ENGINEERING CHANGE NOTICE

Page 1 of 2

1. ECN 644759

Proj. ECN

2. ECN Category (mark one)

Supplemental []
Direct Revision [X]
Change ECN []
Temporary []
Standby []
Supersedure []
Cancel/Void []

3. Originator's Name, Organization, MSIN, and Telephone No.
LF Hill, W-030, R1-56, 373-6424

4. USQ Required?
[] Yes [X] No

5. Date
5/13/97

6. Project Title/No./Work Order No.
AY/AZ Ventilation/W-030/NB205

7. Bldg./Sys./Fac. No.
241/AZ-271 10/24/97

8. Approval Designator
Q 10/24/97

9. Document Numbers Changed by this ECN (includes sheet no. and rev.)
WHC-SD-WM-CSCM-028, Rev 0

10. Related ECN No(s).
n/a

11. Related PO No.
n/a

12a. Modification Work
[] Yes (fill out Blk. 12b)
[X] No (NA Blks. 12b, 12c, 12d)

12b. Work Package No.
n/a

12c. Modification Work Complete
n/a

Design Authority/Cog. Engineer Signature & Date

12d. Restored to Original Condition (Temp. or Standby ECN only)
n/a

Design Authority/Cog. Engineer Signature & Date

13a. Description of Change

13b. Design Baseline Document? [] Yes [X] No

Revise in entirety per attached, from Rev 0 to Rev 1.

14a. Justification (mark one)

Criteria Change	[X]	Design Improvement	[]	Environmental	[]	Facility Deactivation	[]
As-Found	[]	Facilitate Const	[]	Const. Error/Omission	[]	Design Error/Omission	[]

14b. Justification Details
Revise to correctly describe how the software items will be identified and controlled. Include a simplified control methodology for simple changes which do not affect the functional design basis.

15. Distribution (include name, MSIN, and no. of copies)

(1)	DB Cole,	R3-25
(1)	KA Colosi,	R3-25
(1)	HM Chaffin,	R3-25
(1)	SC Pierce,	S5-05
(1)	T Choho,	R3-47
(1)	W. M. HARTY JR	S5-13
(1)	W. D. WINKELMAN	R2-12
(1)	G Hopkins,	S5-03
(1)	PC Barrows,	S2-47
(1)	LF Hill,	R1-56

RELEASE STAMP

OCT 28 1997

DATE:
STA: 27
HANFORD RELEASE
ID:

ENGINEERING CHANGE NOTICE	Page 2 of 2	1. ECN (use no. from pg. 1) 644759

16. Design Verification Required	17. Cost Impact						18. Schedule Impact (days)	
	ENGINEERING			CONSTRUCTION				
[] Yes	Additional	[]	$	Additional	[]	$	Improvement	[]
[X] No	Savings	[]	$	Savings	[]	$	Delay	[]

19. Change Impact Review: Indicate the related documents (other than the engineering documents identified on Side 1) that will be affected by the change described in Block 13. Enter the affected document number in Block 20.

SDD/DD	[]	Seismic/Stress Analysis	[]	Tank Calibration Manual	[]
Functional Design Criteria	[]	Stress/Design Report	[]	Health Physics Procedure	[]
Operating Specification	[]	Interface Control Drawing	[]	Spares Multiple Unit Listing	[]
Criticality Specification	[]	Calibration Procedure	[]	Test Procedures/Specification	[]
Conceptual Design Report	[]	Installation Procedure	[]	Component Index	[]
Equipment Spec.	[]	Maintenance Procedure	[]	ASME Coded Item	[]
Const. Spec.	[]	Engineering Procedure	[]	Human Factor Consideration	[]
Procurement Spec.	[]	Operating Instruction	[]	Computer Software	[]
Vendor Information	[]	Operating Procedure	[]	Electric Circuit Schedule	[]
OM Manual	[]	Operational Safety Requirement	[]	ICRS Procedure	[]
FSAR/SAR	[]	IEFD Drawing	[]	Process Control Manual/Plan	[]
Safety Equipment List	[]	Cell Arrangement Drawing	[]	Process Flow Chart	[]
Radiation Work Permit	[]	Essential Material Specification	[]	Purchase Requisition	[]
Environmental Impact Statement	[]	Fac. Proc. Samp. Schedule	[]	Tickler File	[]
Environmental Report	[]	Inspection Plan	[]		[]
Environmental Permit	[]	Inventory Adjustment Request	[]		[]

20. Other Affected Documents: (NOTE: Documents listed below will not be revised by this ECN.) Signatures below indicate that the signing organization has been notified of other affected documents listed below.

Document Number/Revision	Document Number/Revision	Document Number Revision

21. Approvals

	Signature	Date		Signature	Date
Design Authority	WD Winkelman Wayne Winkelman	10/6/97	Design Agent		
Cog. Eng.	LF Hill L F Hill	10/3/97	PE		
Cog. Mgr. (W030)	KA Colosi KA Colosi	10/6/97	QA		
QA	HM Chaffin Hank Chaffin	10/6/97	Safety		
Safety			Design		
Environ.			Environ.		
Other	wm Harty Jr	10/20/97	Other		
	DL Baird	10/22/97			

DEPARTMENT OF ENERGY

Signature or a Control Number that tracks the Approval Signature

ADDITIONAL

Software Configuration Management Plan 241-AY and 241-AZ Tank Farm MICON Automation System

LF Hill
Lockheed Martin Hanford Co, Richland, WA 99352
U.S. Department of Energy Contract DE-AC06-96RL13200

EDT/ECN:	ECN-644759	UC:	2040
Org Code:	74731	Charge Code:	NH102
B&R Code:	EW3130010	Total Pages:	31

Key Words: W-030, MICON, Configuration, Software, Ventilation,

Abstract: Provides the Plan for identifying and controlling the configuration software used by the MICON control system.

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.

Printed in the United States of America. To obtain copies of this document, contact: Document Control Services, P.O. Box 950, Mailstop H6-08, Richland WA 99352, Phone (509) 372-2420; Fax (509) 376-4989.

HC Perkins

Release Approval

OCT 28 1997

Date

Release Stamp

Approved for Public Release

RECORD OF REVISION	LFH 10/24/97	(1) Document Number HNF ~~WHC~~-SD-WM-CSCM-028	Page ii

(2) Title
CSCM Plan for 241-AY and 241-AZ Tank Farm MICON System

CHANGE CONTROL RECORD

(3) Revision	(4) Description of Change - Replace, Add, and Delete Pages	Authorized for Release		
		(5) Cog. Engr.	(6) Cog. Mgr.	Date
0	(7) Original Release			
RS 1	Total Revision per ECN-644759	LF Hill	KA Colosi	11/7/97

COMPUTER SOFTWARE CONFIGURATION MANAGEMENT PLAN

FOR THE

241-AY AND 241-AZ TANK FARM

MICON AUTOMATION SYSTEM

TABLE OF CONTENTS

Section Page

1.0 INTRODUCTION

1.1 PURPOSE

This document establishes a Computer Software Configuration Management Plan (CSCM) for controlling software for the MICON[1] Distributed Control System (DCS) located at the 241-AY and 241-AZ Aging Waste Tank Farm facilities in the 200 East Area. The MICON DCS software controls and monitors the instrumentation and equipment associated with plant systems and processes.

A CSCM identifies and defines the configuration items in a system (section 3.1), controls the release and change of these items throughout the system life cycle (section 3.2), records and reports the status of configuration items and change requests (section 3.3), and verifies the completeness and correctness of the items (section 3.4).

1.2 SCOPE

All software development before initial release, or before software is baselined, is considered developmental. This plan does not apply to developmental software. This plan applies to software that has been baselined and released.

The MICON software will monitor and control the related instrumentation and equipment of the 241-AY and 241-AZ Tank Farm ventilation systems. Eventually, this software may also assume the monitoring and control of the tank sludge washing equipment and other systems as they are brought on line.

This plan applies to the System Cognizant Manager and MICON Cognizant Engineer (who is also referred to herein as the system administrator) responsible for the software/hardware and administration of the MICON system. This document also applies to any other organization within Tank Farms which are currently active on the system including system cognizant engineers, nuclear operators, technicians, and control room supervisors.

[1] MICON is a trademark of MICON-Powell Process Systems, Inc.

1.3 DEFINITIONS

Application Software

Software designed to fulfill specific needs of a user: for example, software for navigation, payroll, or process control. (IEEE Std. 610.12-1990). For this DCS, this is the user created configuration software for the SPARC II workstations, and user generated configuration programs for the U-32[2] and RCM-32[2] controllers.

A/S OPEN[2]

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

A/S VIEW[2]

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 II workstation.

Commercial Software

Licensed or copyrighted off-the-shelf software that is not subject to Hanford design or specification requirements unique to Hanford and is typically used in applications other than Hanford facilities. This software is typically ordered from the manufacturer or supplier on the basis of requirements set forth in the manufacturer's published product description (such as catalogs). Commercial software includes operating systems, language processors, spreadsheets, etc. (WHC-CM-3-10, Rev. 0).

Configuration Item

An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process. (IEEE Std. 610.12-1990).

Configuration Management (CM)

A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (IEEE Std. 610.12-1990).

Controller

[1] Sometimes generically refers to an RCM-32 or U-32 programmable controller (see RCM-32 and U-32).
[2] Sometimes refers to an analog control device (see PID Controller).

[2] U-32, RCM-32, A/S OPEN and A/S VIEW are trademarks of MICON-Powell Process Systems, Inc.

Data files

Data files are primarily developed using MICON utilities and subroutines, and Sun Microsystems editing utilities to a lesser extent. Data files define input and output variables (analog and digital), define data control and processing variables, provide specific attributes to these variables, and direct the RCM-32 and U-32 controllers in the processing of these variables (see Tag).

Distributed Control System (DCS)

A 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

The General Purpose Local Area Network (LAN) Interface (GPLI-32) serves as a universal communications interface, or bridge, between the Sun operator/engineer workstations and the field control processors (RCM-32 and U-32).

Intelligent Operator Keyboard (IOK)

A dedicated, non-QWERTY keyboard used to access displays on a SPARC II workstation and control plant processes.

Local Area Network (LAN)

A data highway used to pass information between the GPLIs and U-32s. It uses a token-passing carrier-based protocol.

Local Control Unit (LCU)

A process control cabinet containing up to two U-32 controllers, several RCM-32 process controllers, a communications bus, a Local Operator Interface, and miscellaneous hardware (racks, cooling fans, power supplies).

Local Operator Interface (LOI)

A personal computer clone with an amber electroluminescent touch screen display located in the door of an LCU cabinet. The touch screen is visible from the outside of the cabinet. An LOI can display information for signals and tags residing in the LCU. This information is in the form of MICON group displays and simple alarm messages. Graphics cannot be displayed on an LOI.

Pipe and Instrument Diagram (P&ID)

A schematic of a process. These drawings show the major equipment components (chillers, fans, filters, heaters, pumps, separators, tanks, valves, and so on), the connecting piping and services, and the instrumentation. These drawings are traditionally used as a design guide and reference for process control.

RCM-32

A multi-loop programmable controller capable of reading real world inputs, providing outputs, processing data, performing continuous control/logic functions, and limited batch control.

Release

Release is an activity that certifies by a stamp that the document is a controlled version, is approved for the intended use, is entered into a database, and is retrievable. (WHC-CM-3-10, Rev. 0).

Software

Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. This includes user-provided instructions and data that implement preprogrammed algorithms in control systems; computer codes and data that will reside in firmware; and where specified by the Cognizant Manager, user-provided instructions and data used by commercial software such as spreadsheet and database packages. (IEEE Std. 610.12-1990 Modified per WHC-CM-6-1; WHC-CM-3-10, Rev. 0).

Software Custodian

The 241-AY, 241-AZ MICON Cognizant Engineer responsible for maintaining control of computer software, computer software media, and their access.

Solaris software

Proprietary software containing the UNIX[3] operating system and the X-Window[4] Motif software. This software is provided by Sun Microsystems.

System Administrator

See Software Custodian.

System Configuration

The completed databases which establish a specific control and display strategy on the DCS for the plant.

Tag

A generic term for variables (analog and discrete) defined by the A/S VIEW software and used by the programmable controllers to process input and output data as specified by the executable logic files.

[3] UNIX is a trademark of the American Telephone and Telegraph Company.

[4] X-Window is a trademark of Massachusetts Institute of Technology.

User

The person or persons, who operate or interact directly with the system. The user(s) and customer(s) are often not the same person(s). (IEEE Std. 830-1984).

U-32

A multi-loop programmable controller with dual network communications capability. The U-32 distributes data between the RCM-32 and GPLI. Like the RCM-32, the U-32 is capable of processing data, performing continuous control, logic control, and limited batch control.

1.4 SECURITY

The security for the MICON system is provided by limiting access to the system through the use of passwords. The system administrator controls access through a login procedure which consists of Login name and a password consisting of six to sixteen characters. The access control programs are pre-existing and are found in the UNIX operating system and A/S VIEW. These programs allow the system administrator to define the level of access and the breadth of allowed operations.

1.5 HARDWARE/SOFTWARE DESCRIPTION

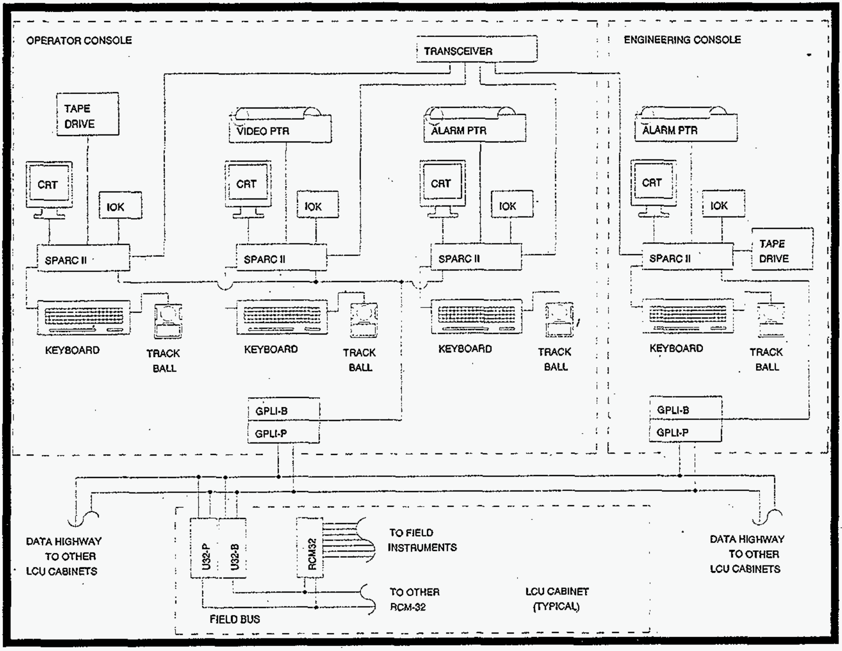

Figure 1: MICON System Architecture

The MICON A/S OPEN Distributed Control System (see Figure 1) consists of four workstations (3 operator, and 1 engineering), a data highway, and six process controller cabinets (4 Local Control Units, LCU's, and 2 Remote Control Units, RCU's).

Each workstation is based on a Sun Microsystems Scalable Process Architecture (SPARC) II workstation, which provides 64 megabytes of memory, a single one gigabyte hard drive, one 3-1/2 inch floppy drive, a 150 megabyte (MB) tape drive, a QWERTY keyboard, and a trackball. In addition, each SPARC II provides a video output, an RS-232 serial port, and two Ethernet[5] ports (a thick-net and a thin-net). The video port is connected to a high resolution color monitor. The RS-232 port is connected to an Intelligent Operator Keyboard (IOK). The IOK is preprogrammed by the MICON Company and cannot be changed by the user. The thin-net Ethernet port is connected to the data highway via a General Purpose Local Area Network (LAN) Interface (GPLI). The GPLIs pass information between the SPARC-based consoles and the process control cabinets. The thick-net provides a LAN connection between the four SPARC II consoles via a multiport transceiver.

[5] Ethernet is a trademark of the Xerox Corporation.

The redundant data highway, which is a LAN using a high speed (10 megabaud) token-passing carrier-based protocol, is the main data link between the consoles and the process control cabinets. It consists of two redundant rings of coax cable that run between the GPLIs and the U32's in the LCU cabinets. One data highway is monitored by one of the redundant GPLI, and the other highway is monitored by the other GPLI. If one of the redundant cables fail, communication is automatically passed to the other and an alarm is generated. Each GPLI (of a pair) is dedicated to monitoring only one highway - thus if one GPLI fails, the data highway ceases to be redundant until the faulty GPLI is replaced. However, highway redundancy for this MICON DCS is achieved by using two pairs of GPLIs. As long as both GPLIs in one of the pairs are fully operational, the highway is redundant because the good pair will broadcast a switch-over message to all other units when an error is detected.

A process control cabinet, or Local Control Unit (LCU), consists of two U-32 controllers, several RCM-32 process controllers, a communications bus, and a Local Operator Interface (LOI). There are four LCU cabinets, and in addition, LCU-3 and LCU-4 are each connected to a Remote Control Unit (RCU). The RCUs (not shown in Figure 1) contain RCM-32 controllers which are connected to LCU-3 and LCU-4 via a field bus. LCU-1 and LCU-2, which are located in separate rooms and separated by a fire barrier, provide for redundancy of safety class 2 controls. Each LCU contains a pair of U-32 controllers, which are redundant. The primary purpose of the U-32's is to pass information between the GPLIs and the RCM-32's, but they can also perform logic functions. The RCM-32's perform control and logic functions, and provide the wiring terminations for the inputs and outputs to plant equipment. The RCM-32's are not physically redundant, although Safety Class 2 functions have been made redundant by system logic and hardware design. Each U-32 communciates with its RCM-32s via a slower (1 megabaud) token-passing communication network called a field bus. The field bus is not redundant, uses RS-485 twisted pair, and communicates using the MICON LAN Protocol (MLP). An LOI (not shown in Figure 1) is a personal computer clone with an amber electroluminescent touch screen display located in the door of each LCU cabinet. The touch screen is visible from the outside of the cabinet and can provide group-like displays for signals and tags residing in the LCU.

There are four types of RCM-32s used in this system - A, F, D, and Dr. The A and F cards are used primarily for analog signals. They can accept inputs from any standard analog instrument type (4-20 milliamp, and DC voltages) and provide standard 4-20 milliamp output signals. In addition they provide two 28 volt DC discrete (on/off) channels. These may be used for input, output, or both. An A card typically provides 26 analog inputs and 4 analog outputs. Each F card provides 26 resistance temperature device (RTD) inputs, 4 analog outputs and 2 digital I/O points. The D card is used for discrete control. It provides 32 on/off channels that can be used as inputs, outputs, or both. Both inputs and outputs are 28 volt DC. The Dr cards are similar to the D cards except inputs are 120 volt AC or DC and the outputs are 3 amp dry contact relays.

Software for the SPARC II workstations consists of four layers. The first layer is the UNIX operating system, and the second is the X-11 windowing system with the Motif (X-Window Motif) graphics user interface

(GUI). Both the UNIX operating system and X-Window Motif are provided by Sun Microsystems under the trade name Solaris. The third layer is the A/S VIEW process control software provided by the MICON Company. The last layer is the user configuration, or application software, which implements the functions specific to our application.

The U-32 and RCM-32 software consists of three layers. The first is the RTS-C based operating system supplied by the MICON Company. The next layer is the MICON controller program compiler, also supplied by the MICON Company. The third layer is the user configuration program, which is compiled object code. This program is created by the MICON controller program compiler using source code input. The source code, or applications software, is created by the A/S VIEW software in the SPARC II workstations based on user input. The source code is then downloaded over the data highway to the U-32s and RCM-32s, where it is compiled.

The UNIX, X-Window Motif, A/S VIEW, RTS-C operating system, and the MICON controller program compiler are off-the-shelf software and are not subject to this configuration management plan except as they are required to reboot the consoles should the entire system crash. Only the application software (user created configuration software for the SPARC II workstations, and user generated configuration programs for the U-32 and RCM-32 controllers) is subject to the revision control covered by this document.

2.0 MANAGEMENT

2.1 ORGANIZATION

The Cognizant Manager responsible for the MCS shall identify a Facility System Cognizant Engineer and a MICON System Administrator. In general, the System Cognizant Engineer is responsibile for the Design Basis which the MCS is designed to meet. The System Administrator is responsible for maintaining the configuration of the software consistent with the design basis documents. Additional personnel may be utilized to perform the necessary work.

2.2 RESPONSIBILITIES

2.2.1 Cognizant Manager

The Cognizant Manager is responsible for ensuring the configuration management controls identified by this document are used; for determining the need for and extent of the software development; for ensuring appropriate approval and reviews are obtained in accordance with the identified "approval designator" (WHC-CM-3-5, *Document Control and Records Management Manual*, 12.7, "Approval of Environmental, Safety, and Quality Affecting Documents"); for ensuring that computer software documentation procured by or transferred to WHC is assigned an appropriate "approval designator"; for designating system administrators and alternates; for designating engineers who have the technical ability and authority to change software related to their plant system; and for being cognizant of the requirements contained in WHC-CM-3-5, *Document Control and Records Management Manual*.

2.2.2 System Administrator (MICON Cognizant Engineer)

The system administrator, or MICON Cognizant Engineer, is responsible for identifying the functional requirements of the computer software; for establishing the "approval designator" of the computer software documentation; for maintaining software documentation; for approving, implementing and tracking Engineering Change Notice (ECN); for implementing new Engineering Data Transmittal (EDT); for ensuring the configuration management requirements are followed; for revising existing software; for overseeing and ensuring the configuration and security of the system; for maintaining the system data directory; and for maintaining and storing the backup tapes and/or other backup media.

2.2.3 Facility System Cognizant Engineer

The Facility System Cognizant Engineer is responsible for approving ECNs for new software revisions, for identifying the functional requirements within the ECN, for reviewing and concurring with proposed changes, for authorizing changes to proceed, and for preparing any work packages necessary to implement or test the changes.

2.3 INTERFACE CONTROLS

The facility system and process P&ID drawings function as the mechanism which controls and defines the system interfaces. In general, the interface between the MICON system and the system which the MICON controls is at the digital/analog input/output terminals. All changes to P&ID drawings which show the MICON as the control system, shall be approved by the MICON Cognizant Engineer.

2.4 IMPLEMENTATION

Currently the MICON system to be installed at the aging waste Tank Farm is non-operational and will remain so until all users have been trained and all system configuration for groups, users, passwords and access levels have been validated to insure all software applications can be performed at the required system levels.

2.5 POLICIES, DIRECTIVES, AND PROCEDURES

Software shall be designed and developed in compliance with WHC-CM-4-2, *Quality Assurance Manual*, QR 19.0, "Software Quality Assurance Requirements", and WHC-CM-3-10, *Software Practices*, Section 6.0, "Configuration Control". The computer software design process shall follow the applicable guidelines of WHC-IP-1026, *Engineering Practice Guidelines*, EPG-2.0, "Engineering System Design Control". Computer software shall be design verified in accordance with WHC-CM-6-1, *Standard Engineering Practices*, EP-4.1, "Design Verification Requirements". Computer software shall be validated in accordance with WHC-CM-6-1, *Standard Engineering Practices*, EP-4.2, "Testing Practices". Computer software documents shall be approved and released in accordance with the following documents:

- WHC-CM-6-1, *Standard Engineering Practices*, EP-1.6, "Engineering Data Transmittal"
- WHC-IP-1026, *Engineering Practice Guidelines*, EPG-1.6, "Engineering Data Transmittal Processing"
- WHC-CM-6-1, *Standard Engineering Practices*, EP-1.7, "Engineering Document Approval and Release Requirements"
- WHC-IP-1026, *Engineering Practice Guidelines*, EPG-1.7, "Initial Release of Engineering Documents"

Computer software documents shall be revised in accordance with WHC-CM-6-1, *Standard Engineering Practices*, EP-2.2, "Engineering Document Change Control Requirements", and WHC-IP-1026, *Engineering Practice Guidelines*, EPG-2.2, "Engineering Document Change Processing".

3.0 ACTIVITIES

3.1 CONFIGURATION IDENTIFICATION

The primary documents which define and control the software configuration are the P&ID's, Logic Diagrams, and Tag Listings. These are the design basis documents which define the functional operation of the software.

To implement these functions they are entered into the MICON Distributed Control System (DCS), where the resulting information is internally stored in numerous data files. Most of the DCS files are unreadable, incomplete, or otherwise poorly suited for generating human-readable hard copies. Consequently; the DCS files will be controlled by version identification, rather than by actual content of, the file. A software release document will define the version of each file which is applicable to that release. The System Administrator is responsible for assuring (by test, inspection, etc) that the release meets the functions of the controlled design basis. Backup procedures will be employed to assure retrievability of each file version, and to ensure that the proper version is currently installed.

Three types of software related items need to be identified for the purposes of controlling revisions and installation:

Design Basis Documents which define the functional requirements:

1) P&IDs
2) Logics
3) Tag Lists

Commercial software which provides the application base:

4) Solaris
5) A/S VIEW

On-line configuration data files:

6) Controller Files (U32/RCM files)
7) Graphics Files
8) Annuncitor Config file
9) Group Config files
10) Trend Config file
11) Historian Config file

These are discussed in the following sections.

3.1.1 P&ID's (H-2-131060 thru H-2-131081)

The P&ID's define basic system functions, tagnames, and locations of interlocks and alarms. The P&ID's are H-2 drawings, and are identified and controlled in accordance with applicable drawing requirements.

3.1.2 Logic Diagrams (H-2-826366 thru H-2-826458)

The Logic Drawings define the required logic of the control system. The Logics Diagrams are H-2 drawings, and are identified and controlled in accordance with applicable drawing requirements. (Note: Custom graphics screens have been developed from the released H-2's to allow on-line viewing of the dynamic state of this logic; these graphics are distinct from the "source" H-2 Logic Diagrams, and are described in section 3.1.2.7.)

3.1.3 Tag Lists (WHC-SD-WM-CSWD-TBD)

The Tag Lists define attributes associated with each tag, such as descriptive name, range, units, alarm setpoints, and alarm priorities. Tag Lists will be released as a Supporting Document and identified in accordance with applicable requirements. Note that the released Tag Lists will not be the actual on-line tag database, but rather a document which defines requirements for the on-line database. The controlled Tag List may be a subset of the actual on-line database, in that it will define only those tags and attributes which are important to functional operation of the system.

3.1.4 Solaris software

The Solaris operating system is loaded identically on all four operator stations, except for minor adjustments to provide unique addresses for each station. Only recovery capability is needed. Recovery is most expeditiously provided by copying from one station to another, nevertheless, a tape backup will also be provided. Two backups of this software shall be created and retained in locked cabinets. One copy shall be kept by the System Administrator and the second shall be held by the Cognizant Manager.

3.1.5 A/S VIEW Software

A/S VIEW is also loaded identically on all four stations, except for minor addressing changes. Recovery can also be accomplished by copying between stations, with minor adjustments. Two backups of the A/S VIEW software shall be created and retained in locked cabinets. One copy shall be held by the System Administrator and the second shall be retained by the Cognizant Manager. These backups will only be used for recovery purposes.

The A/S VIEW and supporting software is located in the Run, display_builder, and DataViews directories on a SPARC II workstation. Backups of these files shall be kept on magnetic streaming tape, which shall be labelled. Any new release shall be labelled with the system identifier, the tape name (RUN BACKUP), the MICON Company's revision identifier of RUN, the owner's name (System Administrator or Cognizant Manager), and the date the backup was created. For example:

AY-AZ MICON DCS
RUN BACKUP
3.0.41
SYS. ADMINISTRATOR
09/10/94

This label shall be placed on the outer housing of the tape.

The following command executed from the *home* directory is used to copy the entire A/S VIEW system from a SPARC II workstation to a 150 MB streaming tape located in the tape drive named rst0.

```
tar cvf /dev/rst0 Run display_builder DataViews
```

The following command executed from the *home* directory may be used to extract the entire contents of previously saved A/S VIEW software from the 150 MB streaming tape to a SPARC II workstation hard drive.

```
tar xvf /dev/rst0 Run display_builder DataViews
```

3.1.6 RCM/U32 Configuration Files

Three unique files exist for each MICON controller that is configured using the MICON controller configuration utility. The three files are a link file, a controller file, and a "scroll" file. The configuration utility is designed to keep these three files consistent, which is necessary for the configuration program to function and to prevent corruption or loss of configuration data.

The **link file** provides linkage pointers for the program to correlate the other two files, but is an unreadable (binary) file.

The **controller file** is the file which is actually downloaded to the RCM-32 or U-32 controllers and compiled there to run the process. It is a C-language type program in ASCII format. The program is readable by experienced programmers of MICON systems, however, the lines of code are not commented and are sometimes too long to handle using normal UNIX tools.

The **scroll file** is an ASCII text file; the name is based on its use in the configuration utility. It provides a "user-friendly" list containing most of the parameters which are defined during the configuration process. Unfortunately, some of the details are ommitted or truncated, so that the complete configuration cannot be rebuilt from this file alone.

Configuration filenames must follow certain conventions. The scoll and link filenames have two parts. The first part identifies the MICON controller tag (as defined in file *devices.txt*) by relating it to the controller type (RCMA, RCMD, RCMDR, RCME, RCMF, or U32) and controller number. The controller number, which matches the number on the U-32 and RCM-32 hardware, is the hardware "slot" number for which the file was developed. The second part of the identifier is the name of the controller file, which can be up to 8 characters long and can be adjusted by the user. The convention which will be used is a shorthand notation to identify the RCM, followed by the revision number which is modified when the file is changed.

```
syntax:     [CONTROLLER TAG].[controller filename]
example:    RCMDR_20.dr20_r0
              |    |    |  |___ revision number
              |    |____|______ controller number
              |________________ controller type
```

The configuration files will be identified by the file name, size, date, and timestamp.

example of all three files:

```
scroll file:      RCMDR_20.dr20_r0  12345 SEP10 12:41
link file:        RCMDR_20_dr20_r0  23456 SEP10 12:42
controller file:  dr20_r0           34567 SEP10 12:41
```

When a change is implemented, the revision number in the file name will be incremented and the above identifier will change its values.

3.1.7 Graphics Files

Graphics files define the pictorial displays which have been developed specifically for this application. The system includes several hundred graphic displays and sub-drawings. Thirty-two displays (names) are reserved for the "P&ID displays", which mimic the P&ID's and are the normal operator interface screens. Because of their special names, these screens work uniquely with the IOK. Another set of (about 200) graphics shows the dynamic state of the control logic diagrams. Finally, there are several dozen sub-drawings, which are included by reference in the main graphics. Graphics filenames have a ".v" extension, and subdrawings have a ".sd" extension.

Graphics filenames are fixed and cannot change with revision number. Graphic files will be identified by the file name, size, date, and timestamp. Old revisions can be retained by giving them new names.

```
example:
current file:  ay101.v        40404   Sep10      12:41
old rev     :  ay101.96Sep10  40506   Sep10      12:41
```

3.1.8 Annunciator Configuration file

The annunciator configuration file defines the name of each of the possible 40 annunciator windows, which alarms will be grouped to actuate that window, and which graphic screen is to be associated. By design, the annunciators have been defined so that each one displays all the alarms associated with a single "P&ID" graphic display (except in a couple of cases where two annunciators were needed to hold all the screens alarms.)

The file which defines the annunciator groups will be identified by the name, size, date, and timestamp on the file, for example:

```
annunc.cfg    10101     Sep10       12:41
```

3.1.9 Process Groups files

The process group files define which tags are co-located together on the "faceplate" displays. Each group can display 0-8 tags. By design, the groups have been organized and numbered to correspond to the graphics screens, so that related process variables are together. One file defines the arrangment of all the process groups for the OCS, while a separate file is used to define each group for the LOI's. This results in a large number of files to define the LOI groups. However, by design, the LOI groups have been constructed to match those of the main console (OCS). Thus, only the OCS group configuration will be controlled; maintaining the LOI's consistent will be an implementation detail under the responsibility of the System Administrator. The group configuration will be identified by the name, size, date, and timestamp on the OCS group file:

```
group.cfg    20202      Sep10       12:41
```

3.1.10 Process Trends display configuration

The trend configuration file defines which tags are co-located on each trend display. Each trend can display 0-4 tags. By design, the trend groups have been organized and numbered to correspond to the graphics screens, so that related process variables are together. The file defining the trend displays will be identified by the name, size, date, and timestamp on the file, for example:

```
trendcnfg.cfg    30303   Sep10       12:41
```

3.1.11 Historian display configuration

The historian configuration file defines which tags are co-located on each historian display. Each display can show 0-4 tags. By design, the historian groups have been organized and numbered to correspond to the graphics screens, so that related process variables are together. However, for data space considerations, only selected variables are recorded in the history file, so consequently there are fewer historian displays than trend displays. The file defining the historian displays will be identified by the name, size, date, and timestamp on the file, for example:

```
histcnfg.cfg    30303   Sep10       12:41
```

3.1.12 Release Document

The software release document defines the files and versions applicable to a particular identifiable version of the software. It shall identify the applicable versions of each of the above software items (as described in sections 3.1.1 thru 3.1.11). The release document establishes an identifiable and auditable "Release Version" for each step change in the software configuration. The release identifier shall be in the following form:

```
syntax:         M.N[a]      : M=[1..], N=[0..], a=[a-z]
example1:       1.0         : Initial release
example2:       2.3a        : Error correction to version 2.3
```

The first numeral ("M") is intended for significant or major evolutions of the software. The second numeral ("N") would be incremented for a series of minor upgrades. Finally, the optional alpha-character ("a") would be used to signify correction of errors in the prior release.

A utility has been prepared to generate the Release Document automatically. Each change (as described in section 3.2) shall be identified as a new "Release" and include a new Release Document.

3.1.13 Data Directory (Application Software) Backup

The application programs and files listed above (Sections 3.1.6 thru 3.1.11) are stored in the /home/Data directory on the SPARC II workstation, and shall be backed up for each Release Version. (The security access files are also included in the /home/data directory.) Two backups shall be created and retained in locked cabinets. One copy shall be held by the System Administrator and the second shall be retained by the Cognizant Manager.

Backups shall be kept on magnetic streaming tape, which shall be labelled. The label shall contain the system identifier, tape name (DATA BACKUP), volume name, the owner's name (System Administrator or Cognizant Manager), and the date the backup was created. For example:

AY-AZ MICON DCS
/DATA BACKUP
VOLUME 1 OF 1
SYS. ADMINISTRATOR
09/10/96

This label shall be placed on the outer housing of the tape.

The copy and extract commands are the same as described in section 3.1.2.5 except that *Data* is substituted for *Run*. These operations are again executed from the *home* directory. For example:

```
copy SPARC to tape:     tar cvf /dev/rst0 /home/Data

extract tape to SPARC:  tar xvf /dev/rst0 /home/Data
```

3.2 CONFIGURATION CONTROLS

Two categories of software revisions are defined as:

Major Changes, which affect the configuration basis documents - P&ID, Logic diagrams, and/or Tag Lists as defined in sections 3.1.1 thru 3.1.3.

Minor Changes, which do not affect these baseline documents, but only their implementation into the MCS data files. By definition, such changes do not affect process operation, but only the manner of presentation to the operator. Examples would be adjustments to the display screens or revising the trend displays. Minor Changes do not require an ECN, but will be controlled as specified in this document.

3.2.1 Problem Tracking

Problems, faults and failures will be documented and tracked at the discretion of operations.

3.2.2 Job Control System

Software changes which will affect the process operation will be part of a Job Control System (JCS) work package to control the overall revision and testing activity. (Reference WHC-CM-8-8). The specific problem or change needed shall be documented on a JCS J-1 Work Request and processed in accordance with WHC-IP-0842, *Waste Tanks Administration*, Section 9A.5, "Job Control System".

Assuming modifications are required to resolve or correct the problem, the engineering process shall be documented in accordance with WHC-CM-6-1, *Standard Engineering Practices*, and WHC-IP-1026, *Engineering Practice Guidelines*. The resulting ECN shall be developed, processed, approved, and released in accordance with WHC-CM-6-1, *Standard Engineering Practices*, EP-2.2, "Engineering Document Change Control Requirements", and WHC-IP-1026, *Engineering Practice Guidelines*, EPG-2.2, "Engineering Document Change Processing".

3.2.2 Software Change Form

All revisions to the software identified in section 3.1 shall be initiated and tracked by preparing a software change request in accordance with Figure 1. A log and master copy of all change requests shall be maintained. Figure 2 gives a sample form for the Log information.

For **Major Changes**, an ECN describing the desired changes to the configuration basis documents (Ref. 3.1.1-3.1.3) may accompany the Software Change Request, but in any case, must be prepared and approved prior to installing the software change. The MICON Cognizant Engineer must sign all ECNs and, in addition, the System Cognizant Engineer of the affected plant or process system must also sign and approve the ECN.

For **Minor Changes**, the configuration basis documents are not affected, so the change request describes the desired change. For simple changes, the MCS SOFTWARE CHANGE form may be all that is needed to authorize and track the work. In the more general case, the MCS SOFTWARE CHANGE form would be part of a JCS work package.

Approval by the Change Authority, typically the Facility System Cognizant Engineer, shall be required to proceed with implementation. The System Cognizant Engineer is responsible to assure that applicable reviews have been performed.

3.2.3 Preparing the Change

After approval to proceed, the System Administrator shall incorporate and test the change to the maximum extent possible on the (off-line) Engineering Workstation. The prior file versions shall be retained so that the configuration can be restored to the prior Release Version.

3.2.4 Installing and Testing the Change

After installation on the actual control system, the change shall be tested commensurate with the extent and nature of the change. Some Minor Changes, such as a display-only change, do not affect the process and may be performed under the authority of the Software Change Request. More extensive changes may require a JCS work package to organize the resources and system operations to conduct the test.

3.2.5 New Release Version

After the change has been installed and successfully tested, the Release Version documentation (Section 3.1.12) and backup media (Section 3.1.13) are prepared.

3.2.6 Change Request Closeout

Closeout of a change request shall identify the changes and testing performed to implement the change. Also the new Release Version shall be be either identified or attached. The status of open and completed Software Change Requests shall be tracked.

3.3 CONFIGURATION STATUS ACCOUNTING

Section 3.1, Configuration Identification, descibes how individual components are identifed, including their revisions. The software Release Document prescribes the versions of each file which constitute a particular release. The Change Request forms relate the functional changes to the affected files, and identify the resulting Release Version. All files applicable to a particular release are backed up and can be retrieved.

3.4 AUDITS AND REVIEWS

Yearly, the System Administrator shall review the software for completeness and correctness. The Release Document shall be reviewed against the current operating software to ensure that the correct software is in place.

It is also crucial to ensure that operating software are maintained per the requirements laid down in this plan. To ensure this, internal and independent audits are planned.

3.5 ACCESS CONTROL

The MICON security system is configured completely by the System Administrator, who defines the security system layout, passwords, user capabilities and restrictions.

The System Administrator assigns each user (ie: operators, supervisors, etc.) to a user group. Each group of users is assigned certain capabilities to perform operations, along with certain restrictions. If a user is assigned the capability with restrictions, then a password is required to perform the operation.

Four groups of users have been defined, as described below. All of these groups may not necessarily be implemented or given access. As a minimum, the system administrator and operator are required to have access to the system.

3.5.1 System Administrator

The System Administrator (MICON Cognizant Engineer) has the highest access level and is permitted any and all software operations including access to security data file (password assignments), changes to access levels, and breadth of operations. There will be one alternate System Administrator who will be designated by the Cognizant Manager.

3.5.2 Engineer

The Engineer access level is similar to that of the System Administrator but does not permit access to security files and password information. Engineers are also nominally restricted in their access to normal process operation commands; however, since they (must) have access to the underlying logic for setup and configuration, this restriction is not absolute.

3.5.3 Operator

The Operator group consists of the nuclear operators and their supervisors. In general, this group can control and monitor facility systems and processes. The group can change equipment settings within the prescribed operating ranges, alter equipment line up, select approved data displays, backup operating files, and print historical and operational data.

Trainee. The trainee is a subset of the Operator group, with a "look-only" restriction, so that they cannot operate the process.

Supervisor. The supervisor is an Operator, with the additional authority to inhibit alarms. Supervisor requires an additional password.

3.5.4 Technician

The Technician group is for instrument technicians who are assigned access levels which will permit testing and maintenance of the system to include trouble-shooting hardware. Limited changes and adjustments to input and output parameters are permitted. Breadth may be limited to specific cabinets, buildings, or systems.

3.6 BACKUP AND RECOVERY

Media control is exercised to ensure that the Sun, MICON, and Hanford-developed software is backed up after each modification. Backup media will allow reconstruction of the computer within a few work days. Two sets of backups are maintained and stored in locked file cabinets, which are located so that there is a sufficient distance from the application location. A single backup set includes the streaming tapes for the Run and Data directories. One set of media shall be held by the system administrator and the second set shall be retained by the Cognizant Manager.

The system administrator will maintain at least two preceding sets of removal media before releasing all the older media copies for other uses. These two prior backups will remain so that if during the modification process, the entire system crashes or is lost, the last operating computer software can be used to regenerate the operating files and recover.

Historical data files will be transferred to 150 megabyte tapes weekly or monthly as necessary. These tapes are maintained in the Control Room for at least six months after which time they can be cleared for reuse or temporarily archived (up to three years). Archives will be secured by the system administrator.

A label shall be placed on the tape cover. The label shall contain the system identifier, tape name (HISTORICAL DATA), start and end dates representing the time period of collected data, and a volume name. For example:

AY-AZ MICON DCS
HISTORICAL DATA
09/10/96 TO 09/16/96
VOLUME 1 OF 1

4.0 TOOLS, TECHNIQUES, AND METHODOLOGIES

There are no additional tools, techniques, or methodologies required in maintaining configuration control other than those supplied as part of the commercially available MICON and Solaris software.

To facilitate revision accounting per this document, a custom UNIX script has been prepared to generate the "Release Document" described in section 3.1.12. The Release script is located in the "/home" directory, and is invoked by entering the command "Release".

5.0 SUPPLIER CONTROL

Solaris and A/S VIEW are commercially available products produced by their respective suppliers. MICON has combined these two products into a integrated and tested system which they market competitively, and which was supplied to meet our specification. We have no explicit control over their software development process. Suitability for our application has been demonstrated by acceptance testing at various stages.

Problems or issues which require revisions to Solaris or A/S VIEW will be transmitted to the Supplier, probably MICON initially. The Supplier will make and test any revisions in accordance with their internal methodology. Prior to implementing the revision, the MICON Cognizant Engineer shall at a minimum assure that:

1. The Supplier provides a list of all changes made to the affected software.
2. The identified changes do not adversely affect functions which our application is using.
3. Suitable tests are conducted to verify that our application still performs its essential functions under the new software.

6.0 RECORD COLLECTION AND RETENTION

Historical Data Files shall be collected and retained by the system administrator for a minimum of 6 months.

7.0 REFERENCES

WHC-CM-1-3, *Management Requirements and Procedures*
MRP 3.13, "Acquisition of Automatic Data Processing Systems, Equipment, and Related Resources"
MRP 5.46, "Safety Classification of Systems, Components and Structures"

WHC-CM-3-5, *Document Control and Records Management Manual*
12.7, "Approval of Environmental, Safety, and Quality Affecting Documents"

WHC-CM-3-10, *Software Practices*

WHC-CM-4-2, *Quality Assurance Manual*
QR 19.0, "Software Quality Assurance Requirements"

WHC-CM-6-1, *Standard Engineering Practices*
EP-1.6, "Engineering Data Transmittal Requirements"
EP-1.7, "Engineering Document Approval and Release Requirements,"
EP 2.2, "Engineering Document Change Control Requirements"
EP-4.1, "Design Verification Requirements"
EP-4.2, "Testing Requirements"

WHC-CM-8-8, *Job Control System*

WHC-IP-0842, *Waste Tank Administrative Procedures*
Section 9A.5, "Job Control System"

WHC-IP-1026, *Engineering Practice Guidelines*
EPG-1.6, "Engineering Data Transmittal Processing"
EPG-1.7, "Initial Release of Engineering Documents"
EPG-2.2, "Engineering Document Change Processing"

WHC-SD-WM-CSWD-071, *Aging Waste Tank Farm MICON Distributed Control System Computer Software Documentation*

Figure 1: W-030 Change Request / Problem Report

CR/PR Number ____________

Page 1 of ____

1. Software/Document Identification (Name): ______________________________

2. Prepared by: ______________________________ Date: ____________

System Name: ______________________________ TPCN, W/O: ____________

3. CR/PR Type: [ ] Change Request [ ] Problem Report Requested Completion Date: ____________

4. Description:

5. Justification if Change Request:

6. Submitter's Priority [ ] Routine [ ] High [ ] Emergency

7. Change Authority: ____________ [ ] Accept [ ] Modify [ ] Reject [ ] Defer Until: ________

8. Assigned to: ____________ Planned Release Date: ____________

9. Solution Comments Cost/Schedule Estimate: __________ / __________

10. Software/Documents Affected:

11. Testing:

12. Approvals Indicate CR is Complete or PR is Resolved. Release No. ____________

System Developer: ____________________ Date: ____________

Responsible Manager: ____________________ Date: ____________

CR or PR Preparer: ____________________ Date: ____________

Other: ____________________ Date: ____________

Change Request and Problem Report Instructions:

These instructions provide guidelines for preparing the CR/PR.

1. Record document identification or name for the CR/PR.

2. Record the name of the person preparing the form, date, system name, and Task Package Control Number (TPCN) or Work Order (W/O) to which the work is to be charged.

3. Indicate if this is a change request or problem report and the requested completion date.

4. Provide a description of the changes requested or the problems being reported. When appropriate, describe any effect the requested change may have on the other systems.

5. Provide justification if this is a change request.

6. Indicate preparer's priority.

7. The person with change control authority signs and indicates whether the decision is to accept, modify, reject, or defer the CR/PR until the specified date.

8. Indicate to whom the CR/PR is assigned, and provide a planned release date.

9. Describe the (planned) solution and an estimate of the cost and schedule.

10. Describe software and/or documents affected by the solution. Reference and/or attach applicable ECN's.

11. Describe how the change was verified. Reference or attach applicable documents.

12. Record approvals indicating requested changes have been completed or the problem report resolved. Record the software release number which implements the change.