MAR 06 2000

ENGINEERING DATA TRANSMITTAL

Page 1 of 1

1. EDT

622388

2. To: (Receiving Organization) Distribution		3. From: (Originating Organization) Fuel Handling I&C Engineering		4. Related EDT No.: N/A	
5. Proj./Prog./Dept./Div.: FFTF/SRS		6. Design Authority/Design Agent/Cog. Engr.: L. F. Hill		7. Purchase Order No.: N/A	
8. Originator Remarks: Original release for project use.				9. Equip./Component No.: C-1167	
				10. System/Bldg./Facility: 405	
				12. Major Assm. Dwg. No.: H-4-302596	
				13. Permit/Permit Application No.: N/A	
11. Receiver Remarks:				14. Required Response Date:	
11A. Design Baseline Document? ☐ Yes ☒ No					

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	FFTF-5631	All	0	Computer Software	Q	2	1/2	1
				Configuration Management			1/2	
				Plan for the Sodium				
				Removal System at the				
				Fast Flux Test Facility				
				Interim Examination and				
				Maintenance Cell				

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

17. SIGNATURE/DISTRIBUTION (See Approval Designator for required signatures)														
(G) Reason	(H) Disp.	(J) Name	(K) Signature	(L) Date	(M) MSIN	(G) Reason	(H) Disp.	(J) Name	(K) Signature	(L) Date	(M) MSIN			
1	I	System Cog. Eng. Design Authority PW	McGuinness	2/9/00	N2-02	1	I	SJ Gray	Sandra J. Gray	3/2/00	N2-13			
		Design Agent				I	I	DAGantt, ATO	DC/250	1/27/00	N2-13			
1	I	Cog. Eng. LF Hill	LF Hill	1/27/00	N2-54									
1	I	Cog. Mgr. GN Ruge	GN Ruge	2/7/00	N2-54									
1	I	QA JE Duda	JE Duda	2/7/00	N2-11									
		Safety												
		Env.												

18. LF Hill Signature of EDT Originator Date 1/27/00		19. George N. Ruge GN Ruge Authorized Representative for Receiving Organization Date 3-2-00		20. George N. Ruge GN Ruge Design Authority/Cognizant Manager Date 3-2-00		21. DOE APPROVAL (if required) Ctrl No. _____ ☐ Approved ☐ Approved w/comments ☐ Disapproved w/comments	
--	--	--	--	--	--	--	--

INFORMATION CLEARANCE FORM																																	
A. Information Category ☐ Abstract ☐ Journal Article ☐ Summary ☐ Internet ☐ Visual Aid ☐ Software ☐ Full Paper ☐ Report ☒ Other <u>Supporting Document</u>		B. Document Number FFTF-5631, Revision 0 C. Title Software Configuration Management Plan for the Sodium Removal System																															
E. Required Information 1. Is document potentially Classified? ☒ No ☐ Yes (MANDATORY) <u>George N. Ruge</u> Manager's Signature Required If Yes _____ ☐ No ☐ Yes Classified ADC Signature Required 2. Internal Review Required? ☐ No ☐ Yes If Yes, Document Signatures Below Counsel _____ Program _____ 3. References in the Information are Applied Technology ☒ No ☐ Yes Export Controlled Information ☒ No ☐ Yes		4. Does Information Contain the Following: (MANDATORY) a. New or Novel (Patentable) Subject Matter? ☒ No ☐ Yes If "Yes", Disclosure No.: _____ b. Information Received in Confidence, Such as Proprietary and/or Inventions? ☒ No ☐ Yes If "Yes", Affix Appropriate Legends/Notices. c. Copyrights? ☒ No ☐ Yes If "Yes", Attach Permission. d. Trademarks? ☐ No ☒ Yes If "Yes", Identify in Document. 5. Is Information requiring submission to OSTI? ☒ No ☐ Yes If Yes UC-_____ and B&R-_____ 6. Release Level? ☒ Public ☐ Limited 7. Charge Code <u>101587</u>																															
F. Complete for a Journal Article 1. Title of Journal <u>N/A</u>																																	
G. Complete for a Presentation 1. Title for Conference or Meeting <u>N/A</u> 2. Group Sponsoring _____ 3. Date of Conference _____ 4. City/State _____ 5. Will Information be Published in Proceedings? ☐ No ☐ Yes 6. Will Material be Handed Out? ☐ No ☐ Yes																																	
H. Author/Requestor <u>L. F. Hill</u> (Print and Sign) <u>L F Hill</u>		Responsible Manager <u>G. N. Ruge</u> (Print and Sign) <u>George N. Ruge</u>																															
<table border="0" style="width: 100%;"> <tr> <th style="text-align: left;">I. Reviewers</th> <th style="text-align: center;">Yes</th> <th style="text-align: center;">Print</th> <th style="text-align: center;">Signature</th> <th style="text-align: center;">Public Y/N (If N, complete J)</th> </tr> <tr> <td>General Counsel</td> <td style="text-align: center;">☐</td> <td>_____</td> <td>_____</td> <td style="text-align: center;">Y / N</td> </tr> <tr> <td>Office of External Affairs</td> <td style="text-align: center;">☐</td> <td>_____</td> <td>_____</td> <td style="text-align: center;">Y / N</td> </tr> <tr> <td>DOE-RL</td> <td style="text-align: center;">☐</td> <td>_____</td> <td>_____</td> <td style="text-align: center;">Y / N</td> </tr> <tr> <td>Other</td> <td style="text-align: center;">☒</td> <td><u>D. A. Gantt</u></td> <td><u>D. A. Gantt, Applied Technology Officer</u></td> <td style="text-align: center;">☒ / N</td> </tr> <tr> <td>Other</td> <td style="text-align: center;">☐</td> <td>_____</td> <td>_____</td> <td style="text-align: center;">Y / N</td> </tr> </table>				I. Reviewers	Yes	Print	Signature	Public Y/N (If N, complete J)	General Counsel	☐	_____	_____	Y / N	Office of External Affairs	☐	_____	_____	Y / N	DOE-RL	☐	_____	_____	Y / N	Other	☒	<u>D. A. Gantt</u>	<u>D. A. Gantt, Applied Technology Officer</u>	☒ / N	Other	☐	_____	_____	Y / N
I. Reviewers	Yes	Print	Signature	Public Y/N (If N, complete J)																													
General Counsel	☐	_____	_____	Y / N																													
Office of External Affairs	☐	_____	_____	Y / N																													
DOE-RL	☐	_____	_____	Y / N																													
Other	☒	<u>D. A. Gantt</u>	<u>D. A. Gantt, Applied Technology Officer</u>	☒ / N																													
Other	☐	_____	_____	Y / N																													
J. If Information Includes Sensitive Information and is not to be released to the Public indicate category below.																																	
<table border="0" style="width: 100%;"> <tr> <td>☐ Applied Technology</td> <td>☐ Protected CRADA</td> </tr> <tr> <td>☐ Personal/Private</td> <td>☐ Export Controlled</td> </tr> <tr> <td>☐ Proprietary</td> <td>☐ Procurement-Sensitive</td> </tr> <tr> <td>☒ Business-Sensitive</td> <td>☐ Patentable</td> </tr> <tr> <td>☐ Predecisional</td> <td>☐ Other (Specify) _____</td> </tr> <tr> <td>☐ UCNI</td> <td></td> </tr> </table>				☐ Applied Technology	☐ Protected CRADA	☐ Personal/Private	☐ Export Controlled	☐ Proprietary	☐ Procurement-Sensitive	☒ Business-Sensitive	☐ Patentable	☐ Predecisional	☐ Other (Specify) _____	☐ UCNI																			
☐ Applied Technology	☐ Protected CRADA																																
☐ Personal/Private	☐ Export Controlled																																
☐ Proprietary	☐ Procurement-Sensitive																																
☒ Business-Sensitive	☐ Patentable																																
☐ Predecisional	☐ Other (Specify) _____																																
☐ UCNI																																	
K. If Additional Comments, Please Attach Separate Sheet																																	

Software Configuration Management Plan for the Sodium Removal System

Prepared for the U.S. Department of Energy
Assistant Secretary for Environmental Management

Project Hanford Management Contractor for the
U.S. Department of Energy under Contract DE-AC06-96RL13200

Fluor Hanford

P.O. Box 1000

Richland, Washington

Software Configuration Management Plan for the Sodium Removal System

LF Hill
Fluor Hanford

(Total Pages: 26)

Date Published
March 2, 2000

Prepared for the U.S. Department of Energy
Assistant Secretary for Environmental Management

Fluor Hanford
P.O. Box 1000
Richland, Washington

**SOFTWARE CONFIGURATION MANAGEMENT PLAN
FOR THE SODIUM REMOVAL SYSTEM**

L. F. Hill
February 2000
FFTF Engineering
Fluor Hanford, Inc.

Key Words: FFTF, IEM Cell, SRS, SCMP, Software

Abstract: This document establishes the Software Configuration Management Plan (SCMP) for the software associated with the control system of the Sodium Removal System (SRS) located in the Interim Examination and Maintenance (IEM Cell) Facility of the FFTF Flux Test Facility (FFTF). The control system monitors and displays the instrumentation associated with the process and allows the operator to control the process control devices.

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.

Printed in the United States of America

TABLE OF CONTENTS

1.0 INTRODUCTION	1
1.1 PURPOSE	1
1.2 SCOPE	1
1.3 DEFINITIONS	2
1.4 SECURITY	3
1.5 HARDWARE / SOFTWARE DESCRIPTION	3
2.0 MANAGEMENT	4
2.1 ORGANIZATION	4
2.2 RESPONSIBILITIES	4
2.2.1 Cognizant Manager	4
2.2.2 (Control System) Cognizant Engineer	5
2.2.3 System Administrator	5
2.3 INTERFACE CONTROLS	5
2.4 IMPLEMENTATION	5
2.5 POLICIES, DIRECTIVES, AND PROCEDURES	5
3.0 ACTIVITIES	6
3.1 CONFIGURATION IDENTIFICATION	6
3.1.1 P&ID (H-4-28240)	7
3.1.2 Wiring Diagrams (H-4-302597 through H-4-302606)	7
3.1.3 Logic Diagrams	7
3.1.4 Computer Software Design Description	7
3.1.5 Windows NT Software	8
3.1.6 Paradym Software	8
3.1.7 Paradym Logic Files	8
3.1.8 Paradym User Defined Functions Blocks (UDFB's)	9
3.1.9 FIX Database	9
3.1.10 Graphics Picture Files	9
3.1.11 Historian Configuration File	10
3.1.12 Security Configuration Files	10
3.1.13 Release Document	10
3.1.14 Backup and Configuration Control Directories	10
3.2 CONFIGURATION CONTROLS	11
3.2.1 Problem Tracking	11
3.2.2 Software Change Form (SCR)	11

3.2.3	Job Control System	12
3.2.4	Preparing the Change	12
3.2.5	Installing and Testing the Change	12
3.2.6	New Release Version	13
3.2.7	Release for Plant Use	13
3.3	CONFIGURATION STATUS ACCOUNTING	13
3.4	AUDITS AND REVIEWS	13
3.5	ACCESS CONTROL	13
3.5.1	System Administrator	14
3.5.2	Engineer	14
3.5.3	Operator	14
3.5.4	Supervisor	14
3.5.5	Guest	14
3.6	BACKUP AND RECOVERY	15
4.0	TOOLS, TECHNIQUES, AND METHODOLOGIES	15
5.0	SUPPLIER CONTROL	15
6.0	RECORD COLLECTION AND RETENTION	16
7.0	REFERENCES	16
FIGURE 1:	SRS CHANGE REQUEST/PROBLEM REPORT	17
FIGURE 2:	CHANGE REQUEST AND PROBLEM REPORT LOG	19

1.0 INTRODUCTION

1.1 PURPOSE

This document establishes the Computer Software Configuration Management Plan (SCMP) for the software associated with the control system of the Sodium Removal System (SRS) located in the Interim Examination and Maintenance (IEM Cell) Facility of the Fast Flux Test Facility (FFTF) in the 400 Area. The control system monitors and displays the instrumentation associated with the process and allows the operator to control the process control devices.

The SCMP:

- 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

The SRS Control software will monitor and control the SRS at the FFTF IEM Cell. The software provides minimal automatic control, being essentially a monitoring and display system, with provisions for the operator to "manually" make system changes via computer input. The control system is built upon a commercial software package called Paradym-31TM¹ (or P31, for short). Thus, most of the "software" which needs to be controlled is the configuration data associated with customizing this generic software to our specific application.

All software development before initial release, or before software is base-lined, is considered developmental. This plan does not apply to developmental software. This plan applies to software that has been base-lined, released, and accepted for plant use.

This plan applies to the System Cognizant Manager, SRS Cognizant Engineer and System Administrator who are responsible for the software/hardware and administration of the system. This document also applies to any other organizations which use the system, including system cognizant engineers, nuclear operators, technicians, and control room supervisors.

¹ Paradym-31 is a product of the Intellution Corporation.

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 system, this is the user created configuration files, which customize the FIX^{TM2} and Paradym system for our application.

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.

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. 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).

Data files. Data files are primarily developed using vendor-supplied utilities and subroutines. 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 processing of these variables.

FIX. Proprietary software supplied by the Intellution Company, which provides a Human-Machine Interface. FIX runs on the Windows NT^{TM3} platform.

Paradym. Also called Paradym-31 or P31. Proprietary software provided by the Intellution Company which provides a software Programmable controller (soft-PLC). Paradym runs on the Windows NT platform.

² FIX is a product of the Intellution Corporation.

³ Windows NT is a product of the Microsoft Corporation.

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.

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.

Windows NT. Proprietary software supplied by Microsoft, which provides the operating system for the computer. The Intellution software is designed to run under this operating system.

System Administrator. The Cognizant Engineer responsible for maintaining control of computer software, computer software media, and their access.

System Configuration. The completed data files that establish a specific control and display strategy to utilize the general commercial system for a specific application.

Tag or Tagname. A generic term for variables (analog and discrete) defined and used in the software to process input and output data as specified by the executable logic files.

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).

1.4 SECURITY

Limiting access to the system through the use of passwords provides the security for the Intellution system. The System Administrator controls access through a login procedure which consists of Login name and a password consisting of 6 to 16 characters. The access control programs are pre-existing and are found in the Windows operating system and FIX. These programs allow the System Administrator to define the level of access and the breadth of allowed operations.

1.5 HARDWARE / SOFTWARE DESCRIPTION

The SRS control system hardware consists of a computer workstation, a communication network, and I/O modules to interface to the field devices. The workstation is a standard personal computer (PC) with 128MB of memory, a hard drive and a pointing device to select items on the graphic screens. The video port is connected to a 21-inch high-resolution color monitor. An Opto-22 AC37 communications adapter is provided in the PC for communication to the I/O modules via

an RS485 serial link at 115K baud. The I/O modules are packaged in OPTO-22 "bricks", which are nodes on the network and communicate to the Host CPU via the OPTO-22 "Mystic" protocol. There are 20 digital nodes and 3 analog nodes, each of which can provide up to 16 channels of discrete or analog I/O. The digital bricks are OPTO model number G4D16R, which provide 16 digital I/O points. The analog nodes are OPTO G4A8R with G4RAX expansion racks to provide a total of 16 analog points at each node.

Software for the PC workstation consists of three layers. The first layer is the Windows NT operating system provided by Microsoft. The second layer is the Paradym/FIX program supplied by Intellution. Finally, the third layer is the program, configuration and data files which customize Paradym/FIX and implement functions specific to our application. Each OPTO-22 node includes embedded network communications software, but this software is not addressed since it does not have to be changed, downloaded or controlled.

Windows NT and Paradym/FIX are commercial off-the-shelf software and are not subject to this configuration management plan, except as necessary to support rebuilding or rebooting the workstation should the entire system crash. Only the user created configuration programs and files are subject to the revision control covered by this document.

2.0 MANAGEMENT

2.1 ORGANIZATION

The Cognizant Manager responsible for the SRS control system shall identify a Cognizant Engineer and a System Administrator (which may be the same person). In general, the Cognizant Engineer is responsible for the Design Bases, which the system is required 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; and for designating the Cognizant Engineer, System Administrator, and alternates (if needed).

2.2.2 (Control System) Cognizant Engineer

The Cognizant Engineer is responsible for identifying the functional requirements of the computer software; for maintaining the software documentation; for approving and implementing any necessary changes in accordance with configuration management requirements; and for overseeing and ensuring the configuration and security of the system.

2.2.3 System Administrator

The System Administrator is responsible for ensuring that the approved configuration is being used in the system; for maintaining and storing the backup media; and for adjustments to access control permissions.

2.3 INTERFACE CONTROLS

The facility system and process P&ID drawings define the facility interfaces to the control system. In general, the interface is at the digital/analog input/output terminals. All changes to P&ID drawings which affect the control system interface shall be approved by the Control System Cognizant Engineer.

2.4 IMPLEMENTATION

Currently the system 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. Changes during development will be controlled in a similar, but informal, process as necessary to ensure integrity of the product. The configuration process shall be formalized per this procedure when the system is released for plant use.

2.5 POLICIES, DIRECTIVES, AND PROCEDURES

Software shall be designed and developed in compliance with HNF-PRO-309, "Computer Software Quality Assurance Requirements," and HNF-PRO-2778, "IRM Application Software System Life Cycle Standards."

Testing of the system shall use the requirements of HNF-PRO-286, "Test Control" as applicable, using the graded approach relative to the significance of the change.

Documentation associated with the computer software shall be approved and released in accordance with the following documents, as applicable:

- HNF-PRO-244, "Engineering Data Transmittal Requirements."
- HNF-PRO-440, "Engineering Document Change Control Requirements."
- HNF-PRO-709, "Preparation and Control Standards for Engineering Drawings."

Changes and physical control of the software shall be in accordance with FFTF-EI-074, "Preparation, Release and Revision of Critical System Software" and A-23, "FFTF Computer Systems Software Physical Control".

3.0 ACTIVITIES

3.1 CONFIGURATION IDENTIFICATION

The primary documents which define and control the software configuration are the P&IDs, Wiring Diagrams, Logic Diagrams, and Computer Software Design Description (CSDD). These are the design basis documents, which define the functional operation of the software.

To implement the required software functions they are entered into the Intellution software, where the resulting information is internally stored in numerous data files. Most of the data files are unreadable or otherwise poorly suited for generating human-readable hard copies. Consequently, the data 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 recoverability 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&ID
- 2) Wiring Diagrams
- 3) Logic Diagrams
- 4) Software Design Description

Commercial software which provides the application base:

- 5) Windows NT
- 6) Paradym/FIX

On-line configuration data files:

- 7) P31 soft-PLC Logic Files

- 8) P31 User-Defined Function Blocks (UDFB's)
- 9) FIX Database File
- 10) Graphics picture files
- 11) Historian Configuration file

These are discussed in the following sections.

3.1.1 P&ID (H-4-28240)

The SRS P&ID defines basic system functions, tag names, and locations of interlocks and alarms. The P&ID is an H-4 drawing, and is identified and controlled in accordance with applicable drawing requirements.

3.1.2 Wiring Diagrams (H-4-302597 through H-4-302606)

The Wiring Drawings define the I/O Configuration to the P31 program. They are H-4 drawings, and are identified and controlled in accordance with applicable drawing requirements. (Note: Custom graphics screens have also been developed from the released H-4's wiring diagrams to show the dynamic state of the wiring; these graphics are distinct from the "source" H-4 Diagrams, and are really only standard picture files as described in section 3.1.10.)

3.1.3 Logic Diagrams

The Logic Diagrams define the logic performed in the P31 soft-PLC. It is actually desired to control the engineering basis for the logic, rather than the actual computer implementation. However, since Paradym can very conveniently printout a picture of the actual implemented logic, these printouts will be used as the controlled media rather than developing an additional set of drawings. Tag names are shown (and hence will be controlled) by these drawings, however, the detailed definition (e.g., Real, Integer, or Long) will be left as an implementation detail.

The Logic Diagrams will be released as a supporting document and identified and controlled accordingly. Note that each logic function, which is generally a one-page ladder chart, is the smallest modifiable block within the document.

3.1.4 Computer Software Design Description

The CSDD documents and controls a number of engineering bases for the software. In addition to describing the basic software structure, it defines things like color schemes, alarms, and timing constraints, which should be maintained for any changes. The CSDD is a supporting document, and is identified and controlled in accordance with standard requirements for supporting documents.

3.1.5 Windows NT Software

The standard Windows NT operating system is used, with necessary "service packs" provided by Microsoft. The version is identified by the basic Windows version and applicable service pack number(s). Only recovery capability is needed. If reloading is necessary, this will be accomplished from the master Windows CD, which will be retained with the Cognizant Manager or his designee. A copy of any "service packs" used shall also be maintained.

Only one copy of these is needed, because they are also readily available from Microsoft. Should it become, for any reason, inappropriate to rely upon Microsoft for backup copies, then a second set of the master disks should be maintained in a separate location.

3.1.6 Paradym Software

Paradym is also a commercial software package, similarly identified by the basic version number and applicable SIM's (System Improvement Modules). Again, only recovery capability is needed. Paradym is provided on a master CD, which will be retained by the Cognizant Manager or his designee, and a second backup copy shall be retained by the System Administrator. Any vendor upgrades (or bug fixes) shall also be stored in both locations.

The current version of the software requires a hardware key for the software to run, and only one key is available (unless an additional copy purchased). This key will be left installed on the SRS computer.

3.1.7 Paradym Logic Files

Since the engineering basis for the logic is controlled as described in section 3.1.3, the remaining issue is to identify a specific configuration for confirmation of proper version. The logic is entered pictorially and the resulting data files are located in the */Paradym/SRS* working directory, along with five backups. A series of backups are generated (round-robin style) each time Paradym is started, and includes only the "source" files necessary to re-generate the system. Thus a copy of the appropriate backup directory provides a snapshot of a specific version of the configuration, which is readily identifiable by the timestamp common to all the files. For convenience, the entire *srs* directory may be saved when a version is saved, with the understanding that the current version is the most recently dated backup. Since the timestamps may differ by a small amount (<1 min), the official Release identification will be the timestamp and size of the file *rts/MAIN.thr*.

Inspection to verify what version is actually being run in the working directory is a little more complicated. The difficulty is that the working versions of the above "source" files

can have their dates changed without any change in the program, for example by simply clicking on "save" while in the Paradym program viewer. However, any changes (if made) would not affect the actual running program unless the system were re-built, which re-generates the executable *rts/MAIN.dll* file and some other data files. The timestamp on this dll file thus provides primary verification of what program is running. However, we also need to accommodate re-building the system, which will result in a different timestamp (even if the program was not changed). It should be noted that these are engineering functions, not accessible to the operator.

Generally, the files in the working directory will retain their timestamps and will match the version captured for the Release control. Thus the Release timestamp would also be found on the *rts/MAIN.thr* file in the working directory, and (approximately the same timestamp) on the *rts/MAIN.dll* file. In the event it becomes necessary to rebuild the system from the same Release version, this will be identified as a Release version plus Build-Date to denote that the system was recompiled. The System Administrator shall ensure that Build-versions are controlled and correlated to the Release versions.

3.1.8 Paradym User Defined Functions Blocks (UDFB's)

The Paradym application also includes several UDFB's, which are C-language programs packaged so they can be used the same as normal Paradym function blocks. The quantity of code is small enough that the UDFB's will be controlled as hard-copy listings attached to the CSDD discussed above. The C-code files and header files are located in the *Paradym/User* directory.

3.1.9 FIX Database

The FIX Database defines variables and calculations associated with the graphics displays, and specifically implements the alarming functions. The database is generated by the FIX Database editor, is in a proprietary format, and is not readily readable. The file is *FIX32/Pdb/database.pdb* and version control will utilize the timestamp and size of this file.

3.1.10 Graphics Picture Files

Picture files define the graphic displays, including dynamics information, which have been developed specifically for this application. Features such as the alarm summary and trend plots are actually defined by the display file that includes them. The active picture files are located in the *Dynamics/pic* directory with *.grf* extensions; the base filenames must be fixed for the system to work properly. Picture files are generated by the FIX Picture editor, are in a proprietary format, and are not readily readable. Picture files will be controlled by name, timestamp, and size.

3.1.11 Historian Configuration File

The information and recording rates for historical information is stored in a series of files in directory *Dynamics/htr*. The timestamps and sizes of these files will be used for version control.

3.1.12 Security Configuration Files

Security information is stored in encrypted files in several places. A password change will not be considered a configuration change and will not result in a new Release version. The System Administrator is responsible for ensuring security is configured as described in section 3.5, Access Control.

3.1.13 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 through 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]
 example 1: 1.0 ; Initial release
 example 2: 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 may be 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.

3.1.14 Backup and Configuration Control Directories

For each Release Version, the application files shall be copied to a subdirectory in the *Release* directory. This provides an auditable copy of the release files, and a location from which they can be restored. Note that a full backup of the release requires more than just the files which are being controlled by timestamps. To provide restoration, the backup should include all files in the following directories:

Dynamics/htc
Dynamics/local
Dynamics/pdb
Dynamics/pic
Paradym/srs
Paradym/user

The files for each Release shall also be stored in two other controlled locations, not on the active workstation, in accordance with section 3.6.

3.2 CONFIGURATION CONTROLS

Two categories of software revisions are defined as:

- **Major Changes** affect the configuration basis documents - P&ID, Wiring, Logic Diagrams, and/or CSDD as defined in sections 3.1.1 through 3.1.4. Such changes require an Engineering Change Notice (ECN) to change the baseline documents.
- **Minor Changes** do not affect the baseline documents, but only the implementation of these requirements into the data files. Such changes will probably not affect process operation, but rather 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 must be controlled as specified in this document.

3.2.1 Problem Tracking

Problems, faults and failures may be documented and tracked at the discretion of FFTF Operations.

3.2.2 Software Change Form (SCR)

All revisions to the software identified in section 3.1 shall be initiated and tracked by preparing a Software Change Request (SCR) in accordance with Figure 1. While the SCRs officially become part of their respective work package, the System Administrator shall also maintain a log and master copy of all change requests generated since the last major release. (At a major release, the preceding detail may optionally be summarized.) Figure 2 gives a sample form for the Log information.

For **Major Changes**, an ECN describing the desired changes to the configuration basis documents (reference 3.1.1-3.1.3) may accompany the SCR, but in any case, must be prepared and approved prior to installing the software change. ECNs must be

approved by the Control System Cognizant Engineer and by the SRS System Cognizant Engineer.

For **Minor Changes**, the configuration basis documents are not affected, so the SCR fully describes the desired change. For small changes, the disposition of the SCR may provide the only record needed of what was actually changed and what retest was performed.

The Control System Cognizant Engineer shall approve the SCR prior to installation of the change in the plant – however, note that this is a technical approval, not approval to install in the plant (see following section). The Cognizant Engineer shall also ensure that the disposition and retest portions of the SCR are completed during implementation, so that the completed form provides an accurate record of the change.

3.2.3 Job Control System

Most **Major Changes** (which require an ECN) would be expected to require a custom work package to establish proper plant initial conditions, mobilize personnel, make plant physical modifications, or operate equipment for installation or testing. On the other hand, many of the **Minor Changes** are expected to be able to be implemented and tested without affecting any plant equipment (except the SRS computer). For such simple changes, the SCR provides the needed work instructions and record of the change.

Work performed in the plant shall be done in accordance with the plant work control system (A-28, "FFTF Work Management Process"). It is the intent of this Configuration Plan to not preclude making **Minor Changes** software changes using only the SCR attached to a simple work package (i.e., a J-3). However, if the work control process requires a full work package (i.e., a J-1), then this must be followed. Whichever work control document is used, the SCR shall be included and used to document the software implementation and testing.

3.2.4 Preparing the Change

To the extent possible, the change shall be developed and tested off-line on the development Engineering Workstation. Prior to installation, the overall new configuration shall be verified to be functional using the built-in simulation mode. The Cognizant Engineer is responsible for ensuring that all related documentation is changed.

3.2.5 Installing and Testing the Change

As part of the installation process, the prior file versions shall be retained so that the configuration can easily be restored to the previous Release Version. Installation of the

revised software for testing shall be controlled as a Limited Release in accordance with EI-074 and A-23.

The change shall be tested commensurate with the extent and nature of the change. Changes, such as a display-only change, which do not affect the process may be tested under the authority of the SCR. More extensive changes may require a detailed procedure to organize the resources and system operations to conduct the test. Some adjustments or corrections to the software may be made during this phase, consistent with the approved work package.

3.2.6 New Release Version

After the change has been installed and successfully tested, the Release Version documentation (section 3.1.13) and backup media (section 3.1.14) shall be prepared. Closeout of the SCR shall identify the changes and testing performed to implement the change, and the new Release Version shall be either identified or attached.

3.2.7 Release for Plant Use

When all testing and documentation is completed, the new Release Version can be installed for Unlimited Use in the Plant. The new version shall be installed from the released media, rather than being "left" installed after the testing evolution.

3.3 CONFIGURATION STATUS ACCOUNTING

Section 3.1, Configuration Identification, describes how individual components are identified, including their revisions. The software Release Document prescribes the versions of each file or component that constitute a particular release. The SCR 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 security system is configured by the System Administrator, who defines the security system layout, passwords, user capabilities and restrictions.

The System Administrator assigns each user (e.g., 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 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 may be 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 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.

3.5.4 Supervisor

The Supervisor is an Operator with selected additional authority, such as inhibiting alarms. Supervisor requires an additional password.

3.5.5 Guest

The Guest account is entered by default upon system startup, or upon logging out of the above accounts. Guest provides view-only capability, with reduced navigation capabilities. The Guest user also cannot shutdown the system.

3.6 BACKUP AND RECOVERY

Media control is exercised to ensure that the Microsoft, Intellution, and Hanford-developed software is backed up after each modification. Backups will allow reconstruction of the computer software within a few workdays. Two sets of backups shall be maintained at locations physically separated from the application location. This Configuration Management Plan does not require these backups to be on removable media, however, the backup shall be in accordance with A-23 (which currently does prescribe removable media). At least the two preceding versions shall be retained, although these may need to be in other locations in order to not conflict with A-23.

Historical data files will be transferred to removable media weekly or monthly as necessary. These records are maintained 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 historical data. The label shall contain the system identifier, data name (e.g. HISTORICAL DATA), start and end dates representing the time period of collected data, and a volume number. For example:

SRS HISTORICAL DATA 09/10/99 TO 09/16/99 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 Microsoft and Intellution software.

To facilitate revision accounting per this document, a custom script may be prepared to generate the "Release Document" described in section 3.1.13.

5.0 SUPPLIER CONTROL

Windows NT and Paradym/FIX are commercially available products produced by their respective suppliers. 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 with these products will be communicated to the respective Supplier. The Supplier will make and test any revisions in accordance with their internal methodology. Prior to implementing the revision, the 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 six months.

7.0 REFERENCES

HNF-PRO-244, "Engineering Data Transmittal Requirements."

HNF-PRO-286, "Test Control."

HNF-PRO-309, "Computer Software Quality Assurance Requirements."

HNF-PRO-440, "Engineering Document Change Control Requirements."

HNF-PRO-709, "Preparation and Control Standards for Engineering Drawings."

HNF-PRO-2778, "IRM Application Software System Life Cycle Standards."

A-23, "FFTF Computer Systems Software Physical Control Procedure"

A-28, "FFTF Work Management Process."

HNF-PRO-CSDD-TBD, "SRS Computer Software Design Description."

Figure 1: SRS Change Request/Problem Report

CR/PR Number _____

Page 1 of _____

1. Software/Document Identification (Name): _____

2. Prepared by: _____ Date: _____
System Name: _____

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. JCS Ref: _____ ECN Ref: _____

13. 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 (CR/PR) 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 (WO) 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 Engineering Change Notices.
11. Describe how the change was verified. Reference or attach applicable documents.
12. Record implementing JCS number and/or ECN number(s) for reference, or n/a if not applicable.
13. Record approvals indicating requested changes have been completed or the problem report resolved. Record the software release number which implements the change.

Figure 2: Change Request and Problem Report Log

SYSTEM NAME _____ CUSTODIAN NAME _____

<u>CR/PR #</u>	<u>DATE SUBMITTED</u>	<u>SUBMITTED BY</u>	<u>PRIORITY</u>	<u>TITLE</u>
	<u>STATUS/RESOLUTION</u>			

[illegible]