POEF-LMUS-14

CONFIGURATION CONTROL PLAN FOR THE PORTS NCS IBM RS/6000

1996

by

Angela S. Brown
Battelle

Under Contract 400183

to

LOCKHEED MARTIN UTILITY SERVICES, INC.

PORTSMOUTH GASEOUS DIFFUSION PLANT
P.O. Box 628 Piketon, Ohio 45661

Under Contract USECHQ-93-C-0001

to the

U.S. ENRICHMENT CORPORATION

Available to DOE and DOE Contractors from the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831; prices available from (615) 576-8401, FTS/626-8401.

Available to the public from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.

DISTRIBUTION

LOCKHEED MARTIN UTILITY SERVICES, INC.

Portsmouth

J. Harris
R. Lemming
B. Rumble (4)
J. Smith

Central Files (2)
X-710 Technical Library (2)
Technical Review (2)

Battelle-Columbus

A. Brown
M. Carmel

S. Negron
Files (2)

Table of Contents

1.0 Introduction

The configuration control plan for nuclear safety (NS) software system used by the Nuclear Criticality Safety group will:

1.1 Ensure accurate and reliable results

1.2 Prevent unauthorized changes to the software

1.3 Restrict access to approved System Users only

1.4 Provide a disaster plan in the event of a system failure

1.5 Define positions and responsibilities for the Nuclear Safety Software Team

2.0 Scope

This document describes the actions and responsibilities for maintaining the quality and integrity of the NS software resident on the IBM RS/6000 workstation managed by the Nuclear Criticality Safety group at the Portsmouth Gaseous Diffusion Plant. This document does not address the validation of NS software packages for the RS/6000. These validations are covered in separate documents.

3.0 Definitions

Configuration Control: The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests.

Configuration Item: A collection of hardware or software elements treated as a unit for the purpose of configuration control.

Disaster: For the purpose of this control plan, a disaster is an unforeseen major failure of the NSS system, such as hard disk failure or major system malfunction.

Disaster Plan: A description of contingency steps to be initiated to recover from a disaster including restoration of calculational ability.

Executable Code: The machine-language program that is the output after translation (compiling) and linking of the source.

Non-conformance: Any event in which there is loss, damage, or alteration of any of the system software or hardware, loss of or damage to system files, such as user files, or any event that affects the reliability of the calculations performed by the system. (e.g., user files are missing, a code will not run, a piece of the hardware is damaged, etc.)

Nuclear Safety Software (NSS): Software utilized mainly for the purpose of nuclear criticality safety calculations.

Password: Combination of letters, numbers, or symbols specific to each person that allows that person only access to the system which ensures user knowledge protection of the system.

Production Storage Area: A computer storage area from which the NS software is invoked by approved System Users. Only the current version of the NS software shall be in the Production Storage Area. Only the System Administrator and a designated back-up shall have write access to this area. This area will be located in the /usr/local/nss/"code"/prod subdirectory, where "code" is the specific NSS code (e.g., mcnp4a).

Software: Instructions that determine and define the operation of an electronic computer or computer system. Data tables that are used as a basis for decision making by programs are included.

Software Configuration Control: The systematic evaluation, coordination, verification, implementation, and documentation of all changes to software.

Software System: A group of related programs and data that act in concert toward a particular purpose, have a common developing organization, and are suitable for a single set of control mechanisms.

Source Code: The original mnemonic or high-level statement versions of a program. The starting information or "source" from which the final "object" (machine language or executable code) is derived.

Source Storage Area: An area in computer storage in which the source code is stored. This area will be located in the /usr/local/nss/"code"/source subdirectory.

Storage (Also "External storage"): A portion of a computer system where software and data are stored. This is most commonly a magnetic disk, but other media, such as magnetic tape or a CD-ROM, may be used where appropriate. Storage may be on-line or off-line (external) to the computer operating system.

System Administrator: An individual responsible for the control of software for a defined Software System, including issuance, revision, documentation, and archiving.

System Manager: The person appointed to represent the NCS group in the implementation of a software configuration control plan for defined software system(s).

System Security Administrator: An individual appointed by the System Manager responsible for performing system security functions and any System Administrator activities in the System Administrator's absence.

System Security: The protection of the system software and information stored on the system from alteration or misuse.

System User: Person given access by the System Administrator and approved by the System Manager to use the RS/6000 and the software contained on it, including the Nuclear Safety Software.

Test Storage Area: An area in computer storage in which software verification tests are performed in a simulated production environment. Access to the Test Storage Area is limited to that necessary for testing. This area will be located in the /usr/local/nss/"code"/test subdirectory.

Validation: Validation is the establishment of the bias in the results produced by the combination of the computer software, computer hardware, the data libraries, and the modeling method employed. When experimental data is unavailable, a calculational method that has been shown to be valid by comparison with experimental data may be used, provided sufficient allowances are made for uncertainties in the data and in the calculations. NOTE: Validation is not a required part of the Verification Test.

Validation Storage Area: An area in computer storage in which the validation package is stored. This area will be located in the /usr/local/nss/"code"/valid subdirectory.

Verification Test: A periodic comparison of the results of a sample set of problems from the validation data set to the results of the same problems from the original validation.

Version: A number and/or letter attached to the name of a code in order to identify the version of the computer code (e.g., MCNP4a).

Workstation: The computer and all peripherals specifically designated in Appendix F of this report.

4.0 Staff Responsibilities

4.1 Section Manager

4.1.1 Appoints/Removes System Manager.

4.2 System Manager

4.2.1 Appoints/Removes System Administrator.

4.2.2 Appoints/Removes System Security Administrator.

4.2.3 Approves System Users.

4.2.4 Orders activation and deactivation of System User Accounts.

4.2.5 Schedules annual NS software charter meeting.

4.2.6 Approves modifications to the system.

4.3 System Administrator:

4.3.1 Serves as the principal Nuclear Criticality Safety contact to the software user with regard to the content of NS software.

4.3.2 Provides notification to software users of changes to the software systems, non-conformance reports, and current NS software on the system.

4.3.3 Participates in the handling and resolution of software non-conformance reports as prescribed in this plan.

4.3.4 Performs quarterly verification of all validated NS software.

4.3.5 Assumes overall responsibility for the configuration control of the Nuclear Safety Software System.

4.3.6 Retains a current copy of the NSS Charter (See Appendix C for charter).

4.3.7 Requests an external (to the NCS section) surveillance/audit of configuration control once every 5 years for NS software utilized for nuclear safety computations.

4.3.8 Maintains a current listing of System Users.

4.3.9 Distributes pertinent information on the NS software changes, validations, etc. to system users as appropriate.

4.3.10 Maintains hard copy documentation for 5 years, including:

a. Configuration Control Plans
b. Software Non-conformance Reports (Appendix A)
c. Request for User Access (Appendix B)
d. Audit and Surveillance Reports
e. System Users Membership List
f. NSS Charter (Appendix C)
g. Disaster Plan for System (Appendix D)

h. System Hardware Change Requests (Appendix E)

i. System Hardware and Components List (Appendix F)

j. Documentation on Verification Testing

4.3.11 Updates the Configuration Control Plan and sends a copy to all System Users.

4.3.12 Performs the transfer of new NS software to the Production Storage area when all proper tests are completed.

4.3.13 Restricts user access to approved System Users. The Request for User Access form (Appendix B) as received from the System User, shall be used for this purpose. The System Administrator shall activate or deactivate System Users as instructed by the System Manager.

4.3.14 Develops, implements, and maintains an NS Software System User's Manual.

4.3.15 Subject to System Manager approval, procures new computer equipment and ensures the maintenance of the computer equipment as needed.

4.3.16 Ensures the NS software used on the system is properly validated for the intended use.

4.3.17 Authorizes access to the NS software covered under this plan for System Users per the User Access form (Appendix B). Also provides

notification to the System Manager when user access needs to be removed.

4.3.18 Implements Disaster Plan when appropriate and forwards a copy of the plan to the System Users (Appendix D).

4.3.19 Reports problems encountered to the System Manager using the Software Non-conformance Report (Appendix A).

4.3.20 Restores lost information from a backup in the event of a system disaster.

4.3.21 Performs differential tape backups every weekday (Monday-Thursday excluding Lockheed Martin holidays).

4.3.22 Performs full tape backups weekly (Friday or last day of work week).

4.3.23 Ensures that a bootable system image shall be transferred to tape at least monthly.

4.3.24 Has access to the system key.

4.4 System Security Administrator

4.4.1 Assumes the responsibilities of System Administrator in the event that the System Administrator is not available.

4.4.2 Has the same access to the system as the System Administrator, including holding the root password and having access to the system key.

4.4.3 Has access to all system backup tapes, documentation, archived tapes, or any other material necessary to properly perform System Security Administrator activities.

4.4.4 Labels any electronic media used with the system and the hardware system itself with the correct sensitive stickers.

4.4.5 Conducts an annual confirmation of the model and serial numbers on the system hardware to assure that it has not been tampered with.

4.4.6 Changes root password annually, and reports new root password to the System Administrator.

4.4.7 Annually informs System Users of the need to change their system password.

4.5 System Users

4.5.1 Requests System User access through the access request form (Appendix B).

4.5.2 Immediately reports any system event deemed unusual to the system administrator.

4.5.3 Protects personal password from disclosure to others and changes password annually.

4.5.4 "Logs off" or "password locks" the system when unattended.

4.5.5 Ensures that any NS software used is the currently approved version and that the use and application are validated.

5.0 NS Software Identification

Unambiguous labeling shall provide traceability from source modules to executable modules. Versions must be uniquely identified in such a way that the update sequence may be readily determined. The version number and revision number shall be listed at least once on all output.

6.0 NS Software Location

A copy of the validated NS software validation package shall be maintained in the Validation Storage Area. A duplicate copy shall be maintained by the system administrator for use in the configuration control verification for all validated nuclear safety software.

An identical copy of the NS software will be maintained by the system administrator on the IBM RS/6000 for daily use by the System Users. Figure 1 shows the location of Nuclear Safety Software relative to the root directory (the root/usr/local/nss directory may contain all nuclear safety codes). Additional sub-directories for each code may contain production versions, data libraries, validation data sets, and code-specific support utilities.

In terms of location, old versions of codes should be treated as separate codes. Each old code will have its own subdirectory under the NSS subdirectory.

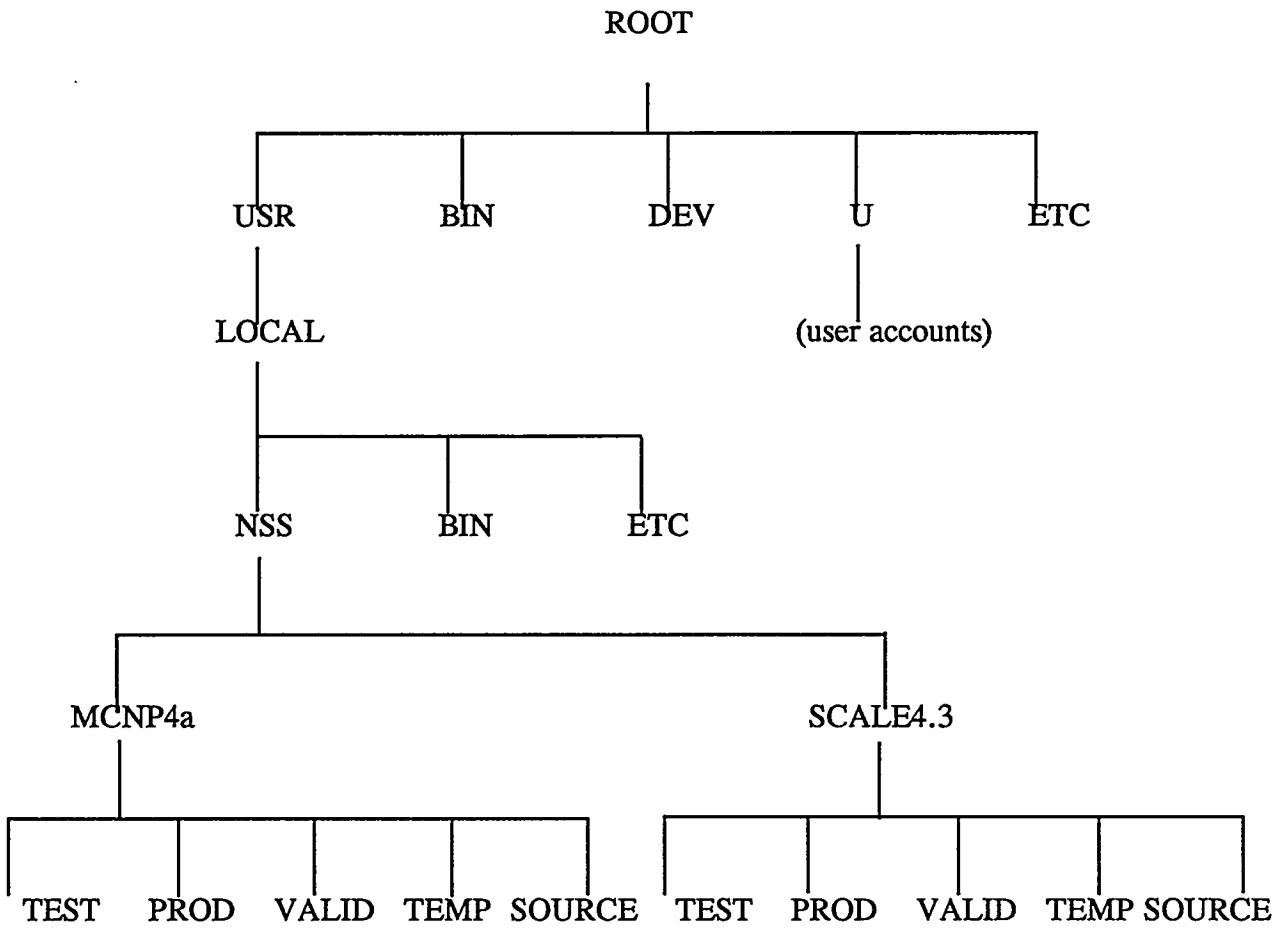

Figure 1. Location of Nuclear Safety Software on IBM RS/6000

7.0 NS Software Protection & Control

7.1 NS Software Protection

In order to assure that the NS software packages available to the users are accurate, various steps will be taken by the system administrator upon installation such that no user may accidentally or purposefully alter the NS software or data libraries in any way. This is to be achieved by protecting the files as follows:

7.1.1 User access to the NSS source codes will be read only. This will prevent any unauthorized changes to the source code while reading the source code.

7.1.2 User access to the executable version of a NSS code will be execute permission only.

7.2 NS Software Control

NS software control will be achieved through the following steps:

7.2.1 System Users of the NS software are responsible for ensuring that any NS software used is the currently approved version and that the use and application are validated.

7.2.2 All modifications to the system (hardware, NS software, or operating system changes) require the approval of the System Manager.

7.2.3 Hard copy computer printouts shall have printed on a header the version and date of revision of the principal NS software unit generating the printout.

8.0 Non-conformance Report Procedure

8.1 Initiating a Non-conformance Report

8.1.1 A Non-conformance Report is initiated by completing Part A of the Non-conformance Report (Appendix A).

8.1.2 The request is sent to the System Administrator.

8.1.3 The System Administrator transmits the report to the System Manager and the other System Users as needed to determine the actions to be taken to prevent the recurrence of the Non-conformance.

8.2 Non-conformance Report Consequences

8.2.1 The Non-conformance Report Procedure provides Non-conformance notification to all System Users.

8.2.2 In extraordinary cases, the System Administrator or the System Manager may authorize shutting down a program until the solution to the Non-conformance can be determined.

9.0 NS Software Testing

9.1 Verification Testing

9.2.1 Quarterly verification testing will be conducted by the System Administrator or designated alternate. Most recent verification test results will be kept in the Test Storage Area.

9.2.2 Approximately 15 of the validation cases (3 cases from each subset) will be run for the verification test for each NSS code. The results of the verification test will be compared to those of the validation.

9.2.3 Documentation on the verification test will be generated by the System Administrator. The documentation will include the date(s) on which the verification test was run, the name and signature of the person who ran the verification test, the name and signature of the person who checked the verification test, and any other information deemed pertinent by the System Administrator.

9.2 Validation

9.2.1 Any new NS Software added to the system must be validated before being used for NS production calculations and that validation must be documented.

9.2.2 If the operating system software or the CPU are replaced, validation testing needs to be performed and documented.

10.0 System Backup Policy

In order to ensure that the loss of critical data is avoided, a rigid system backup policy is employed for the IBM RS/6000. Daily system differential backups are performed each day. This differential backup copies all files with a time stamp different than that of the last full system backup. Each daily differential backup is copied to a unique tape corresponding to the day of the week (Mon, Tues, Wed, Thurs). The Friday, or last working day of the week, tape is used for the weekly full system backup. There are no backups performed on Saturday or Sunday or on Lockheed Martin Utility Services holidays.

Two copies of the full system backup are made each Friday. A copy of each Friday's full system backup will be archived for 10 weeks, after which time all but the first Friday of the month will be recycled back into the Friday backup pool of tapes. Full backup tapes corresponding to the first Friday of the month will remain in storage for 2 years.

A bootable system image shall be transferred to tape at least monthly.

Only the members of the NSS Team (the Section Manager, System Manager, System Administrator, and the System Security Administrator) shall have access to these tapes.

11.0 References

1 American Nuclear Society, ANSI/ANS 8.1, "Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors," Revised 1988

2 Lee Jr., Billy L., POEF-LMUS-12,"Validation of the CSAS25 Calculational Sequence in SCALE-4.2 and the 27 Energy Group ENDF/B-IV Cross Sections on the PORTS NCS IBM RS/6000 Workstation," June 1996

3 Negron, Scott B., POEF-LMUS-13,"Validation of MCNP4a for Highly Enriched Uranium Using the PORTS NCS IBM RS/6000 Workstation," June 1996

Appendix A

Software Non-conformance Report

The Software Non-conformance Report shall include the following information, listed in the following structure:

Part A Report of Non-conformance or Error

- Software users name
- Software title/version/date (if applicable)
- Description, cause, and effect of error
- Recommended corrective action(s)

Part B Non-conformance Assessment and Action Plan

- Cause of Non-conformance
- Recommended Action(s)
- System Manager and System Administrator approval

Appendix B

Request for User Access

The proposed user and his or her supervisor have been informed and understand that validation, (establishment of correctness or bias in calculated results) is a user responsibility and that Lockheed Martin Utility Services makes no claim of correctness for the computer software or for computer calculations performed by others.

Name _____ Date ____/____/_____

Telephone _____

Badge Number _____

Mail Stop _____

User's Supervisor (Signature) _____

(To Be Completed By System Administrator)

User access activation date __/__/__ Deactivation date __/__/__

System Administrator Signature _____

System Manager Signature _____

Appendix C

NSS Charter

Objective: The Nuclear Safety Software (NSS) Team acts as the change control board for nuclear safety software. The team shall:

- maintain the configuration control plan
- determine and implement necessary changes to the NS software pursuant to the configuration control plan
- address software Non-conformance reports as appropriate
- provide assistance to System Users in the area of configuration control
- consist of the Section Manager of the NCS group, the System Manager, the System Administrator, and the System Security Administrator.

Meeting Frequency: At the discretion of the NSS Team (minimum - once per year)

Approved by:

NCS Section Manager	PRINT	SIGNATURE
System Manager	PRINT	SIGNATURE
System Administrator	PRINT	SIGNATURE
System Security Administrator	PRINT	SIGNATURE

Appendix D

NSS Disaster Plan

In the event that an unforeseen major failure of the NS system, such as hard disk failure or major system malfunction, the following Disaster Plan will be implemented.

— System hardware will be restored to operational condition by replacing any faulty components such as hard drives, memory, devices, etc., as necessary.

— The system directory and file structure will be restored from the latest full system backup. Additional files may be restored from other backups such as a daily user backup or an older archived backup.

— A full system verification will be performed before any production use.

Appendix E

System Hardware Change Request

In the event that the system hardware configuration is changed either permanently or temporarily, the following information must be specified in a System Hardware Change Report. The report must be sent to all system users. The System Hardware Change Report must include the following but may contain additional information as well.

- Reason for the change
- Components to be removed, added, or changed
- Estimation of system down time
- Dates and times of changes
- Impact on system operation after change
- Permanent or temporary change

If the CPU is replaced, validation testing must be performed and documented before production use.

Appendix F

PORTS NCS

IBM RS/6000 System and Components

Component	Manufacturer	Name	Model #	Serial #
Keyboard	IBM	N/A	51G8572	0025327
Computer	IBM	RS/6000	410	MS70062612465
CD Rom Drive	IBM	N/A	7210	26-C1482
8mm Tape Drive	Falcon	N/A	PAT04081	9518-0223
2GB Hard Drive	Falcon	N/A	SMB-04001	9524-7431
Power Controller	Kensington	Masterpiece	N/A	88070953
Monitor	IBM	P200	6555-703	55-29121

Appendix G

Periodic Tasks to be Performed for the IBM RS/6000

Daily (Every Business Day)
Incremental tape backups

Weekly
Full tape backups

Monthly
Bootable system image transferred to tape.

Quarterly
Verification Testing

Annually
Review the configuration control plan
Check system hardware model and serial numbers
Hold NSS Charter meeting

Every Five Years
Request an external (to the NCS section) audit of configuration control for nuclear safety software

As Needed
Update configuration control plan
Update System Users list
Update list of current NS software on the system
Notify users of updated versions of NS software
Validation of new NS software or new versions of NS software