and operator response.

2.3 USER CHARACTERISTICS

Software users will be trained operators, familiar with tank farm operations. Software will be transparent to the operators. Process status and control will be performed using process control graphics, alarm lists and historical trends. These will be displayed on the four 19-inch color screen. Process control will be effected by selecting to control via an password protected keyboard or trackball.

2.4 GENERAL CONSTRAINTS

Micon A/S View Software has many drawbacks. The most notable are:

- Alarms must be silenced at all four consoles.
- Group displays can only display an 8 character descriptions making tag differentiation difficult.
- 16 character tags displayed on 2 lines are difficult to read.
- Alarms don't flash but turn off and on.
- Alarm messages appear on alarm summaries as 3 mm high text which is difficult to read.
- Movement of the cursor stops all alarm flashing for several seconds.
- Processors and some networks are not redundant.
- LOIs cannot display data in the same manner as the operator consoles. Graphics cannot be displayed on LOIs.

2.5 ASSUMPTIONS AND DEPENDENCIES

Process control will be effected by using the process graphic displays. Process graphics may occasionally imbed trends within them. The OCS will display up to four graphics at a time. Four OCSs will be available to the operator to display the process.

OCSs will be powered from three sources: line, UPS, and diesel generator. UPS power will be supplied temporarily on loss of line power until diesel generator power is available.

Safety Class 2 systems are required to not be disabled through a single failure. The Project implemented this requirement through the use of

redundant mechanical trains of ventilation. This necessitates the establishment of two associated Safety Class 2 I&C trains. The DCS specification requires that control of dampers, heaters, fans and the MOV for the final K1 cycle be redundant and that a bumpless transfer of the process control to a backup unit be provided. However, this does not create backup for any other Safety Class 2 or 3 signals.

It should be noted that the time available to manually restart the exhaust fans and/or realign the MOVs is the time calculated for the tank to boil without ventilation (i.e., tank bump). This has been approximated to be on the order of 60 day. It is assumed that operator action is considered functionally equivalent to redundant LCU to initiation the redundant ventilation train. Thus, fully redundant controllers requirement has been dropped with the above exception.

2.6 CONTROL SOFTWARE RATIONALE

The overall ventilation control rationale is to start up the ventilation and cooling system with an input command which will activate the proper sequence to start up the process. Failure of the heater or fan on the ventilation train results in the startup of the backup train.

2.7 WATCHDOG CIRCUIT RATIONALE

The current system/equipment configuration is provided with redundancy (i.e., redundant trains) and duplication of components within the redundant control trains. The two redundant mechanical trains of the tank ventilation system are served by redundant control systems in the form of LCU-1 and LCU-2. These two LCUs perform the redundant functions of control of the mechanical trains, however, they are not point by point redundant, that is, they are not identical in their connection to the field safety class inputs and outputs. (There is no requirement that these two LCUs be identical as long as each of the two trains, the mechanical together with the control are capable of fulfilling the safety function without the assistance of the other train. This is based on the fact that redundancy is provided for single failure reasons.)

Each LCU contains two microprocessors (U-32s) that are redundant, that is they function as primary and backup. The inclusion of the watchdog relays in each of the LCUs allow the RCM of the redundant mechanical/control train to act as a back-up (ie: an installed spare) to the controls of the operating train. These extra levels of redundancy are not required from a redundancy for single failure protection point of view, but rather they are duplication at the component level to enhance operability by providing a back-up and to increase overall reliability through the continued operation of the running mechanical equipment in lieu of starting the redundant train. (The probability of a failure to start is significantly higher than the failure to continue to operate.)

3.0 SOFTWARE REQUIREMENTS AND SPECIFICATIONS

3.1 DATABASE & CONTROLLER SOFTWARE REQUIREMENTS & SPECS

Software applicable to the establishment of the database and the U-32 and RCM-32 controller programs shall meet the following requirements:

- 3.1.1 Implementation of the P&IDs, logics, and tag lists (Attachments 1, 2, and 3).
- 3.1.2 All software for the I/O and controls shall be configured at the board level (ie: the RCMs, rather than U-32s) unless otherwise defined by the P&IDs, logic drawings, or tag lists (Attachments 1, 2, and 3).
- 3.1.3 If tags other than those defined by the tag lists must be configured, then these tags shall have meaningful names. For example: if a tag for a hand switch is needed the tag name shall be assigned according to ISA standards of nomenclature. In this example the tag would be named "HS_" rather than "VD_" or "ISW_". Generic tag names such as "VD_" or "ISW_" shall not be used.
- 3.1.4 The developed software shall have annotated comments after each step to aid in troubleshooting.
- 3.1.5 Discrete input or output signals that are associated with interlocks shall be configured to show the various states (ie: on, off, interlocked, failed) where applicable.
- 3.1.6 All software configurations for the U-32 and RCM-32 controllers shall be generated and maintained using the Controller Configure utility. Scroll and controller files are required for software documentation. Configurations entered using the 'vi' or text editors or some other similar method are not acceptable.
- 3.1.7 All interlocks shall fail to the "0" or un-powered state.

3.2 OPERATOR INTERFACE SOFTWARE REQUIREMENTS & SPECS

Operator interfaces consist of two broad display categories; standard system displays, and customized displays.

Standard system displays are implemented by fill-in-the-blank type tables. Standard system displays consist of loop and analog detail, group, overview, history, trend, and annunciator displays.

Customized displays, or graphics, are implemented using the display builder utility. These are generally free-form, flowsheet-like displays of the process or any type of display that can be envisioned.

3.2.1 LOOP AND ANALOG DETAIL DISPLAYS

Loop and analog detail displays consist of graphical and textual representations of a single loop or point by combining pertinent information contained in group displays, including simulated controller faceplates, with listings of alarm limits and tuning parameters such as gain, reset, and rate. The controller faceplate contains the tag name, an alphanumeric descriptor, the engineering range and units, loop mode indication, and a numeric and bar graph of the process variable, setpoint, and output. Tag names, alphanumeric descriptors, engineering ranges, units, alarm levels, tuning constants, and other parameters will be obtained from the tag lists.

3.2.2 GROUP DISPLAYS

Group displays shall meet the following requirements:

- 3.2.2.1 Group displays will be provided for graphical and textual representations of devices, statuses, alarms, analog loops, and process variables. Tag names, alphanumeric descriptors, engineering ranges, units, alarm levels, tuning constants, and other parameters will be obtained from the tag lists.
- 3.2.2.2 Group displays shall be sequentially arranged such that all groups containing tags for a single graphic shall be in numerical order. For example, a graphic containing information of 20 tags shall be associated with at least 3 group displays which are numbered in order (ie: 1, 2, and 3; not 1, 9, and 15). This is to permit use of the 'Next' and 'Previous' selections within the 'Goto' button of group displays.
- 3.2.2.3 The total collection of group displays shall contain all tags in the tag lists except intermediate tags used in logic or calculations that are not required for operator command, response, or display. Group displays shall contain the following kinds of tags:
 - Analog inputs
 - Analog outputs
 - Analog loops
 - Discrete inputs
 - Discrete outputs
 - Virtual analogs
 - Virtual discretes
 - Multi-state discretes
 - Internal switches

3.2.3 OVERVIEW DISPLAYS

Overview displays containing multiple groups will be implemented. These will provide a summary of process variables and normal and alarm

conditions for selected groups. Multiple overview displays containing all groups shall be provided.

3.2.4 TREND AND HISTORY DISPLAYS

Trend and history displays shall meet the following requirements:

- 3.2.4.1 Trend and history displays of preselected process variables allow viewing of a set of variables over a period of time. All analog variables are to be defined in trend and history displays. All analog variables are also to be archived on magnetic media for later recall.
- 3.2.4.2 Trend displays shall be sequentially arranged such that all trends containing tags for a single graphic shall be in numerical order. For example, a graphic containing 10 analogs shall be associated with at least 2 trend displays which are numbered in order (ie: 1, 2; not 1, 9). This is to permit use of the 'Next' and 'Previous' selections within the 'Goto' button of trend and history displays.

3.2.5 ANNUNCIATOR DISPLAYS

Each operator workstation has a process system alarm annunciator display with 40 windows. Each window can be linked to as many as 24 alarms, or tags. Select windows will be linked by software to multiple alarms to allow a single keystroke on the annunciator display to bring up the proper graphic display on a CRT. Thus, the alarm can be viewed in relationship to the surrounding process environment for enhanced recognition and operator response.

The annunciator window shall meet the following requirements:

- 3.2.5.1 Each of the 40 windows in an annunciator display will be uniquely configured. That is, each alarm will be linked to only one annunciator window and to one specific process graphic display.
- 3.2.5.2 The annunciator display configuration on each workstation shall be identical. That is, the 40 'unique' windows in one workstation annunciator display will be configured exactly the same as all other workstations (ie: lamp #1 is unique from all other lamps on a single workstation, but lamp #1 is configured the same on all workstations). In the event there are not enough windows on one workstation for all of the alarms or graphics, then two separate annunciator configurations shall be provided with each annunciator configuration loaded on two separate workstations to provide redundancy of the annunciators.
- 3.2.5.3 Each of the 40 windows in the annunciator shall bring up a process graphic having alarm information presented on it. That is, the associated process graphic shall not be overview in nature requiring the operator to access some other display.

3.2.6 GRAPHIC DISPLAYS

The following kinds of graphics shall be provided:

- Overview graphics
- Process graphics
- Process sub-graphics (tabular list of all tags in the process graphic and showing current values or statuses)
- Interlock graphics
- PID tuning graphics

General requirements of all graphics are discussed first followed by specific requirements of the individual graphic types.

3.2.6.1 GENERAL REQUIREMENTS OF ALL GRAPHICS

- 3.2.6.1.1 Process control will be effected by using process graphic displays. Graphic displays will be created to mimic, in flowsheet-like format, the equipment within the cooling and ventilation system. Graphic displays will be built in compliance with ANSI/ISA S5.5 Standard (ANSI/ISA 1985).
- 3.2.6.1.2 All graphics shall provide dynamic updates of the process being monitored and controlled including discrete event occurrences, alarm generation by changing colors and flashing messages, valve and fan symbol fill in accordance with ANSI/ISA S5.5 (ANSI/ISA 1985), and process values.
- 3.2.6.1.3 Graphic displays shall provide graphical representation of interrelationships and interactions by means of process mimicry. Cluttered screens will be avoided.
- 3.2.6.1.4 Displays shall consist of standard process symbols (ie: dampers, valves, fans, filters, tanks, piping, condensers, and other equipment) that, in combination, represent the process being monitored.
- 3.2.6.1.5 The graphic displays shall be built in compliance with the alarm color code recommendations of Table 1, Section 3.2.7, and graphic display color usage, Section 3.2.8. Specifically, color will be used to convey a single meaning only. Red shall be reserved to indicate a warning (operator to take immediate corrective action). Red and green for two and three-way valve status is not acceptable. Two and three-way valves shall use the ANSI/ISA S5.5 design format which uses hollow valve symbols to indicate a closed valve and a filled valve symbol to indicate an open valve.
- 3.2.6.1.6 Color coded piping, valves, and other equipment will be used to indicate the flow path. Color code usage for all graphic displays shall be standardized.

- 3.2.6.1.7 The order or position of the special or customized 'Goto' buttons (other than the standard 'Displays' and 'Goto' buttons in the graphics display window) shall be consistent on all graphics. The exception to this is the overview graphics, which are menu-like and have a different organization of data than other graphic display types.
- 3.2.6.1.8 All graphics shall contain a title representing the process or display. The title shall be distinguishable from other static text on the screen. This shall be accomplished using a different but consistent size and/or font.
- 3.2.6.1.9 All graphics shall contain a file name. The syntax for the file name shown in the graphic shall be *filename.v*. This file name shall appear in a standardized location on the graphic, such as lower right corner, or bottom center.

3.2.6.2 OVERVIEW GRAPHICS

Graphic displays will be done in a logical, hierarchical manner to cover the process. The process overview graphic displays will be used to summarize the process and a quick ascension to more detailed displays of smaller sections of the process will be incorporated to obtain more detail. Overview graphics shall contain 'Goto' buttons, in addition to the standard 'Displays' and 'Goto' buttons in the graphics display window, to provide quick and direct access to the associated process graphics.

3.2.6.3 PROCESS GRAPHICS

A process graphic called-up by a single annunciator window shall contain all specific alarm and tag information (tag name, alarm description, symbol with alarm dynamics, and a process value if analog). That is, the need to access some other display from the process graphic shall not be necessary for deterministic alarm processing by operators (ie: the graphic called-up from the annunciator window shall not be overview in nature with the alarm information contained in a sub-graphic that is accessed from the process graphic).

Process graphics shall employ 'Goto' buttons, in addition to the standard 'Displays' and 'Goto' buttons in the graphics display window, to provide quick and direct access to the following associated graphics or displays.

- First group display associated with the graphic
- First trend display associated with the graphic
- First history display associated with the graphic
- All associated interlock graphics
- Process sub-graphic
- Return to overview graphic

3.2.6.4 PROCESS SUB-GRAPHICS

Process sub-graphics shall use a tabular format with rows and columns of data. Separate columns for the tag name, tag description, and current process values or discrete statuses shall be provided as a minimum.

Process sub-graphics shall employ 'Goto' buttons, in addition to the standard 'Displays' and 'Goto' buttons in the graphics display window, to provide quick and direct access to the following associated graphics or displays.

- First group display associated with the graphic
- First trend display associated with the graphic
- First history display associated with the graphic
- All associated interlock graphics
- Return to process graphic

3.2.6.5 INTERLOCK GRAPHICS

Other graphics portraying the process interlocks shall be provided. The statusing of all interlocks shall be done so that interlock graphics can be used to troubleshoot the process. All tags acting as an interlock for a device shall be dynamically statused along with the device, or device tag name, on the interlock graphic.

Interlock graphics shall employ 'Goto' buttons, in addition to the standard 'Displays' and 'Goto' buttons in the graphics display window, to provide quick and direct access to the following associated graphics.

- All associated interlock graphics
- Return to process graphic

3.2.6.6 PID TUNING GRAPHICS

Graphics shall be provided for tuning PID control loops. There shall be one tuning graphic for every PID loop. Each tuning graphic shall be identically formatted. A tuning graphic shall be a line graph showing three variables plotted against time. The three variables plotted shall be the process value, PID output, and loop setpoint.

Tuning graphics shall not require the use of custom 'Goto' buttons.

3.2.7 ALARM COLORS

Alarm color assignments shall be in accordance with the following rationale summarized in Table 1 below:

Table 1. Alarm Color Usage

COLOR	MEANING
Red ¹	A condition of significant adverse consequence ² has occurred which requires appropriate and immediate mitigating action. This includes but is not limited to emergency, unsafe, personnel hazard, process non-permissive, eminent damage to equipment, critical parameter out-of-tolerance, or abnormal conditions.
Yellow ¹ (amber)	A situation has occurred that could result in a condition of significant adverse consequence if appropriate precautionary action is not taken.
Green ¹	This indicates a normal condition to reassure the viewer that no significant adverse consequence has occurred and no mitigating action is required. It is used in association with red and/or yellow indicators.
White ³	An advisory indicator that indicates conditions which do not have "right" or "wrong" implications.
Blue ³	An advisory indicator that can indicate conditions opposite from those indicated by white which do not have "right" or "wrong" implications. The preferential use of blue should be avoided.

Note 1: Consequence illuminated indicator colors (red, yellow, and green) shall not be used for common advisory indications.

Note 2: A condition of significant adverse consequence is one that could cause injury to any person or all persons, cause unacceptable damage to the environment, compromise security, or cause unintended property/equipment damage or monetary loss.

Note 3: When white or blue advisory indicators are used as component status indicators for electrical/electrically controlled components, white shall be used to indicate the energized state and blue shall be used to indicate the de-energized state.

Note 4: Illuminated indicator color coding, by itself, is insufficient to adequately signal significant adverse consequence or advisory conditions. Additional coding and display integration methods shall be used to convey the exact meaning to the proper person.

Refer to DOE Order 6430.1A section 1300-12.4.7 and its references, which include NUREG 0700 and MIL-STD-1472d.

- Note 5: Visual display illuminated indicators currently include simple indicator lights (lamps), legend lights, annunciator panels and CRT displays. For other coding methods that are specific to annunciator panels, refer to NUREG 0700 Exhibit 6.3-2. CRT screens that are not used for monitoring, indication, annunciation, or control functions are not subject to the color coding guidelines herein.
- Note 6: Illuminated "consequence" indicators coded red and yellow in a control room environment must be accompanied by appropriate audible indication prior to being acknowledged. Audible indications accompanying illuminated indicators outside of a control room are at the discretion of design verification personnel.
- Note 7: The number of colors used for the coding of simple indicator lights (lamps), legend lights and annunciator panels should not exceed 11. All color coded meanings shall be uniform throughout a DOE special facility. The five colors shown in the above table are commonly available lens colors for indicator lights, legend lights and annunciator panels.
- Note 8: For devices with more color generating capability, such as CRT displays, the use of more than 11 distinctive colors for visual alarms/annunciations, graphics and labels is permissible if the additional colors do not result in unintended operator confusion or distraction, and do not cause the attention-getting value of each color to be diminished. However, the meanings of colors should remain the same whether applied to panel surfaces or projected in signal lights or on CRTs.
- Note 9: General recommendations with respect to CRT color coding include the following.
1. Color coding may be applied to bar graphs or other graphic media and data summary screens.
 2. Graphics using outlined figures and filled figures should be used to convey on/off, open/closed, or filled/empty vessel. The fill color used should be the same as the color of the graphic figure.
 3. A hollow, outlined graphic should be used to depict de-energized equipment that is "off", equipment that is empty (such as pipes), or the portion of the vessel that is empty.
 4. A filled graphic shall be used to depict energized equipment that is "on," equipment that is filled (such as pipes), or the portion of a vessel that is filled.

5. For systems that do not have the capability of filled or hollow graphic figures, but have the capability to depict these situations with varying colors, the following is recommended.
 - Equipment which is energized and valves which are open should be depicted with the same color. White or light gray is recommended.
 - Equipment which is de-energized and valves which are closed should be depicted with the same color. Blue is recommended.
6. Process flow diagram depictions should be done with colors that remain. Care must be taken to select colors that do not create confusion or discomfort in viewing. Care must be taken to be consistent. Systems continuing through more than one screen shall maintain consistent use of colors.
7. Real-time data can be depicted in green or process color to indicate normal conditions, yellow/amber to indicate the need for precautionary measures to avoid a condition of significant adverse consequence, or red to indicate that a condition of adverse consequence has occurred which requires appropriate and immediate mitigating action. As an alternative, data can be displayed in black or other contrasting color in a small background of the appropriate consequence color (red, amber, or green).

Note 10: Flashing is an approved illuminated indicator coding used when it is necessary to call the operator's attention to some condition requiring immediate action.

Note 11: An advisory illuminated indicator can be elevated to a consequence illuminated indicator providing that proper coding and/or display integration techniques are employed. Proper coding techniques employed are size (large), brightness (intense), location (prominent) and flashing (to emphasize attention/immediate action.)

3.2.8 GRAPHIC DISPLAY COLOR USAGE

Color usage for the various graphic displays shall be standardized. The following color assignments are summarized below in Table 2.

Table 2. Graphic Display Color Assignments

DISPLAY ELEMENT	COLOR ASSIGNMENT
Construction lines for equipment outlines	White
Process Fluid (water)	Blue
Background	Black or Gray
Tag names and descriptions	Cyan
Controls accessible to the operator	Magenta

All neutral colors may vary in shade. However, red, yellow, and green will never be used in any shade other than their brightest hue.

3.2.9 LOCAL OPERATOR INTERFACE

Each LCU has a LOI that enables the operator to access all signals within that LCU. Each LOI shall be configured to provide access to all tags within the cabinet, or cabinets, to which the LOI is connected. Table 3 below shows the cabinets containing tags that must be accessible from the various LOIs.

Table 3. LOI Definition

MODULE	CAN ACCESS TAGS IN CABINETS BELOW
LCU-1 LOI	LCU-1 only
LCU-2 LOI	LCU-2 only
LCU-3 LOI	LCU-3 and associated RCU-6
LCU-4 LOI	LCU-4 and associated RCU-5

4.0 REFERENCES

- ANSI/ISA, 1985, *Graphics Symbols for Process Displays*, American National Standard/Instrument Society of America, New York, New York.
- Clem, Bill, 1992, *Illuminated Indicator Color Coding* (internal memo to Stuart White, September 24), Westinghouse Hanford Company, Richland, Washington.
- NRC, *Guidelines for Control Room Design Reviews*, NUREG-0700, U.S. Nuclear Regulatory Commission, Washington, D.C.
- WHC, *Standard Engineering Practices*, WHC-CM-6-1, EP-2.1, "Computer Software Configuration Management." Westinghouse Hanford Company, Richland, Washington.
- WHC, *Standard Engineering Practices*, WHC-CM-3-10, Appendix F, "System Requirements Specifications." Westinghouse Hanford Company, Richland, Washington.
- DOE, 1989, *General Design Criteria*, DOE Order 6430.1A, U.S. Department of Energy, Washington, D.C.