DISTRIBUTION SHEET

To	From	Page 1 of 1
Distribution	Tank Farm Projects	Date 04/27/95
Project Title/Work Order		EDT No. 607934
Computer Software Configuration Management Plan for the 241-AY and 241-AZ Tank Farm MICON Automation System		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

607934

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 configuration management plan 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-CSCM-028		0	Computer Software Config. Management Plan 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 2. Release 3. Information 4. Review 5. Post-Review 6. Dist. (Receipt Acknow. Required)	1. Approved 2. Approved w/comment 3. Disapproved w/comment	4. Reviewed no/comment 5. Reviewed w/comment 6. Receipt acknowledged

(G)	(H)	17. SIGNATURE/DISTRIBUTION (See Approval Designator for required signatures)				(G)	(H)				
Reason	Disp.	(J) Name	(K) Signature	(L) Date	(M) MSIN	(J) Name	(K) Signature	(L) Date	(M) MSIN	Reason	Disp.
1,2	1	Cog. Eng. F.T. CLIFTON	<i>[Signature]</i>	3/16/95	G6-06	M.C. TEATS	<i>See below</i>		R1-43	3	1,2
1,2	1	Cog. Mgr. K.A. COLDS	<i>[Signature]</i>	3/14/95	G6-27						
1,2	1	QA H.M. CHAFIN	<i>[Signature]</i>	3/13/95	G6-07						
1,2	1	QA M.L. HERMANSON	<i>[Signature]</i>	3-9-95	A4-79						
		Safety									
		Env.									

18. Signature of EDT Originator <i>M.C. Teats</i> 3/16/95	19. Authorized Representative for Receiving Organization <i>[Signature]</i> 3/15/95	20. Cognizant Manager <i>[Signature]</i> 3/14/95	21. DOE APPROVAL (if required) Ctrl. No. ☐ Approved ☐ Approved w/comments ☐ Disapproved w/comments
--	--	---	---

RELEASE AUTHORIZATION

Document Number: WHC-SD-WM-CSCM-028, Rev. 0

Document Title: Computer Software Configuration Management Plan 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 29
2. Title Computer Software Configuration Management Plan for the 241-AY and 241-AZ Tank Farm MICON Automation System	3. Number WHC-SD-WM-CSCM-028	4. Rev No. 0
5. Key Words W-030, MICON, Configuration Management	6. Author Name: M. C. Teats <i>M.C. Teats</i> 4-26-95 Signature Organization/Charge Code 71730/NB103	
7. Abstract Software configuration items are identified and configuration controls are defined.		

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

MASTER

A-6400-073 (08/94) WEF124

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

et

COMPUTER SOFTWARE CONFIGURATION MANAGEMENT PLAN
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 DEFINITIONS	2
1.4 SECURITY	6
1.5 HARDWARE/SOFTWARE DESCRIPTION	7
2.0 MANAGEMENT	10
2.1 ORGANIZATION	10
2.1.1 System Administrator	10
2.1.2 Engineer	10
2.1.3 Operator	10
2.1.4 Technician	11
2.2 RESPONSIBILITIES	11
2.2.1 Cognizant Manager	11
2.2.2 System Administrator	11
2.2.3 System Cognizant Engineer	11
2.2.4 Configuration Management	11
2.2.5 Information Resource Management	12
2.3 INTERFACE CONTROLS	12
2.4 IMPLEMENTATION	12
2.5 POLICIES, DIRECTIVES, AND PROCEDURES	12
3.0 ACTIVITIES	13
3.1 CONFIGURATION IDENTIFICATION	13
3.1.1 Software Documentation	13
3.1.2 Software Identification	13
3.1.3 Problems, Faults, and Failures	17
3.1.4 Changes and Enhancements	17
3.2 CONFIGURATION CONTROLS	18
3.2.1 Software Changes	18
3.2.2 Access Levels	18
3.2.3 Backup and Recovery Operations	19
3.2.4 Historical Data File	19
3.3 CONFIGURATION STATUS ACCOUNTING	19
4.0 TOOLS, TECHNIQUES, AND METHODOLOGIES	21
4.1 CONFIGURATION CONTROL TOOLS	21
4.2 APPLICATION BUILDING STEPS	21
5.0 SUPPLIER CONTROL	22
6.0 RECORD COLLECTION AND RETENTION	23
7.0 REFERENCES	23

LIST OF FIGURES

1 MICON System Architecture	7
---------------------------------------	---

1.0 INTRODUCTION

1.1 PURPOSE

This document establishes a Computer Software Configuration Management Plan (CSCMP) for controlling software for the MICON¹ 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 CSCMP 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 3.3).

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 will 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 Engineering Cognizant Manager and MICON Cognizant Engineer (which will be 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-32² and RCM-32² controllers.

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 II workstation.

Commercial Software

Licensed or copyrighted off-the-shelf software that is not subject to Westinghouse Hanford Company (WHC) design or specification requirements unique to WHC and is typically used in applications other than WHC 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, spread sheets, 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).

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

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).

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).

Group

A level of access to plant components related to the MICON system. Access levels are defined by the system administrator for each individual or group of individuals.

Group text file

Consist of variables which defines the parameter for the group displays that facilitates a user's interaction with their system.

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.

PID Controller

A process controller (flow, level, pressure, temperature and so on) using the Proportional-plus-Integral-plus-Derivative (PID) algorithm.

Pipe and Instrument Diagram (P&ID)

A schematic of a manufacturing 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 PID control, logic control, 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 System Cognizant Engineer responsible for maintaining control of computer software, computer software media, and their access.

Solaris software

Proprietary software containing the UNIX³ operating system and the X-Window⁴ 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.

System Life Cycle

The period of time that begins when a system is conceived and ends when the system is no longer available for use. (IEEE Std. 610.12-1990).

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.

Transceiver

A device which allows Ethernet devices to be connected to an Ethernet⁵ Local Area Network.

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).

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

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

5. Ethernet is a trademark of the Xerox Corporation.

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 PID 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 LCUs and 2 Remote Control Units).

Each console is based on a Sun Microsystems Scalable Process Architecture (SPARC) II workstation. Each workstation contains 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 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.

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 three 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. Neither GPLI monitors both highways, but each GPLI is dedicated to monitoring only one highway. For a network having only one pair of GPLIs, this means that if a GPLI fails then 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, with LCU-3 and LCU-4 each being connected to a Remote Control Unit (RCU). The RCUs (not shown in Figure 1) contain RCM-32 controllers and 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. Although a U-32 controller can be used to directly control plant equipment, its primary purpose is to pass information between the GPLIs and the RCM-32 controllers. In addition, the U-32 controllers of LCU-1 and LCU-2 provide for the redundancy of Safety Class 2 controls. Each U-32 has a redundant backup. The RCM-32 controllers perform most of the control and logic functions and provide the wiring terminations for the inputs and outputs to plant equipment. The RCM-32 controllers are not physically redundant, although Safety Class 2 controls are redundant by software logic and hardware design. The U-32s and RCM-32s communicate 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). If the RCM-32 controllers were redundant, then the field bus would also be redundant. An LOI (not shown in Figure 1) is 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 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, C, D, and Dr. The A and C cards are used primarily for analog signals. They provide hardware for any standard analog instrument input (4-20 milliamp, and DC voltages) and provide a standard 4-20 milliamp output signal. 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 C card provides 18 analog inputs and 12 analog outputs. The D card is used only 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. This is a database of all process information that can be displayed and/or recorded by the system.

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 the source is compiled.

The UNIX, X-Window Motif, A/S VIEW, RTS-C operating system, and the MICON controller program compiler programming 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 covered by this document.

2.0 MANAGEMENT

2.1 ORGANIZATION

There are four groups of system users and these groups define the level of access to the data files and other programmable files within the MICON A/S OPEN. These access levels permit certain operations and exclude others. The breadth of these operations may also be limited depending upon the user group. The groups are defined below in terms that not only relate them to Tank Farm organizational elements, but also to operations that are permitted or restricted under the MICON A/S OPEN access control system. 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. Engineer and technician may or may not have access to the system.

2.1.1 System Administrator

The system administrator is the MICON cognizant engineer. The system administrator 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 designed by the System Engineering Cognizant Manager.

2.1.2 Engineer

The engineer access level is immediately below that of the system administrator but does not permit access to security files and password information. Engineers are also restricted in the breadth of operation and may only change software that controls and monitors their system or process. For example, the HVAC cognizant engineer has the capability (meaning ability and proper authorization) to change software configuration and data displays only for the HVAC system and is denied access to similar operations dealing with tank sludge washing systems or other systems. The engineer is a system cognizant engineer and is required to have a single backup who will have the same access level and breadth restrictions as the system cognizant engineer.

2.1.3 Operator

The operator group consists of the nuclear operators and their supervisors. The access level of this group permits all operations which would be ordinarily permitted if the MICON system was not available. 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. Breadth of control can be limited to specific systems and processes.

2.1.4 Technician

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

2.2 RESPONSIBILITIES

2.2.1 Cognizant Manager

The cognizant manager, who is the system administrator's 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 procedure 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

The system administrator 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 ensuring that the physical data model meets the intent of the logical model; for maintaining the system data directory; and for maintaining and storing the backup tapes and/or other backup media.

2.2.3 System Cognizant Engineer

The system cognizant engineer is responsible for approving ECNs for new software revisions and for identifying the functional requirements within the ECN.

2.2.4 Configuration Management

Configuration Management is responsible for assigning a supporting document number to the computer software document and for releasing the computer software documents.

2.2.5 Information Resource Management

Information Resource Management (IRM) is responsible for providing appropriate vault storage for record copy of software documentation and for providing appropriate records management requirements.

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 and the ECN shall show the supporting document (WHC-SD-WM-CSWD-071, Aging Waste Tank Farm MICON Distributed Control System Computer Software Documentation) containing the software documentation as an "impacted document" in Block 19.

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

3.1.1 Software Documentation

All software associated with the MICON Distributed Control System shall be documented in a supporting document (WHC-SD-WM-CSWD-071, Aging Waste Tank Farm MICON Distributed Control System Computer Software Documentation). The supporting document will contain the software in hard copy text format. It will also contain the data files for the operator and engineering consoles, the group text file, a listing of the graphics files, and instructions for installing the Solaris and A/S VIEW software.

3.1.2 Software Identification

This supporting document identifies six items which will have identification for controlling revisions and installation. These items are listed below and shall meet WHC-CM-3-10, *Software Practices*, SP-6.2, "Software Control", Sections 5.1.1 (Software Identification) and 5.1.2 (Revision Identification).

3.1.2.1 Solaris software

The Solaris software is contained on a CD ROM disk and will only be used for recovery purposes. 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.

3.1.2.2 A/S VIEW Software

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 contents of the Run directory 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
```

3.1.2.3 Configuration File

Three unique files exist for every MICON controller that is configured using the MICON controller configuration utility. The three files are a binary linked-list file, a controller file, and a configuration file. These files shall be backed up on magnetic media as described in Section 3.1.2.5. The linked-list file is unreadable and not useful in the form of hardcopy documentation. Future enhancements to the configuration utility may eliminate the creation of this file when building applications.

The controller file is downloaded to the RCM-32 or U-32 controllers and compiled there. It is a C-language program in ASCII format. Although the program is readable by experienced programmers of MICON systems, the lines of code are not commented and are not easily understood. The controller file by itself therefore is not suitable for software documentation in hardcopy form. The program shall be proven operable by the engineer and system administrator before it is implemented.

The configuration file, sometimes referred to as the scroll file based on its use in the window environment of the configuration utility, is an ASCII text file. It is a program listing containing all of the user-defined parameters of the U-32 and RCM-32 controller functions. This file can be commented, is readable, and is easily understood by

individuals having some experience with MICON controller functions. This is the file used to document applications software for the U-32 and RCM-32 controllers.

Configuration files are named in two parts. The first part uses upper case lettering and the second part is in lower case. The first part identifies the MICON controller tag (in *devices.txt*) by relating it to the controller type (RCMA, RCMB, RCMC, RCMD, RCMDr, RCME, RCMF, RCMZ, or U32) and controller number. The controller number, which matches the number on the U-32 and RCM-32 hardware, is the sequence number into which the file was developed. The second part of the identifier is the name of the controller file. The controller file name also consists of two parts; the controller number prefaced by ".mic", and the revision number which is modified when the file is changed.

syntax: [CONTROLLER TAG].[controller file name]
 example: RCMDR_20.mic20_r0

revision number
 controller number
 controller type

The configuration file will be identified by the file name, size, month, date, and time.

example: RCMDR_20.mic20_r0 202031 SEP10 12:41

Any modification to this file will be through an ECN. When a change is implemented, the revision number in the file name will be incremented and the above identifier will change its values. This along with a hard copy of the program listing will be placed in the computer software description document (WHC-SD-WM-CSWD-071, Aging Waste Tank Farm MICON Distributed Control System Computer Software Documentation).

3.1.2.4 The Graphics Files

The file name of a graphic relates to the graphic presentation, meaning the file name will be visible in the graphic display on a workstation.

Graphic file names are assigned by the system administrator, and file extensions (.v) are created by the MICON graphic building utility. Graphic files will be identified by the file name, size, month, date, and time.

example: ay101.v 202031 SEP10 12:41

Any modification to this file will be through an ECN. Prior to changing the graphic, the system administrator will ensure a backup file exists or is made (see section 3.1.2.5). Once the change has been implemented, the existing file will be replaced causing the above identifier to change its values. This directory list will be placed in the software description supporting document (WHC-SD-WM-CSWD-071, Aging Waste Tank Farm MICON Distributed Control System Computer Software Documentation).

3.1.2.5 Data Directory (Application Software) Backup

The programs and files listed above (Sections 3.1.2.3 and 3.1.2.4), which are stored in the Data directory on a SPARC II workstation, shall be backed up every time there is an ECN for a modification to any one them. Two backups of the application 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. The backups shall also contain the access level security files and files within the following directories:

- /home/Data/Oconfig
- /home/Data/Dbase
- /home/Data/Dsystem
- /home/Data/Kbfiles
- /home/Data/AOS
- /home/Data/BOS
- /home/Data/L4H
- /home/Data/L4G
- /home/Data/BOB

Files in the AOS and BOS directories are for S-32 configurations, and files in L4H are for P-200 configurations. Directories L4G and BOB are empty directories.

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 09/10/94

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

The copy and extract commands are the same as described in section 3.1.2.2 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 Data
extract tape to SPARC: tar xvf /dev/rst0 Data
```

3.1.3 Problems, Faults, and Failures

Problems, faults and failures will be reported, controlled, processed, corrected, retested, and closed out using the Job Control System (JCS) described in WHC-CM-8-8. The specific problem, fault, or failure 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". If 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".

3.1.4 Changes and Enhancements

Occasionally, software may need to be modified although there is no problem with the existing software. Typically, these kinds of modifications are the result of new projects, new designs, or enhancements to existing software to provide new functionality. This kind of work shall be processed using the JCS described in WHC-IP-0842, *Waste Tanks Administration*, Section 9A.5. Any resulting ECNs 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 CONFIGURATION CONTROLS

3.2.1 Software Changes

Software (commercial and applications) will be controlled using the JCS described in Sections 3.1.3 and 3.1.4. The JCS provides a vehicle to track changes and also notify plant personnel of any changes. Prior to installing a change, system backups will exist and the change will be reviewed for possible impacts. After installation, the change will be verified by a performance check. If the change is acceptable, new backup media will be created as described in Section 3.1. If necessary, the old version can be restored.

The approval process for ECNs is defined in EP-2.2. 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.

Minor pen and ink changes may be made using a supplemental ECN; however, each data file is limited to five supplemental ECNs before it must be issued as a revision. The pen and ink change is made and a notation in the margin is made indicating the number of the ECN authorizing the change, the date the change is entered, and the initials of the individuals making the change.

Page change revisions may also be issued; however, these are considered direct revisions and require a Record of Revision, an Information Release Request, Supporting Document Cover Sheet, and a new title page. The new pages will carry the current revision number followed by a hyphen and a letter which is the next higher alpha character. For example, if the supporting document is Rev. 0, the affected pages of the document are identified as Rev. 0-A.

Section 3.1.2 discusses how data files on the SPARC II workstation hard drives are identified and what the duplication requirements are for these files.

3.2.2 Access Levels

The MICON security system is configured completely by a 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 (read, write, download, etc.), along with certain restrictions. If a user is assigned the capability with restrictions, then a password is required to perform the operation. Each operation type is assigned an access level to perform an operation, restricted or not.

Each data point is assigned a point access level. A user must possess sufficient access level to perform an operation on a protected point. Additionally, an optional point password may be required.

3.2.3 Backup and Recovery Operations

Media control is exercised to ensure that the Sun, MICON, and WHC-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, and the Solaris CD ROM disks. 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.

3.2.4 Historical Data File

Historical data files are 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 09/10/94 TO 09/16/94 VOLUME 1 OF 1

3.3 CONFIGURATION STATUS ACCOUNTING

The JCS will be used to status changes resulting from problems or enhancements. The JCS provides a method to notify personnel of changes and track them. Log books may be used in addition to, but not replace, the JCS records. JCS records shall be official, whereas log book entries shall be for convenience only.

Twice yearly, the system administrator shall review the software for completeness and correctness. The media software loop 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.

4.0 TOOLS, TECHNIQUES, AND METHODOLOGIES

4.1 CONFIGURATION CONTROL TOOLS

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

4.2 APPLICATION BUILDING STEPS

Simplified steps for building application software from scratch are summarized in this section. Details of these steps are supplied in the available MICON documentation.

1. Establish a philosophy of system security. Security access levels and breadth of allowed operations are established for the various user groups.
2. Clear Tag Def, Clear GPLI Def, and Clear Controller Def.
3. Delete *GPLIDEF.DAT* and *MCNDEF.DAT* in Dbase directory.
4. Configure GPLI (from Controller Configure utility) to create *GPLIDEF.DAT*.
5. Define U-32 and RCM-32 Controller tags (from Controller Configure utility) to create *devices.txt*, or create *devices.txt* from spreadsheet or Sun operating system editor.
6. Define all tags for each controller (from Controller Configure), or define tags from spreadsheet or Sun operating system editor.
7. Configure U-32 and RCM-32 controllers (from Controller Configure utility) to create the linked-list, scroll, and controller files. Include entry of system security parameters.
8. Configure group displays.
9. Define hardware using GPLI Definition and Controller Definition utilities.
10. Define and download GPLI LAN Manager and U-32 LAN Manager tables.
11. Define trend displays.
12. Define Local Operator Interface (LOI) displays.
13. Define annunciator windows.
14. Create graphics.

5.0 SUPPLIER CONTROL

1. The MICON Company cognizant manager ensures that the specification for the product to be provided, and the requirements for testing, installation, configuration control, maintenance, and operation of the system for the duration of the contract are specified.
2. The MICON Company cognizant manager ensures the product acceptance criteria are specified.
3. The MICON Company cognizant manager ensures the deliverable software to be provided by the supplier are specified.
4. The Tank Farm System Engineering Cognizant Manager ensures the minimum documentation required for the contract-developed, quality affecting software is specified in or included with the:
 - Inter contractor work authorization, or
 - Application/implementation plan (see WHC-CM-1-3, MRP 3.13, "Acquisition of Automatic Data Processing Systems, Equipment, and Related Resources").
5. The minimum set of deliverables (see WHC-CM-4-2, QR 19.0, Section 4.6.1) required for contract-developed, quality affecting software is software source code on machine-readable media and the following documentation:
 - System requirements specifications,
 - System design description,
 - User documentation, and
 - Verification and validation records, including test procedures, test case specifications, and test results.

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*

This page intentionally left blank.