

Star 5
JAN 20 1997

12

ENGINEERING DATA TRANSMITTAL

Page 1 of 1

1. EDT

619160

2. To: (Receiving Organization) Distribution	3. From: (Originating Organization) PFP Process Engineering	4. Related EDT No.: N/A
5. Proj./Prog./Dept./Div.: 15530	6. Cog. Engr.: W.S. Lewis	7. Purchase Order No.: N/A
8. Originator Remarks: Release this Computer Software Configuration Management Plan.		9. Equip./Component No.: N/A
		10. System/Bldg./Facility: 73T/234-5Z/PFP
11. Receiver Remarks: 11A. DESIGN BASELINE DOCUMENT? <i>[] YES <i>1</i> [] NO</i>		12. Major Assm. Dwg. No.: N/A
		13. Permit/Permit Application No.: N/A
		14. Required Response Date: 11/22/96

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 Trans- mittal	Orig- inator Disposi- tion	Receiv- er Disposi- tion
1	WHC-SD-CP-CSCM-009	-	0	Computer Software Configuration Management Plan for the Honeywell Modular Automation System	Q	1		

16. KEY												
Approval Designator (F)		Reason for Transmittal (G)				Disposition (H) & (I)						
E. S. Q. D. or N/A (see WHC-CH-3-5, Sec 12.7)		1. Approval	4. Review	1. Approved	4. Reviewed no/comment	5. Post-Review	2. Approved w/comment	5. Reviewed w/comment	3. Information	6. DISC. (Receipt Acknow. Required)	3. Disapproved w/comment	6. Receipt acknowledged
(G)	(H)	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)	Reason	Disp	
1	1	Cog. Eng.	W.S. Lewis	12-26-96	T5-55	L.T. Cunningham	12-26-96	T5-55	1	1		
1	1	Cog. Mgr.	M.W. Gibson	12-26-96	T5-55	J.F. Durnil	12-26-96	T5-55	1	1		
1	1	QA D.R. Groth	12-26-96	T4-15								
		Safety										
		Env.										

18.	19.	20.	21. DOE APPROVAL (if required)
<i>L.T. Cunningham 12-3-96</i>	<i>ATL-JL 12-3-96</i>	<i>M.W. Gibson 12-3-96</i>	Ctrl. No.
Signature of EDT Date Originator	Authorized Representative Date for Receiving Organization	Cognizant Manager	<input type="checkbox"/> Approved <input type="checkbox"/> Approved w/comments <input type="checkbox"/> Disapproved w/comments

COMPUTER SOFTWARE CONFIGURATION MANAGEMENT PLAN FOR THE HONEYWELL MODULAR AUTOMATION SYSTEM

L.T. Cunningham

B & W Hanford Co., Richland, WA 99352

U.S. Department of Energy Contract DE-AC06-87RL10930

EDT/ECN: 619160

UC: UC-506

Org Code: 15530

Charge Code: K6134

B&R Code: EW7003000

Total Pages: 15

Key Words: Honeywell, Modular Automation System, Computer Software Management Plan

Abstract: This document provides a Computer Software management plan for a new Honeywell Modular Automation System (MAS) being installed in the Plutonium Finishing Plant (PFP). This type of system will be used to control new thermal stabilization furnaces, a vertical denitrator calciner, and a pyrolysis furnace.

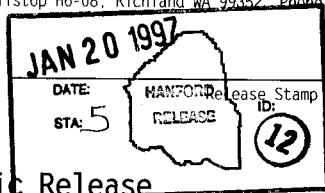
Honeywell is registered trademark of Honeywell Inc., Minneapolis, MN. Intellution and FIX DMACS are registered trademarks of Intellution, Inc. INTEL and Pentium are registered trademarks of INTEL Corp. Microsoft Windows and Excel are registered trademarks of Microsoft Corp.

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: WHC/BCS Document Control Services, P.O. Box 1970, Mailstop H6-08, Richland WA 99352. Phone (509) 372-2420; Fax (509) 376-4989.


Release Approval

11/20/97
Date



Approved for Public Release

TABLE OF CONTENTS

1.0	INTRODUCTION	3
1.1	PURPOSE	3
1.2	SCOPE	3
1.3	DEFINITIONS	4
1.4	SECURITY	6
1.5	HARDWARE/SOFTWARE DESCRIPTION	6
2.0	MANAGEMENT	7
2.1	ORGANIZATION	7
2.1.1	System Administrator	8
2.1.2	Engineer	8
2.1.3	Operator	8
2.2	RESPONSIBILITIES	8
2.2.1	Cognizant Manager	8
2.2.2	System Cognizant Engineer	8
2.2.3	System Administrator	9
2.2.4	Configuration Management	9
2.3	INTERFACE CONTROLS	9
2.4	IMPLEMENTATION	9
2.5	POLICIES, DIRECTIVES, AND PROCEDURES	10
3.0	ACTIVITIES	10
3.1	CONFIGURATION IDENTIFICATION	10
3.1.1	Software Documentation	10
3.1.2	System Software Identification	10
3.1.2.1	Honeywell Control Software	10
3.1.2.2	Software Configuration Files	10
3.1.2.3	Graphical Files	11
3.1.3	Problems, Faults and Failures	12
3.2	CONFIGURATION CONTROLS	12
3.2.1	Software Changes	12
3.2.2	Access Levels	12
3.2.3	Backup and Recovery Operations	13
3.2.4	Historical Data File	14
3.3	CONFIGURATION STATUS ACCOUNTING	14
4.0	TOOLS, TECHNIQUES, AND METHODOLOGIES	14
5.0	SUPPLIER CONTROL	14
6.0	RECORD COLLECTION AND RETENTION	14
7.0	REFERENCES	15

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to establish a Computer Software Configuration Management Plan (CSCMP) for controlling the Plutonium Finishing Plant (PFP) Honeywell Modular Automation System (MAS) with Intellution® FIX DMACS™ operator interface. Figure 1 shows a system that will be used to control thermal stabilization furnaces in glovebox HA-21I and provide temperature and some interlock control for the vertical denitration calciner (VDC) in HC-230-C2. Figure 2 is a system that will be dedicated to control the pyrolysis furnace and off-gas treatment equipment to be installed in HC-15.

This CSCMP identifies and defines the configuration items for each system, controls the release and change of these items throughout the system life cycle, records and reports the status of configuration items and change requests, and verifies the completeness and correctness of each item.

1.2 SCOPE

The Honeywell MAS and Intellution® software installed at PFP will monitor and control thermal stabilization furnaces in glovebox HA-21I and pyrolysis furnaces in HC-15. The system will monitor and provide temperature control for the VDC in HC-230-C2.

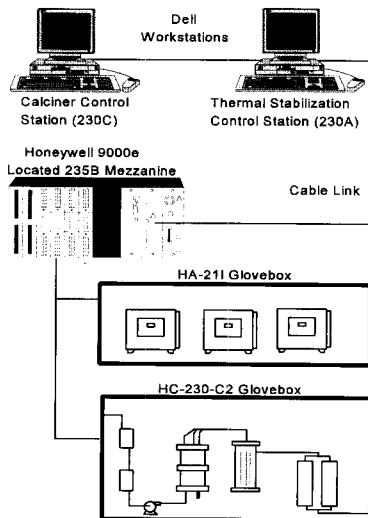


Figure 1

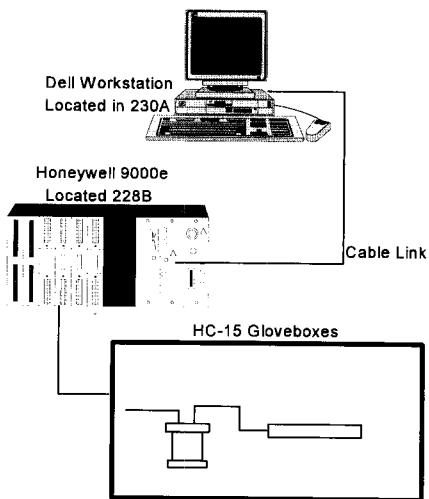


Figure 2

1.2 SCOPE (cont.)

This plan applies to PFP Process Engineering Cognizant Manager and Stabilization Cognizant Engineers responsible for the Honeywell MAS software/hardware and administration of the Honeywell System. This document also applies to support engineers and operations personnel who have access to the system.

1.3 DEFINITIONS

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 because of requirements set forth in the manufacturer's published product description (such as catalogs). Commercial software includes operating systems, language processors, spread sheets, etc.

Computer Software Validation

The process of evaluating computer software at the end of the computer software development process to ensure compliance with computer software requirements. Validation of the Honeywell MAS will be done with Acceptance Test Procedures (ATP). WHC-SD-CP-ATP-071 was used to validate the software and Input/Output (I/O) for thermal stabilization portion of software and hardware. Additional tests will be done to check VDC and pyrolysis furnace software and I/O. Once equipment installation is complete, Operability Test Procedures (OTP) will be done to confirm the link between software and field equipment. WHC-SD-CP-OTP-156 was done for thermal stabilization furnaces. Additional tests will be written and performed for the VDC and pyrolysis furnaces.

Configuration Management

A discipline applying technical and administrative direction and surveillance to: identify and document function and physical characteristics of a configuration item, control and implementation status, and verify compliance with specified requirements.

1.3 DEFINITIONS (cont.)

PC Supervisor (PCS)

A single-user operator interface and configuration station for the S9000 Controller. Both functions can be active concurrently, so one window can display an operating graphic while another displays a control chart.

S9000 Controller

Honeywell controller for continuous and batch applications that integrates sequential, continuous, and fast logic control. The S9000 can have up to 32 PID loops and 1000 inputs/outputs (the recommended limit for flow or pressure control is 16 loops).

Software

Computer programs, procedures, and possible associated documentation and data concerning operation of a computer system. This includes user-provided instruction 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.

Software Custodian

Designated individual or organization that maintains control of computer software, computer software media, and their access. PFP Process Engineering is responsible for maintaining the Honeywell MAS software.

System Administrator

Designated individual or organization responsible for the configuration and security scheme for the Honeywell MAS.

System Cognizant Engineer

Responsible engineer that assumes Cognizant Engineer responsibility for the system as defined by Standard WHC-CM-6-1, *Standard Engineering Practices*.

1.3 DEFINITIONS (cont.)

System Configuration

Completed data base which allow the control system to set up a specific control and display strategy for each process.

User

The person or persons, who operate or interact directly with the system.

1.4 SECURITY

Security for the Honeywell system is provided by limiting access to system through use of passwords. The system administrator controls access through a log in procedure that consists of a log in name and a password consisting of up to 20 characters. The access control program is part of the Honeywell PC Supervisor software. This program allows the system administrator to define level of access and breadth of allowed operations for each user.

1.5 HARDWARE/SOFTWARE DESCRIPTION

The Honeywell MAS consists of one or more PC work station, a "cable link," and the process control rack.

The work stations are DELL personal computers with INTEL® Pentium® processor and operates in a Microsoft® Windows™ environment. Available software includes the Honeywell PC supervisor, Intellution® FIX DMACSTM, and Microsoft® Windows™ and Excel™.

The PC work stations are connected to each other and the PLC with a "Cable link," a coaxial cable with 50-ohm terminating resistors.

The process control rack for the thermal stabilization furnaces and the VDC contain the following modules: a Model 9000e logic control processor (9010-012), a 15 amp power supply (620-0083), an Ethernet Loop Processor Module (620-0073), two universal analog input modules (621-0020R), two analog output modules (621-0010AR), a discrete input module (621-1160R), and a discrete output module (621-2150R). Two open slots will remain in the control rack for future expansion.

1.5 HARDWARE/SOFTWARE DESCRIPTION (cont.)

The process rack for pyrolysis will contain the following modules: a Model 9000e logic control processor (9010-012), a 15 amp power supply (620-0083), an Ethernet Loop Processor Module (620-0073), universal analog input module (621-0020R), an analog output module (621-0010AR), a digital input module (621-1100R), and a digital output module (621-2100R). Three open slots will remain in the control rack to allow for future expansion.

The universal analog input modules (621-0020R) can each accept 16 inputs. Individual inputs can be setup for the type of analog signal required. Software set up by the system administrator has configured these inputs to 1 to 5 volts (differential pressure transmitters) or Type K thermocouples where appropriate for thermal stabilization furnaces and vertical denitrator calciner.

Each analog output module (621-0010AR) is capable of 4 output signals. These analog output modules have been factory calibrated and will be used to send 4-20mA control signals to Silicon-Controlled Rectifiers (SCR).

The 621-1160R discrete input modules can accept 16 inputs. The 621-1100R discrete input modules accept 8 input signals. These inputs will be used for furnace door limit switches, exhaust fan power indication, dP switch, pressure switch, flow switch, and level elements. Each 621-2150R discrete output module has 16 outputs and each 621-2100R has 8 outputs. Some outputs will allow relays to energize and permit power to furnaces and calciner heating elements. These relays are an integral part to the interlock schemes for powering the furnaces and calciner. The remaining outputs will be used to start/stop vacuum fans, start/stop pumps, and open/close solenoid valves.

2.0 MANAGEMENT

2.1 ORGANIZATION

Three groups of system users are available and these groups are provided an appropriate level of access to data files and other programmable files within the Honeywell MAS. Access levels permit certain operations and exclude others. The breadth of these operations may also be limited depending upon the user group. Individual users can also be given additional abilities dependent on their job function.

2.1.1 System Administrator

The system administrator has access to all functions of the Honeywell MAS. Through the security function, the administrator assigns capabilities to the other user groups.

2.1.2 Engineer

The engineering level is immediately below that of the system Administrator. The engineer can make changes to the software configuration and operator displays, but cannot access the security file and password information. An ECN will be required against appropriate documentation to implement any configuration changes.

2.1.3 Operator

The operator group consists of the transition operators and shift managers. The access level for this group provides the functions necessary for operation of the equipment.

2.2 RESPONSIBILITIES

2.2.1 Cognizant Manager

The cognizant manager is responsible for ensuring configuration management controls identified by this document are used; for determining need and extent of software development; for ensuring appropriate approval and review are obtained in accordance with the approval designator; and for ensuring that computer software documentation by or transferred to PFP is assigned an approval designator. The cognizant manager will designate the system administrator.

2.2.2 System Cognizant Engineer

The cognizant engineer or delegate for the affected process is responsible for approving ECN(s) to revise software and for identifying functional requirements within each ECN.

2.2.3 System Administrator

The system administrator is responsible for identifying the functional requirements of the computer software; for establishing approval designation of computer software documentation; for ensuring configuration management requirements are followed; for overseeing and ensuring configuration and security of system; for approving, implementing and tracking ECNs to system documentation; and for revising existing software.

2.2.4 Configuration Management

Configuration Management is responsible for assigning a supporting document number to Computer Software Documents and for releasing 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 that controls and defines system interfaces. Overall, interfaces between the MAS and process equipment are at discrete/analog input/output terminals. All changes to P&ID drawings, that show the MAS as the control system, shall be approved by the Cognizant Engineer responsible for affected system. The cognizant engineer will notify the system administrator to make appropriate modifications to software and configuration documentation.

2.4 IMPLEMENTATION

This document in concert with process specific ATPs and OTPs will be used to bring the Honeywell MAS on line at the PFP. The Honeywell MAS will be considered operational when all users have been trained, necessary group text files have been defined, validated, recorded, and required passwords and access levels have been assigned. The cognizant engineer for each process being brought on-line is responsible for complete implementation of this system to the process equipment.

2.5 POLICIES, DIRECTIVES, AND PROCEDURES

Software will be designed and developed in compliance with WHC-CM-4-2, *Quality Assurance Manual*, QR 19.0, "Software Quality Assurance Requirements." Computer software will be design verified according to WHC-CM-6-1, Standard Engineering Practices, EP 4.1, "Design Verification Requirements," and validated following EP 4.2, "Testing Practices." Computer software Documents will be approved and released in accordance with EP 1.6, "Engineering Data Transmittal," EP 1.7, "Engineering Document Approval and Release Requirements," and revised following EP 2.2, "Engineering Document Change Controls." All training will be conducted under the general auspices of WHC-CM-2-15, "Training Administration Manual."

3.0 ACTIVITIES

3.1 CONFIGURATION IDENTIFICATION

3.1.1 Software Documentation

All software associated with the Honeywell MAS will be documented in supporting document WHC-SD-CP-CSWD-018, Honeywell Modular Automated System Computer Software Documentation.

3.1.2 System Software Identification

This supporting document identifies items for controlling revisions and installation.

3.1.2.1 Honeywell Control Software

The control software consists of the Honeywell PC supervisor and Intellution® FIX DMACS™ Release 150 (9000-152 PCS/MASNET S/W). Honeywell part number for this 9 disk software package is 64190A through 64198A. Backup to these files will be kept by the system administrator on 3½" disks.

3.1.2.2 Software Configuration Files

The continuous control chart (CCC) is the configuration software file for the S9000 Controller that creates loop control graphically through the PC Supervisor. Addresses and point names are used to define source and destination of data within the CCC

3.1.2.2 Software Configuration Files (cont.)

configuration. These addresses identify physical connection points for field wiring to I/O modules plus internal I/O and registers for the relay ladder logic.

The sequential control chart (SCC) is a graphic oriented programming language for sequencing operations in conjunction with the CCC configuration.

The PCS Relay Ladder Logic allows the programmer to define discrete control functions in the control strategy with logic elements such as coils and relays.

Set point programs are developed with the PC Supervisor to provide input to Set Point Programmer control blocks in the CCC. Each program can contain up to 49 pairs of ramp and soak segments. Each segment can turn on 1 to 12 events through a Set Point Program Event control block in the CCC.

A printed copy of these configuration files will be placed in the computer software description document, WHC-SD-CP-CSWD-018. The configuration file printout will have the documentation date in the header and will be referenced in the computer software description document.

3.1.2.3 Graphical Files

These files provide graphical representation of the system being controlled or monitored. Graphical files are generated to provide an interface to the CCC configuration. Graphical displays allow real time data monitoring by user. Configuration control will be through reproduction of actual graphics from the DRAW program. An ASCII file report will be generated for each graphic in the DRAW program and will be printed. Each graphic and graphic report will become part of the computer software description document.

3.1.2.4 Tag Group Files

The tag group files are a set of tagnames that can be used in a common graphical display to replace generic tagnames with specific data points. Tag group reports are generated by the Tag Group Editor to an ASCII file that will be printed and will become part of the Computer Software Description Document.

3.1.3 Problems, Faults and Failures

Hardware problems, faults and failures will be reported, controlled, processed, corrected, retested, and closed out using the Job Control System (JCS). Should modifications be required to resolve or correct the problem, the engineering process will be documented according to WHC-IP-0848, PFP Engineering Directives, Section 1.16, "Engineering Design File." The resulting ECN will be developed, processed, approved, and released according to EP 2.2.

Any problems, faults, or failures resultant of the software will have changes done per section 3.2.1 or recovery actions per section 3.2.3.

3.2 CONFIGURATION CONTROLS

3.2.1 Software Changes

When a change to the software is required, that change will be reviewed by the system administrator and/or cognizant engineer for system being affected. All changes to software files will first be done at the system administrator's development station. An ECN against the computer software configuration document will be written for change. The system cognizant engineer or delegate and cognizant manager must sign all ECNs. In addition, the appropriate authorities must sign and approve ECNs based on assigned approval designator. Once ECN is approved for release, the modified software file will be downloaded to the Honeywell MAS replacing the existing file. The Honeywell MAS will be tested to check system configuration as determined by the cognizant engineer. The backup file will be saved on a disk and labeled with "PFP Developed Honeywell MAS Control Software," Date of release, and ECN number that changed the software configuration document. The system administrator will maintain the two most recent revisions on disk.

3.2.2 Access Levels

The Honeywell MAS security system is configured by the system administrator. The administrator provides users with a password and provides software abilities based on the user's need.

The system Administrator assigns each user to a user group. Each user group is assigned capabilities required to do their work. Additional capabilities may be provided as needed to the user.

3.2.3 Backup and Recovery Operations

Media control is exercised by the system administrator to ensure that the Honeywell software and PFP developed software is backed up after each modification. This back up will allow reconstruction of the system software in a few days. Two back up copies of the Honeywell and PFP developed software will be maintained. One copy of the software will be maintained on floppy disk by PFP Process Engineering. An additional working copy will be maintained on the system administrator's computer.

Backup of the PFP developed configuration software can be performed by clicking on "Control Cfg" icon. After logging into the CONFIGURATION ACCESS level, enter the Configuration Library under File menu. Select Configuration Model and press "Backup..." button. Place floppy into selected drive and press "OK" button. The backup file will be saved on a disk and labeled with "PFP Developed Honeywell MAS Control Software - Configuration," configuration name, date of release, and ECN or EDT number that released the software configuration document.

Recovery of the PFP developed software will be done by the system administrator. Recovery is accomplished by accessing Configuration Library as describe above and press "Restore..." button. Place floppy with backup files into selected drive, select Configuration to restore and press "OK" button. The nonfunctional configuration file may need to be deleted before restoration. This is done by highlighting the file name and pressing Delete button and then the "OK" button in CONFIRM block. After the configuration is restored, downloading configuration is accomplished by highlighting configuration and pressing "Download..." button.

Graphical and tag group files will be backed up using file manager. Files location is C:\wdmacs\pic. Graphics designed with the Draw program have (*.odf) tags. Tag groups are saved as (*.tge) files. These files will be saved on a disk and labeled with "PFP Developed Honeywell MAS Control Software - Graphics," disk number (if there are multiple disks), date of release, and ECN or EDT number that released the software configuration document.

Recovery of the Honeywell software will be done by the system administrator per the Honeywell operating manual.

Once any recovery action is complete, the Honeywell MAS will be tested to check system configuration as determined by the cognizant engineer.

3.2.4 Historical Data File

Historical data files will be collected for designated data points. The data points are specified within Historical Assign and collection is started with Historical Collect. A separate data file is initiated every 24 Hours. The files are retained by the system for 30 days and then are deleted. The data will periodically be exported from Historical Display and loaded into a Microsoft® Excel spreadsheet. The data will be manipulated into graphs and/or tables. These graphs and tables will be maintained by Process Engineering and will be documented in campaign reports.

3.3 CONFIGURATION STATUS ACCOUNTING

The System Administrator will review the software for correctness biannually. The current operating software will be compared with the current revision of WHC-SD-CP-CSWD-018, Honeywell Modular Automated System Computer Software Documentation. This review will provide a listing of the following information:

1. Cognizant engineer for controlled system
2. Software custodian
3. Current revision of configuration
4. Location of master and backup configuration and Honeywell files
5. EDT and ECN numbers for documentation.

4.0 TOOLS, TECHNIQUES, AND METHODOLOGIES

No additional tool, techniques, or methodologies are used in maintaining configuration control other than those supplied as part of the commercially available Honeywell and FIX DMACSTM software.

5.0 SUPPLIER CONTROL

The cognizant engineer will ensure that the Honeywell MAS software meets the specifications in the purchasing contract.

The cognizant engineer will ensure the Honeywell MAS is being supported during all phases of installation, setup, programming and debugging.

6.0 RECORD COLLECTION AND RETENTION

See section 3.2.4.

7.0 REFERENCES

MAS-8988C. *Modular Automation System, PC Supervisor Graphics*

MAS-8992C. *Modular Automation System, S9000 Controller*

MAS-8993C. *Modular Automation System, PC Supervisor*

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"
EP 1.7. "Engineering Document Approval and Release"
EP 2.2. "Engineering Document Change Control"
EP 4.1. "Design Verification Requirements"
EP 4.2. "Testing Practices"

WHC-SD-CP-CSWD-018. *Plutonium Finishing Plant Honeywell Modular Automation System Computer Software Document*

WHC-SD-CP-ATP-071. *Plutonium Finishing Plant Honeywell Modular Automation System Computer Software Acceptance Test.*