CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

CORRECTIVE ACTION REQUEST

CAR No: 97-02   Associated AR, SR, NCR No: _CNWRA Audit Report 97-01_

PART A: DESCRIPTION OF CONDITION ADVERSE TO QUALITY

Contrary to the requirements of TOP-018, paragraph 5.8, changes (both "serious" and "minor") were implemented in MULTIFLO, Version 1.0, without completion of a Software Problem/Change Report (SPCR). Some, but not all, changes were documented in the developer's scientific notebook. This code has been distributed to personnel within the CNWRA and traceability would not be possible if personnel were to use it for licensing purposes or in published documents.

J.C. Trbovich

Initiated by: T.C. Trbovich   Date June 12, 1997

PART B: PROPOSED ACTION   Responsible Party: B. Sagar/P. Lichtner
                                               Response Due: July 11, 1997

1) **Extent of Condition:**
   A team composed of P. Lichtner, S. Mohanty, W. Murphy, and M. Ahola will investigate the extent to which stated condition affects other CNWRA codes. Team recommendation is due by October 2, 1997.

2) **Root Cause:**
   The TOP-018 requirements are ambiguously worded and it is not clearly stated when a SPCR must be prepared.

3) **Remedial Action:**   **Proposed Completion Date:** November 30, 1997

   Change TOP-018 to clearly identify when a SPCR must be prepared. A team has been formed to study the problem and propose changes to TOP-018. The change to TOP-018 is due by November 30, 1997.

4) **Corrective Action to Preclude Recurrence:**   **Proposed Completion Date:** January 1, 1998

   Change TOP-018 to clearly state circumstances requiring preparation of a SPCR form. Completion of all actions is by January 1, 1998.

Director: _B. Sagar_   Date: 7/8/97

PART C: APPROVAL
Comments/Instructions

Director of QA: _[signature]_   Date: 7/9/97

PART D: VERIFICATION OF CORRECTIVE ACTION IMPLEMENTATION

1. TOP-018 Committee Report issued 9/23/97
2. TOP-018 re-written by Important Committee. Revised by & checked technical reviewers and RCh Director 3. Sent to NRC 2/11/98 - response by NRC 3/10/98. 4. TOP-018 distributed 5/1/98.
5. A TOP-018 Rev 6 Training session was held 5/6/98.

Verified by: _[signature]_   Date: 5/19/98

J.C. Trbovich   6/25/98

Distribution: W. Patrick
B. Sagar
EMS
Directors
P. Lichtner
W. Murphy
S. Mohanty
J. Stamatakos
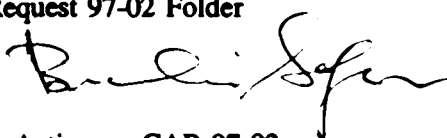
CNWRA FORM QAP 14-2

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

MEMORANDUM

April 20, 1998

TO: QA Records Corrective Action Request 97-02 Folder

FROM: Budhi Sagar, Technical Director

SUBJECT: Extension Request for Corrective Action on CAR 97-02

REFERENCE: CAR 97-02, Annual 1997 CNWRA QA Audit

This memorandum to the Corrective Action Request (CAR) 97-02 folder is to document progress and request an extension.

CAR 97-02 was originated June 12, 1997 at the conclusion of the 1997 annual CNWRA QA Audit. It was responded to by B. Sagar on July 8, 1997. A team of CNWRA technical staff members was assembled to help revise Technical Operating Procedure (TOP)-018 "Development and Control of Scientific and Engineering Software." That team was composed of P. Lichtner, S. Mohanty. W. Murphy, and M. Ahola (later replaced by J. Stamatakos when Ahola took other employment).

The TOP-018 Improvement Team completed their work and the draft Operating Procedure went through Technical and Programmatic review. A decision was made toward the end of that cycle to submit the draft TOP-018 directly to the NRC for comments. On February 11, 1998, the draft TOP was sent to the NRC (letter to Ms. Deborah A. DeMarco from Budhi Sagar, requesting NRC review). The NRC responded on March 18, 1998 with three comments (correspondence attached) and they were integrated into the final draft of the TOP-018 document. A QA Review was accomplished and a Concurrence review was requested from Wes Patrick. In that Concurrence review, six pages of comments were generated and some of the comments were major differences in approach. These are being resolved between the President of the CNWRA and the TOP-018 Improvement Team.

Although the targeted date for completion of TOP-018 was set for April 20, 1998 (and total completion of training, remedial, corrective actions, and training was targeted for this CAR as May 22, 1998), it is prudent to request an extension for the completion of TOP-018 to be extended to May 22, 1998 and the completion of all related actions to June 12, 1998. If you have any questions regarding this extension request, please contact me at ext. 5252.

Approved: _____ 4/21/98

       Bruce Mabrito, Director of QA Date

cc: TOP-018 Process Improvement Team
   CNWRA Directors/Element Managers
   W. Patrick   R. Folck/T. Trbovich/D. Dunavant (Institute QA)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 18, 1998

Budhi Sagar, Ph. D.
Technical Director
Center for Nuclear Waste Regulatory Analyses
6220 Culebra Road
P.O. Drawer 28510
San Antonio, TX 78228-0510

SUBJECT CODE: 2of. 01
PROJECT NO. 20 - 1402 1591

SUBJECT: APPROVAL OF THE TECHNICAL OPERATING PROCEDURE (TOP)-018, "DEVELOPMENT AND CONTROL OF SCIENTIFIC AND ENGINEERING SOFTWARE FOR NRC REVIEW" (AI 20-1402-159-801)

Dear Dr. Sagar:

The subject document, dated February 11, 1998, has been reviewed and found acceptable with inclusion of the recommended comments provided below.

Comment 1: Page 3, section 3, "DEFINITIONS." Two definitions needed.

> **Recommendation:** Define "installation testing" used on page 6 in Table 1 (footnote 1)
> **Recommendation:** Define "regulatory reviews" used on pages 2 (section 1), 6 (section 5.1), and 13 (section 5.10.1).

Comment 2: Page 6, Table 1. Possible error in "Table 1, ACQUIRED/EXISTING SOFTWARE, to be modified, Software Development Plan (SDP) Design and Development."

> **Recommendation:** Recommend "x" in this box.

Comment 3: Page 8, section 5.4 - "Software Development Plan," paragraph 5.4.1. Testing as one goes along, instead of only one is about to ship (which may be going on already as a question of prudence even it not as a question of policy) should be performed.

> **Recommendation:** After "testing that will be applied to the software," add "including informal as-you-go testing of logical divisions of code such as subroutines and functions, ..."

Sincerely,

Deborah A. DeMarco
CNWRA Deputy Program Manager
Program Management, Policy Development
and Analysis Staff, NMSS

Copy Dirs/Encs
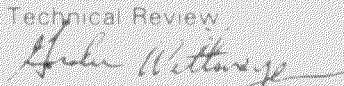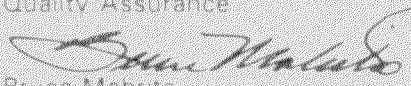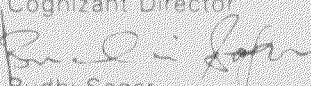Pctr Lichtner

cc: J. Linehan, NMSS/PMDA

Title DEVELOPMENT AND CONTROL OF SCIENTIFIC AND ENGINEERING SOFTWARE

EFFECTIVITY

Revision 6 of this procedure will become effective after NRC approves document. This procedure consists of the pages and changes listed below.

Page No.	Change No.	Date Effective
All	0	05/01/98

Supersedes Procedure No. TOP-018, Rev 5, Chg 0, dated 04 03 97

Approvals			
Written by Peter Lichtner	Date 5/1/98	Technical Review Gordon Wittmeyer	Date 5/1/98
Quality Assurance Bruce Mabrito	Date 5/1/98	Cognizant Director Budhi Sagar	Date 5/1/98

CNWRA Form TOP-1 (8 93)

Center for Nuclear Waste Regulatory Analyses

6220 CULEBRA ROAD • P.O. DRAWER 28510 • SAN ANTONIO, TEXAS, U.S.A. 78228-0510
(210) 522-5160 • FAX (210) 522-5155

May 1, 1998
Contract No. NRC-02-97-009
Account No. 20-1402-159

U.S. Nuclear Regulatory Commission
Attn: Ms. Deborah A. DeMarco
Office of Nuclear Material Safety and Safeguards
Program Management, Policy Development and Analysis Staff
Mail Stop 8-A23
Washington, DC 20555

Subject: Transmittal of Technical Operating Procedure (TOP)-018, Development
            and Control of Scientific and Engineering Software for NRC Review
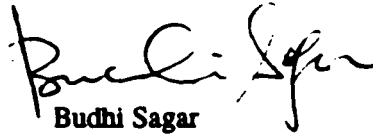   (AI-20-1402-159-801)

Dear Ms. DeMarco:

Enclosed is the Center for Nuclear Waste Regulatory Analyses (CNWRA) TOP-018, Revision 6. This
CNWRA operating procedure addresses the NRC comments of March 24, 1998. The changes requested
in the referenced correspondence have been made resulting in an improved procedure.

This deliverable is being carried in the Commitment Control Log as Administrative Item 20-1402-159-
801. After staff training with the revised TOP-018, the Quality Assurance Corrective Action Request No.
97-02 will be completed. We thank you for your assistance in revising TOP-018, which is important for
both our organizations.

Please contact me at(210) 522-5252 or Peter C. Lichtner at (210) 522-6084 if you have any questions.

Sincerely yours,

Budhi Sagar
Technical Director

HFG/lg
Enclosures
cc: B. Meehan   J. Thoma   P. Lichtner
       J. Linehan   K. McConnell   S. Boyanowski (SwRI Contracts)
       B. Stiltenpole   T. McCartin
       M. Federline   W. Patrick
       J. Greeves   CNWRA Directors/Element Managers
       K. Stablein

TOP-018 DEVELOPMENT AND CONTROL OF SCIENTIFIC ENGINEERING SOFTWARE
Revision 6, Change 0

CONTROLLED COPIES:

Theodore Carter, NMSS
Barbara Meehan, Contracts
Barbara Stiltenpole, NMSS & (20) Uncontrolled copies
Deborah DeMarco, NMSS
Rose Burn, NMSS
Christiana Lui, NMSS
Tim McCartin, NMSS
Keith McConnell, NMSS

UNCONTROLLED COPIES:

DCS
Tae Ahn, NMSS
Mike Bell, NMSS
John Bradbury, NMSS
David Brooks, NMSS
Kien Chang, NMSS
Richard Codell, NMSS
Neil Coleman, NMSS
Norm Eisenberg, NMSS
Margaret Federline, NMSS
Kim Gruss, NMSS
Philip Justus, NMSS
Bret Leslie, NMSS
Mysore Nataraja, NMSS
Jeff Pohle, NMSS
N. King Stablein, NMSS
John Thoma, NMSS
John Trapp, NMSS
Sandra Wastler, NMSS
Rick Weller, NMSS

CENTER FOR NUCLEAR WASTE REQULATORY ANALYSES
MEETING ATTENDANCE

SUBJECT OF MEETING: Technical Operating Procedure - 018
Development and Control of Scientific & Engineering Software Rev. 6 - Training

DATE: May 06, 1998   **Time: 10:30 A.M.**   **LOCATION: Conference Room A237**

PERSON	ORGANIZATION	TITLE/FUNCTION	TELEPHONE NUMBER
Joe Bangs	CNWRA	Sr. Res. Scientist	5224
Laura Deere	CNWRA	Research Scientist	4881
Amitava Ghosh	CNWRA	Sr. Res Engineer	3314
James Weldy	CNWRA	Engineer	6800
Sean Brossia	CNWRA	Research Engineer	5797
David Pickett	CNWRA	Res. Sci.	5582
Asad Chowdhury	CNWRA	Mgr - MGFE	x5151
Simon Hsiung	CNWRA	Pri. Eng.	5209
Peter Lichtner	"	Pri. Sci.	6084
AMIT ARMSTRONG	CNWRA	RES. ENGINEER	5182
Ron Green	"	Prin Sci	5305
Larry McKague	CNWRA	GLGP Eng	5133
Gerrill Sips	CNWRA	Res Sci.	6329
Mike Miklas, Jr.	CNWRA	Sr. Res. Sci.	5207
David R Turner	CNWRA	Sr. Res Sci.	x2139
R. Martin	"	Res Sci	5541
Randy Fedors	"	Res. Eng.	x6818
Jim Prikryl	"	Res Sci	x5467
Bruce Mabrito	"	Dir QA	x5149
Run Chen	"	Res. Eng	x5157
S. Mohanty	"	Sr. Res. Sci	5K5
Gu Jun Yu	"	Res Eng	6641
Z. Janetzke	"	Analyst	3315
Stamatalo	"	Scientist	5247

CNWRA Form AP-5

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES
TRAINING ATTENDANCE

CAR Folder

SUBJECT OF MEETING: Technical Operating Procedure - 018
Development and Control of Scientific & Engineering Software Rev. 6 / Chg. 0

DATE: May 15, 1998   **Time: 10:00 A.M.**   **LOCATION: Conference Room A237**

PERSON	ORGANIZATION	TITLE/FUNCTION	TELEPHONE NUMBER
Bruce Mabrito	CNWRA	QA	x5149
Britt Hill	"	Sr. Res Sci	6087
Maria Padilla	"	Clerk	6833
R. Nataraju	"	Sr Res Sc	5300 cl
Wesley C. Patrick	"	PRES	5158
S. Mohanty	"	Sr. Res. Sci.	5185
Darrell Dunn	"	Res Engr	6090
English Pearcy	"	EM GHGC	x5540
Mark Ciureca	"	Tech Assist.	- N/A -
Joshua Buckner	"	"	- N/A -
William M. Murphy	"	Principal Scientist	x5263
Narasi Sridhar	"	EM - EBS	6533
Darius Daruwalla	"	Sr. Res. Engnr.	3297
P.	"	Asst OIC	5051
Budhi Sagar	"	Tech. AV	5152
NOTE: John Russell and Pat LaPlante from the			
WTSO were sent viewgraphs and were on			
the speaker Telephone during the Training.			

CNWRA Form AP-5

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES
TRAINING ATTENDANCE

SUBJECT OF MEETING: Technical Operating Procedure - 018
Development and Control of Scientific & Engineering Software Rev. 9 / Chn. 0

DATE: May 15, 1998	Time: 10:00 A.M.	LOCATION: Conference Room A237	
PERSON	**ORGANIZATION**	**TITLE/FUNCTION**	**TELEPHONE NUMBER**
Amer Maggio	CNWRA	QA	x5149
Britt Hill	"	Sr Res Sci	6087
Maria Padilla	"	Clerk	6833
R. Nataraja	"	Sr Res Sci	53041
Wesley C. Patrick	"	PRES.	5158
S. Mohanty	"	Sr. Res. Sci.	5185
Darrell Dunn	"	Res Engr	6090
English Pearcy	"	Em GHGC	x5540
Mark Garcia	"	Tech Assist.	— N/A
Joshua Buckner	"	"	— N/A —
William M. Murphy	"	Principal Scientist	x5263
Narasi Sridhar	"	E.M - EBS	. 6538
Darius Daruwalla	"	Sr. Res. Engnr.	3297
P. Mackin	"	Asst Dir	5054
Budhi Sagar	"	Tech. Dir	5162
Theo Russell	"	Dir Washington Office	301/881-0289
	"	Res Scientist	301/881-0289

TECHNICAL OPERATING PROCEDURE - 018
DEVELOPMENT AND CONTROL OF SCIENTIFIC
AND ENGINEERING SOFTWARE
REVISION 6 - TRAINING

MAJOR CHANGES TO TOP-018

- ADDITION OF A SOFTWARE DEVELOPMENT PLAN (SDP)

- ACCEPTANCE TESTING CLARIFIED FOR DEVELOPER AND QA

- SOFTWARE REQUIREMENTS DESCRIPTION REVISED FORMAT

- CLARIFICATION OF OTHER TOP-018 ACTIVITIES

<table>
<tr><td></td><td>Proc. __TOP-018__</td></tr>
</table>

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES	Proc. __TOP-018__
	Revision __6__
TECHNICAL OPERATING PROCEDURE	Page __1__ of __27__

Title DEVELOPMENT AND CONTROL OF SCIENTIFIC AND ENGINEERING SOFTWARE

EFFECTIVITY

Revision __6__ of this procedure will become effective after NRC approves document. This procedure consists of the pages and changes listed below.

__Page No.__	__Change No.__	__Date Effective__
All	0	05/01/98

Supersedes Procedure No. TOP-018, Rev 5, Chg 0, dated 04/03/97

Approvals			
Written by	Date	Technical Review	Date
Peter Lichtner		Gordon Wittmeyer	
Quality Assurance	Date	Cognizant Director	Date
Bruce Mabrito		Budhi Sagar	

Table 1. Categories and requirements application

Software Category	Software Requirements Description (SRD)	Software Development Plan (SDP) Design & Development	Software Change Reporting and Resolution	Acceptance Testing	Configuration Control, Design Verification & Release	Software Validation Test Plan (SVTP)
Developed/ Modified Software	X	X	X	X	X	X
ACQUIRED/EXISTING SOFTWARE						
Not to be modified				X^1	X	X
To be modified	X^2	X^2	X^2	X^2	X	X
Software allowing user-supplied extensions			X^2	X^2	X	X
[1]Installation testing only. [2]A Software Change Report or equivalent can be used for minor modifications.						

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES **TECHNICAL OPERATING PROCEDURE**	Proc. __TOP-018__ Revision __6__ Change __0__ Page __16__ of __27__

APPENDIX A — SOFTWARE REQUIREMENTS DESCRIPTION OUTLINE

The SRD describes what functions the software is to perform, provides the technical basis and computational approach to be used in developing the software, and provides a vehicle for client approval of software development or changes. All SRD content requirements are "as applicable."

1.0 SOFTWARE FUNCTION

Describe purpose of software and software function.

2.0 TECHNICAL BASIS: PHYSICAL AND MATHEMATICAL MODEL

Describe the physical model and present the mathematical equations the software will solve.

3.0 COMPUTATIONAL APPROACH

3.1 Data Flow and User Interface

Describe the data flow in a flow diagram and the user interface (e.g., command line, GUI,...).

3.2 Hardware and Software Requirements

- Target platform (e.g., PC, SUN,...)

- Operating System (e.g., Solaris, MacOS, NT,...)

- Programming language (e.g., FORTRAN 77, C, C++,...)

3.3 Graphics Requirements

List any special graphics requirements.

3.4 Pre- and Post-Processors

List any pre- or post-processors required to run the software.

4.0 REFERENCES

APPENDICES

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES	Proc. __TOP-018__
	Revision __6__ Change __0__
TECHNICAL OPERATING PROCEDURE	Page __17__ of __27__

APPENDIX B — SOFTWARE DEVELOPMENT PLAN OUTLINE

The Software Development Plan (SDP) describes the project plans for conducting a software development effort. The SDP covers new code development, modification, maintenance, and all other activities resulting in software products and documents. All SDP content requirements are "as applicable." If the content requirements of a given subclause do not apply to a particular project, the developer may delete that subclause as authorized under 5.4.4 of this procedure.

1.0 SCOPE

Introduce the project and define its scope. Summarize the purpose and contents of this document and describe any security or privacy considerations associated with its use.

2.0 BASELINE ITEMS

This section shall describe the software products to be produced under the scope of the project. Examples include code, databases, test information, and manuals.

3.0 PROJECT MANAGEMENT

This section shall describe project planning and oversight activities.

3.1 Work Breakdown Structure

This section shall provide a detailed Work Breakdown Structure for the project period of performance. The task name and estimated labor hours should be included.

3.2 Projected Schedule

This section should include a project schedule.

3.3 Staffing

This section shall identify the staffing requirements and/or specialized training needed for the project.

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES **TECHNICAL OPERATING PROCEDURE**	Proc. __TOP-018__ Revision __6__ Change __0__ Page __18__ of __27__

3.4   Risk Management

Risks associated with cost, schedule, resources, and functionality shall be identified. The following should be listed for each identified risk:

- Discussion of most probable risks.
- Estimate risk probability and impact.
- Options for dealing with the identified risks.

4.0   DEVELOPMENT PROCEDURES

This section shall describe the plans for development of the software product.

4.1   Hardware and Software Resources

Describe the hardware and software resources that are planned to be utilized during the software development effort. This may include both in-house, purchased, or customer supplied hardware and software.

4.2   Software Development Lifecycle

·   Describe the phases used to translate the SRD requirements into software (e.g., prototype, design, first release, alpha/beta testing, production, maintenance, etc.). Each phase should have a set of defined inputs, activities and outputs.

4.3   Coding

Describe the coding conventions adopted for the project. Address the following as appropriate:

- The programming language(s) being used.
- Selected coding style guide.
- Limitations, restrictions, or standards not specifically addressed by the selected coding standard(s).

4.4   Acceptance Testing and Analysis

Acceptance testing is performed to demonstrate to the customer that the computer code meets its specified requirements as documented in the SRD. This section shall address:

- Recording of test cases and test inputs.

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES **TECHNICAL OPERATING PROCEDURE**	Proc. __TOP-018__ Revision _6_ Change __0__ Page __19__ of __27__

- Use of software analysis tools (e.g., FOR_WARN or FOR_STUDY for FORTRAN programs, PC-Metrics, or PC-Lint for C language programs).
- Revision and retesting.
- Analyzing and recording test results.

5.0 CONFIGURATION MANAGEMENT PLAN (CMP)

The configuration Management Plan (CMP) describes the plans for conducting configuration control during the software development effort. This CMP is optional and is distinct from the configuration control carried out by the software custodian.

5.1 Tools

Describe the tools that will be used to perform software configuration management, if any.

5.2 Configuration Identification

Identify the software products that will be placed under configuration control. Identify when each software product will be placed under configuration control. Describe the identification scheme.

5.3 Configuration Procedures

Describe:

- Check-in/check-out procedures if appropriate.
- Creating releases and preparing for deliveries.
- Problem reporting and change control. For example, an SCR form, as shown in Appendix D, may be used to report changes to a baselined code.
- Performing system backups of the software.
- Daily release procedures and cleanup.

6.0 REFERENCES

Reference all documents listed in the SDP.

CNWRA Form TOP-2

SOFTWARE SUMMARY FORM

01. Summary Date:	02. Summary prepared by (Name and phone)	03. Summary Action:
04. Software Date:	05. Short Title:	

06. Software Title:	07. Internal Software ID:

08. Software Type:	09. Processing Mode:	10. Application Area
☐ Automated Data System	☐ Interactive	a. General:
☐ Computer Program	☐ Batch	☐ Scientific/Engineering ☐ Auxiliary Analyses ☐ Total System PA ☐ Subsystem PA ☐ Other
☐ Subroutine/Module	☐ Combination	b. Specific:

11. Submitting Organization and Address: CNWRA/SwRI 6220 Culebra Road San Antonio, TX 78228	12. Technical Contact(s) and Phone:

13. Software Application:

14. Computer Platform	15. Computer Operating System:	16. Programming Language(s):	17. Number of Source Program Statements:
18. Computer Memory Requirements:	19. Tape Drives:	20. Disk Units:	21. Graphics:

22. Other Operational Requirements

23. Software Availability: ☐ Available ☐ Limited ☐ In-House ONLY	24. Documentation Availability: ☐ Available ☐ Preliminary ☐ In-House ONLY

25.

Software Developer: Date:

SOFTWARE CHANGE REPORT (SCR)

SCR No. (*Software Developer Assigns*):	Software Title and Version:	Project No:

Affected Software Module(s), Description of Problem(s):		

Change Requested by: Date:	Change Authorized by (*Software Developer*): Date:

Description of Implemented Change(s) (*If changes not implemented, please justify*):

Description of Tests to Approve the Quality of the Changed Version

Implemented by:	Completed Date:

CNWRA Form TOP-5 (05/98)

SOFTWARE RELEASE NOTICE

1. SRN Number:	

2. Project Title:	Project No.

3. SRN Title:	

4. Originator/Requestor:	Date:

5. Summary of Actions

    □   Release of new software

    □   Release of modified software:

        □   Enhancements made

        □   Corrections made

    □   Change of access software

    □   Software Retirement

6. Persons Authorized Access

Name	Read Only/Read-Write	Addition/Change/Delete

7. Element Manager Approval:	Date:

8. Remarks:

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

MEMORANDUM

February 27, 1998

TO: QA Records Corrective Action Request 97-02 Folder

FROM: Budhi Sagar, Technical Director

SUBJECT: Extension Request for Corrective Action on CAR 97-02

REFERENCE: CAR 97-02, Annual 1997 CNWRA QA Audit

This memorandum to the Corrective Action Request (CAR) 97-02 folder is to document progress and request an extension.

CAR 97-02 was originated June 12, 1997 at the conclusion of the 1997 annual CNWRA QA Audit. It was responded to by B. Sagar on July 8, 1997. A team of CNWRA technical staff members was assembled to help revise Technical Operating Procedure (TOP)-018 "Development and Control of Scientific and Engineering Software." That team was composed of P. Lichtner, S. Mohanty. W. Murphy, and M. Ahola (later replaced by J. Stamatakos when Ahola took other employment).

The TOP-018 Improvement Team completed their work and the draft Operating Procedure went through Technical and Programmatic review. A decision was made toward the end of that cycle to submit the draft TOP-018 directly to the NRC for comments. On February 11, 1998, the draft TOP was sent to the NRC (letter to Ms. Deborah A. DeMarco from Budhi Sagar, requesting NRC review). A copy of this correspondence is in the CAR 97-02 folder for reference.

In a telephone discussion between Ms. DeMarco and B. Mabrito 2/26/98, she stated that she expected to have the NRC technical staff comments back in her hands by March 2, 1998. She could not say how long it would be before they could send to the CNWRA one set of final comments for the CNWRA to act upon.

Although all work and remedial actions targeted for this CAR are set for March 31, 1998 (including all changes to TOP-018 and possible training), it is prudent to request an extension for the completion of TOP-018 to be extended to April 20, 1998 and the completion of all other related actions to May 22, 1998. If you have any questions regarding this extension request, please contact me at ext. 5252.

Approved: _____   2/28/98
          Bruce Mabrito, Director of QA   Date

cc: TOP-018 Process Improvement Team
      CNWRA Directors/Element Managers
      W. Patrick   R. Folck/T. Trbovich/D. Dunavant (Institute QA)

Center for Nuclear Waste Regulatory Analyses

6220 CULEBRA ROAD • P.O. DRAWER 28510 • SAN ANTONIO, TEXAS, U.S.A. 78228-0510
(210) 522-5160 • FAX (210) 522-5155

February 11, 1997
Contract No. NRC-02-93-005
Account No. 20-1402-159

U.S. Nuclear Regulatory Commission
ATTN: Ms. Deborah A. DeMarco
Office of Nuclear Material Safety and Safeguards
Program Management, Policy Development and Analysis Staff
Mail Stop 8-A23
Washington, DC 20555

Subject: Transmittal of a Draft Copy of Technical Operating Procedure (TOP)-018, Development and Control of Scientific and Engineering Software for NRC Review (AI 20-1402-159-801)

Reference: NRC Correspondence of July 8, 1997 from Shirley L. Fortuna to Henry Garcia Regarding the Approval of TOP-018
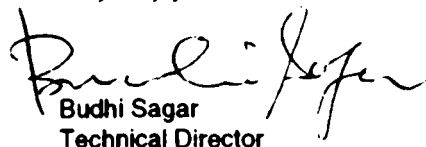
Dear Ms. DeMarco:

Enclosed is a draft of the Center for Nuclear Waste Regulatory Analyses (CNWRA) TOP-018, Revision 6 for NRC review. This CNWRA operating procedure addresses the above referenced correspondence and is being sent to the NRC prior to finalization of the document.

It should be noted that to assist in the effective implementation of this procedure, key CNWRA technical staff have worked on a TOP-018 Team to improve it and have essentially taken "ownership" of this technical procedure. Further, technical reviews of TOP-018 have taken place and responses to reviewer comments have been incorporated into this draft. Finally, the editorial changes requested in the referenced correspondence have been made as long as they meet with the CNWRA Style Guide, which is generally in conformance with the U.S. General Printing Office style recommendations.

We would appreciate a review of this Draft TOP-018 by appropriate NRC staff. This action is being carried in the Commitment Control Log as Administrative Item 20-1402-159-801. We thank you for your prompt attention to this operating procedure, which is important for both our organizations.

Please contact me at (210) 522-5252 or Peter C. Lichtner at (210) 522-6084 if you have any questions.

Very truly yours,

Budhi Sagar
Technical Director

BS/lg
Enclosure

cc: B. Meehan   J. Thoma   P. Lichtner
        J. Linehan   K. McConnell   S. Rowe, SwRI Contracts
        B. Stiltenpole   T. McCartin
        M. Federline   W. Patrick
        J. Greeves   CNWRA Directors Nalehutal
        K. Stablein   CNWRA Element Managers   G:\BRUCE:TOP18.LTR

Washington Office • Twinbrook Metro Plaza, #210 • 12300 Twinbrook Parkway • Rockville, Maryland 20852-1606

To: Annette Mandujano
To: Lucy Gutierrez
To: Maria Padilla
bcc: Bonnie Caudle
bcc: Bruce Mabrito
bcc: Henry Garcia
bcc: Budhi Sagar
From: Bruce Mabrito
Subject: "DRAFT" TOP-018 Going to the NRC
02-12-1998 12:51 PM

   First, this document going to the NRC is an INCOMPLETE document and
that is exactly what we want this time.

   We are sending a incomplete document, meaning that it is not
finished, because we WANT to have the NRC comments so that we CAN finish
the document.

   Second, Annette and I put "DRAFT" on every page of the TOP-018 Rev.
6 document and she will run copies of that.

   Third, NO controlled copies will be sent to the "regular list."
That will only occur after we completely finalize the final Rev. 6
document. That may be as little as two weeks off, two months off, or
two years off (I doubt that very seriously however).

   Annette, please print out this message and put it with the review
documentation that you are assembling for TOP-018. Also, keep a
diskette of the document separate from your hard drive because you may
not be the person working on it when it is returned with (God only know
how many) comments from the NRC. Thanks to all for working with this.
Yes, I know that this is "The Same Only Different," but what can I say?

                    Bruce

To: Budhi Sagar
cc: Peter Lichtner
cc: Wesley Patrick
cc: Henry Garcia
bcc: Bonnie Caudle
bcc: Randall Fedors
bcc: John Stamatakos
bcc: William Murphy
bcc: Sitakanta Mohanty
bcc: Gordon Wittmeyer
bcc: Rui Chen
bcc: Ronald Janetzke
bcc: English Pearcy
bcc: Narasi Sridhar
bcc: Bruce Mabrito
bcc: MEhnstrom@swri.edu at Internet
bcc: Maria Padilla
bcc: rfolck@swri.org at Internet
bcc: JKittle@swri.edu at Internet
bcc: bmabrito@express-news.net at Internet
bcc: Robert Baca
bcc: John L. Russell
bcc: Larry McKague
bcc: Patrick Mackin
bcc: Asadul Chowdhury
bcc: Annette Mandujano
bcc: gmabrito@flash.net at Internet
From: Bruce Mabrito
Subject: Status Report on the Progress of TOP-018, Revision 6
02-01-1998 09:13 PM

Budhi,
    This is a status report on Technical Operating Procedure-018,
Development and Control of Scientific and Engineering Software. A copy
of this e-mail message will be printed and put in the Corrective Action
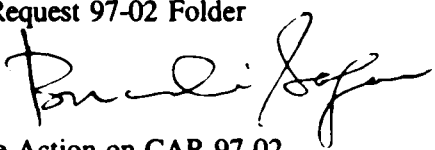Request Folder relating to thes actions, CAR 97-02.

    At this time TOP-018 has been reviewed by the four technical
reviewers and P. Lichtner has responded to their comments, and in so
doing, revised the document to address their comments. The document has
now been changed and typed and is in the hands of R. Fedors who is
reviewing the changes to ensure they address his concerns (before he has
to travel on or about 2/4/98). The document will be routed to the other
technical reviewers (Wittmeyer, Chen, Janetzke) in this same step. P.
Lichtner has suggested that before the document goes into your
programmatic review, it might be best to have the TOP-018 Improvement
Team look at it again. You can speak directly to him on that matter to
have your questions answered and make your views known.

    The extension request you sent to me on 12/1/98 and I approved
12/4/98 stated that "an extension to February 28, 1998 to complete the
remedial actions" would be appropriate. Included in that is you sending
it to the NRC for their review (specifically advised and requested by S.
Fortuna prior to her retirement). Please put that down as an agenda
item to discuss with the NRC in one of your regular meetings

CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

MEMORANDUM

December 1, 1997

TO: QA Records Corrective Action Request 97-02 Folder

FROM: Budhi Sagar, Technical Director

SUBJECT: Extension Request for Corrective Action on CAR 97-02

REFERENCE: CAR 97-02, Annual 1997 CNWRA QA Audit

This memorandum to the Corrective Action Request (CAR) 97-02 folder is to document progress to date to complete corrective actions and request an extension.

CAR 97-02 was originated June 12, 1997 at the conclusion of the 1997 annual CNWRA QA Audit. It was responded to by B. Sagar on July 8, 1997. A team of CNWRA technical staff members was assembled to help take "ownership," as the NRC stated, of Technical Operating Procedure (TOP)-018 "Development and Control of Scientific and Engineering Software." That team was composed of P. Lichtner, S. Mohanty, W. Murphy, and M. Ahola (later replaced by J. Stamatakos when Ahola took other employment). An expert in computer software development and control at SwRI (Dr. Steven Dellenback, Division 10) was brought in to review TOP-018 and make recommendations, which he did for the team in a memorandum dated August 10, 1997. The TOP-018 Revision Committee (sometimes referred to as the TOP-018 Process Improvement Team) issued their report to CNWRA management September 23, 1997. It was followed by an in-depth meeting between CNWRA management and the TOP-018 Revision Committee chairman October 14, 1997. During that meeting, it was decided to proceed with revision of TOP-018 in line with the TOP-018 Committee recommendations. Due to overseas travel and other NRC deliverables and commitments, an incomplete, rough marked up copy of TOP-018 had been produced by the November 30, 1997 target date for proposed completion of remedial actions.

In a meeting between B. Sagar and P. Lichtner, it was decided that an extension to February 28, 1998 to complete the remedial actions (this includes all changes to TOP-018, which must be coordinated with key NRC staff), and to March 31, 1998 to complete all other related possible actions, is necessary. If you have any questions regarding this extension request, please contact me at ext. 5252.

Approved: _____ 12/4/97
              Bruce Mabrito, Director of QA   Date

cc: TOP-018 Process Improvement Team
       CNWRA Directors/Element Managers
       W. Patrick
       R. Folck/T. Trbovich/D. Dunavant (Institute QA)

Center for Nuclear Waste Regulatory Analyses

6220 CULEBRA ROAD • P.O. DRAWER 28510 • SAN ANTONIO, TEXAS, U.S.A. 78228-0510
(210) 522-5160 • FAX (210) 522-5155

October 30, 1997
Contract No. NRC-02-97-009
Account No. 20-1402-158

U.S. Nuclear Regulatory Commission
ATTN: Mrs. Barbara D. Meehan
Contracting Officer
Division of Contracts
TWFN Mail Stop 7 I2
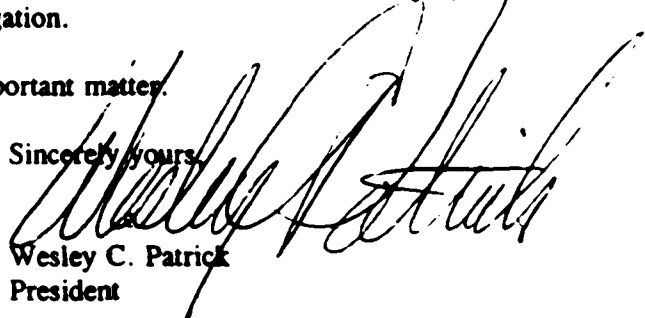Washington, D.C. 20555

Subject: Total-System Performance Assessment Code Development Lessons Learned Analysis

Dear Mrs. Meehan:

Enclosed is the subject Total-System Performance Assessment (TPA) code development lessons learned analysis. This document was prepared by the Center for Nuclear Waste Regulatory Analyses (CNWRA) to fulfill a commitment I made during the July 15, 1997, NRC Center Review Group (CRG) meeting to conduct the analysis and provide NRC with a copy of the results.

This analysis was prepared as part of the ongoing process of evaluating, monitoring, and taking remedial actions concerning problems that arose during development and distribution of TPA Version 3.0 and its successors. To avoid duplication of efforts and in an attempt to achieve a reasonably consistent understanding of what occurred and why, this analysis drew from the annual quality assurance audit of the CNWRA, work on Corrective Action Request 97-03 that was generated by that audit, the deliberations of a process improvement team that was formed to reexamine TOP-018 "Development and Control of Scientific and Engineering Software," the results of an independent analysis by a member of the SwRI Software Engineering Department, limited independent interviews of key CNWRA staff and management, consideration of the internal NRC lessons learned on this subject, and reviews of pertinent program documentation. For convenience, the reader may refer to section 2 of the enclosed analysis for a concise summary and conclusions of the investigation.

Please contact me if you have any questions regarding this important matter.

Sincerely yours,

Wesley C. Patrick
President

/bsc
cc: J. Greeves   T. McCartin   CNWRA Directors
       M. Federline   N. Eisenberg   CNWRA Element Managers
       J. Austin   J. Linehan   S. Mohanty
       M. Bell   S. Fortuna   R. Curtin, SwRI
       K. Stablein   B. Stiltenpole   S. Rowe, SwRI
       K. McConnell

**EVALUATION AND LESSONS LEARNED REGARDING
DEVELOPMENT OF THE TOTAL-SYSTEM PERFORMANCE ASSESSMENT CODE**
October 1997

1 INTRODUCTION

The purpose of this document is to provide a concise evaluation of the factors that led to the production and delivery of a computer code — the Total-System Performance Assessment (TPA) code, Version 3.0 — that did not meet the requirements of the U.S. Nuclear Regulatory Commission (NRC), who sponsored the work. The objectives of the evaluation and analysis are twofold: (i) identify the root causes of the problems that occurred and (ii) make recommendations regarding how to avoid recurrence of this and similar problems.

This document addresses both Corrective Action Request (CAR) 97-03, which was generated as a result of the Quality Assurance (QA) Audit 97-01, and broader management concerns regarding development and distribution of the TPA code that have been expressed in both written correspondence and numerous meetings between the NRC and the CNWRA.

2 SUMMARY AND CONCLUSIONS

The complexity of development of the TPA Version 3.0 code and its successors and the large number of people involved produced a full spectrum of perspectives regarding the problems that led to rejection of the code by the NRC. Taking into consideration all of those perspectives, this lessons learned was able to identify a series of recommendations that will both mitigate the current problem and minimize the likelihood of its recurrence. Implementation of many of these recommendations is already in progress and early success — particularly with regard to NRC staff participation and effectiveness of communications — is being observed.

Participation of NRC Staff in Development

- All NRC-funded code development should be undertaken as a joint effort of the NRC and CNWRA staffs.

Accuracy and Consistency of the Planning Process

- The scope of work for complex activities such as computer code development should be more clearly and completely defined prior to undertaking such activities.

- The schedules and budgets should be carefully reviewed and evaluated to ensure that they are consistent both with the defined scope of work and similar previous development activities.

- The CNWRA should be proactive in addressing potential inaccuracies and inconsistencies among scope, schedule, and budget.

Communication and Dissemination of Information

- A team approach should be followed, with the NRC and CNWRA staff and KTI leads being actively included in all aspects of future NRC-funded code development work, commencing with conceptualization and continuing through preproduction testing.

- Specific reviews by contractor and client staff and management should be conducted at appropriate points during SRD preparation, code development, and code modification.

- Available vehicles for enhancing communication should be more widely and effectively used.

- Special effort should be directed toward improving the environment within which communications and work are occurring.

- Quality Assurance Practices and Procedures

- The TOP-018 procedure should be revised to clearly establish that SRDs must be developed before any code development or modification work is initiated and to provide additional guidance on the level of detail required for SRDs.

- TOP-018 should require that SRDs be reviewed and approved by both CNWRA and client management prior to implementation, and revised, reviewed, and approved again if significant changes occur.

- The CNWRA management should reiterate the critical importance of internal reviews, and emphasize the need to stop delivery of a product if it does not meet CNWRA standards of quality and completeness.

3   BACKGROUND

Performance assessment (PA) is an analytical technique that is used within the high-level waste (HLW) program to evaluate whether the proposed repository will meet the regulatory requirements that have been established to ensure the protection of health and safety and the environment. Within the U.S. program, all interested parties have adopted some version of PA to quantitatively evaluate long-term repository performance. For the Department of Energy (DOE), PA is the basis for the "safety case" that they will make to demonstrate compliance with applicable NRC regulations and Environmental Protection Agency (EPA) standards. PA is also a central element of the DOE Viability Assessment (VA) that is scheduled to be completed in 1998. As the regulatory authority for HLW disposal, NRC will use PA to determine whether DOE has complied with the pertinent regulations. In the intervening years, PA assists NRC in identifying, assessing the relative importance of, and resolving at the staff level key technical issues (KTIs). PA also plays an important role in evaluating EPA proposals regarding an HLW standard and in developing the companion NRC implementing regulation. Utility groups [e.g., the Electric Power Research Institute (EPRI)], the State of Nevada, and other affected parties use PA techniques to independently evaluate the radiological health and safety and environmental effects of the proposed HLW repository.

Because of its central role throughout the repository program and its overarching relationship to all activities within the NRC HLW regulatory program, PA and the development of a capability to conduct PA are vitally important. Consequently, NRC began development of a PA methodology and associated computer codes about 15 years ago. Beginning in the late 1980s, NRC established a policy that NRC staff would be fully capable of conducting PAs to support prelicensing and licensing activities. Subsequently, NRC staff began playing a larger role in the development and use of the PA computer codes, in particular.

The first such endeavor took the form of a project dubbed "Iterative Performance Assessment, Phase 1" (IPA-1). This effort began shortly after the CNWRA was established but before PA staff had been acquired at the CNWRA. Consequently, the preponderance of the effort was conducted by NRC staff. IPA-1 was conducted using a set of computer codes that were previously developed by Sandia National Laboratory (SNL) and other contractor organizations, or were developed by NRC staff to meet the particular needs of the effort.

IPA-2 involved the staffs of the NRC Office of Nuclear Material Safety and Safeguards (NMSS) Division of Waste Management (DWM), the NRC Office of Nuclear Regulatory Research (RES) Division of Regulatory Applications (DRA), and the CNWRA. This collaborative effort (i) produced an integrated computer code known as the Total-system Performance Assessment code, Version 2.0 (TPA Version 2.0); (ii) developed a trained NRC and CNWRA staff team capable of conducting PA analyses; and (iii) documented the results of a trial assessment of repository performance that received wide distribution.

Code development associated with IPA-3, the most recent phase of the PA program, is the subject of this lessons learned analysis. Unlike its predecessor, IPA-3 was undertaken largely using the staff and resident skills of the CNWRA. Coordination was predominantly through a single point of contact [i.e., the NRC Program Element Manager (PEM) and the CNWRA Principal Investigator (PI)] during the planning process and the early stages of code development. A brief description of the code development activities was included in the CNWRA Operations Plan. Key dates related to planning and developing IPA-3 and the associated TPA Version 3.0 code are summarized in attachment 1.

4   INVESTIGATIVE METHOD

This analysis was prepared as part of the ongoing process of evaluating, monitoring, and taking remedial actions concerning problems that arose during development and distribution of TPA Version 3.0 and its successors. To avoid duplication of efforts and in an attempt to achieve a reasonably consistent understanding of what occurred and why, this analysis drew from several sources. These included (i) the annual QA Audit 97-01, (ii) work on CAR 97-03 that was generated by that audit, (iii) the deliberations of a process improvement team (PIT) that was formed to reexamine TOP-018 "Development and Control of Scientific and Engineering Software" in light of CARs 97-02 and 97-03, (iv) the results of an independent analysis by a member of the SwRI Software Engineering Department (SED), (v) limited independent interviews of key CNWRA staff and management, (vi) consideration of the internal NRC lessons learned on this subject, and (vii) reviews of program documentation.

Wherever available, written documents were used as primary information sources concerning the facts surrounding the development and delivery of TPA Version 3.0 and its successors. Much of the information, however, was obtained from discussions with various staff members, managers, auditors, and reviewers. Relatively little information was available in written form, and much of what was written was a transcription of anecdotal information and conversations. Consequently, substantiation of information was difficult, and memories of individuals were found to differ as to what was communicated and when it was communicated relative to key decision points. The relative sparsity of written communication and documentation of agreements is believed to have played a substantial role in the problems encountered.

The reader is referred to a number of related documents for additional details regarding the plans, discussions, critiques, and associated responses. Particularly germane are (i) CNWRA Operations Plan, Revision 8, Change 0; (ii) CNWRA Operations Plan, Revision 9, various changes; (iii) Software Requirements Description (SRD), January 28, 1997; (iv) the NRC Review of the SRD, February 18, 1997; (v) Concerns Regarding CNWRA Actions in Support of the Development of the TPA 3.0 Code, February 26, 1997; (v) the CNWRA response to this item, March 6, 1997; (vi) Non-Acceptance of Updated User's Guide for TPA Code, May 8, 1997; (vii) the CNWRA response to this item, May 22, 1997; and (viii) CNWRA Audit 97-1 Report, transmitted to NRC July 11, 1997.

3

5   ROOT CAUSE ANALYSIS

The investigative method outlined in section 4 was used to identify and analyze potential root causes for the problem. Three components of each root cause that was identified during the investigation stage are documented. First, observations of factual matters and perceptions of what went wrong and why are enumerated. These observations are based on interviewing staff members, inspecting pertinent project documentation, and reviewing the results of QA Audit 97-01. Second, implications with respect to product quality, timeliness, and the like are identified based on an interpretation of those observations. Because of the interrelationship between these first two items, they are discussed together in a single subsection within each root cause. Third, specific recommendations for preventing recurrence of the observed problem and/or mitigating its effects are made, as summarized in section 2.

The investigation and evaluation suggest that four root causes underlie the observed problem, although those interviewed named other more specific root causes that are treated as subsets of these four. The root causes are (i) failure to secure adequate participation of NRC staff in code development; (ii) lack of-accuracy and consistency in the planning process; (iii) inadequate communications and dissemination of information, including identifying and reporting problems; and (iv) deficiencies in quality assurance practices and procedures. Each of these root causes is discussed in the following sections.

5.1   Participation of NRC Staff in Development

It appears that the fundamental underlying problem is that CNWRA developed the TPA Version 3.0 code alone, without the benefit of NRC participation as was the case for IPA-2. Lack of NRC staff participation in code development had collateral effects on the planning process and communications, in particular, which are discussed in sections 5.2 and 5.3, respectively. The following discussion explores this root cause in its historical and programmatic context.

IPA-1 was conducted almost solely by the NRC staff, since the CNWRA had not yet staffed up in this technical area. While it was an important initial effort, the IPA-1 activity did not develop the integrated software and breadth of staff expertise that will be required for repository licensing.

In an effort to improve the effectiveness of the IPA effort, IPA-2 was undertaken as a joint collaborative effort with approximately equal numbers of staff from the NRC and CNWRA. Furthermore, a three-member management oversight board was established that comprised representatives of the NRC DWM, NRC DRA, and the CNWRA. Two team leads were selected from each of these three organizations to manage code development, testing, and operations, as well as production of a comprehensive report on the results of the work. TPA Version 2.0 was developed as part of this effort. This endeavor was widely judged to be a notable success.

Despite the success of IPA-2, the development and conduct of the IPA-3 program took a different approach. Following an extended period of planning that began shortly after IPA-2 was completed, Phase 3 code development was conducted with the CNWRA as the lead with only minor NRC staff involvement. It is noteworthy, however, that the CNWRA carried forward into Phase 3 TPA code development several lessons learned during IPA-2. These included (i) selection of an individual as PI for the TPA code modification effort who had an exceptionally high level of familiarity with TPA Version 2.0; (ii) adoption of the recommendations for code improvements noted in the IPA-2 final report, to the extent permitted by time and resources allocated to the effort; (iii) modification of the basic architecture of the code to make the code easier for a broad cross-section of NRC and CNWRA staff to use; and (iv) retention of the methodology for risk calculation in TPA Version 3.0.

For the first three months of FY97, CNWRA assumed the role of sole developer, consistent with allocated resources. As a result, the wealth of knowledge and experience developed during IPA-1 and IPA-2

were largely untapped by the CNWRA, and the broad base of support needed to modify the code and gain acceptance of TPA Version 3.0 was not developed. This approach also had the unintentional effect of excluding a number of senior staff from the process. The principal NRC participant during this time-frame was the PEM.

5.2 Accuracy and Consistency of the Planning Process

General planning for IPA-3 took place over an extended period, although essentially no code development work was done prior to FY97. The timetable for Congressional budget decisions delayed proper planning for the FY97 scope of work, including that related to TPA code development. Significantly, CNWRA operated without the benefit of a revised plan until December 27, 1996, three months after the beginning of the fiscal year and a little over one month after NRC first expressed concern regarding TPA development.

An examination of the planning process that accompanied TPA code development is enlightening. The CNWRA developed Revision 8, Change 0 of its Operations Plan for FY97 that was submitted July 26, 1996, and approved by NRC shortly thereafter. This plan called for modification of the TPA Version 2.0 code, but provided relatively little detail regarding what would be done and who would do it. The description stated that the planned activities would include (i) modifying the code to make it more representative of the YM setting and current repository design, (ii) formulating and developing improved abstractions and consequence modules, and (iii) modifying the outputs to match new regulatory requirements. While implying that a rather substantial revision of the code was planned at that time, the description did not state that a new architecture would be adopted for TPA Version 3.0. The completion date for the code modifications and user guide was established as August 29, 1997.

Following the budget cut, a complete replanning effort ensued. The former NRC PEM led this replanning effort, which included the CNWRA PI, EM, and Technical Director (TD), and involved meetings with the KTI leads. The revised Operations Plan (i) provided a much more complete description of the scope of code development, which implied an increased scope of work; (ii) redirected the overall TPA effort to focus on sensitivity analyses; (iii) maintained resources essentially unchanged relative to the July 26, 1996, Operations Plan; and (iv) accelerated the due date for completion of TPA Version 3.0 some 5-1/2 months to March 17, 1997. The description of the planned activities provided in Revision 9, Change 0 of the Operations Plan, which was issued December 30, 1996, states that "using the IPA Phase 2 version of TPA as a starting point, a new version of the code will be developed for use in the KTI sensitivity analyses." The phrase "new version" was used no less than three times in the brief one-paragraph description, seemingly leaving little doubt that a major revision was planned and, in fact, was well underway. The language in Operations Plan Revisions 8 and 9 notwithstanding, electronic mail records and recollections of agreements reached in meetings suggest a much more modest endeavor was to be undertaken. The NRC staff generally considers that the resources and schedule were appropriate for the modest changes they envisioned. This is discussed further in section 5.3.

This analysis concludes that the plan and schedule were fundamentally flawed from the outset in one or both of two ways. First, the scope of work was insufficiently defined in the operations plan to provide a clear, complete, and unambiguous determination of what was to be accomplished. Several NRC and CNWRA staff members agreed that neither a common expectation of what was required nor a uniform vision of how to fulfill that expectation was achieved. Some suggested that there was not a recognition of the extent of changes that were required to accommodate DOE revisions to the repository design and anticipated EPA revisions to the standard. Second, resources were inadequate for the scope of work that was executed. The CNWRA clearly undertook a task that was much larger than could be completed while maintaining its traditionally high quality standards. Furthermore, resources allocated to the NRC staff were insufficient for them to play a leadership role from conceptualization through evaluation of the code modifications.

5

The CNWRA did not obtain consensus on the scope of work, nor identify and seek to correct the perceived discrepancy among scope, schedule, and resource allocation. Three vehicles are readily available for notification of such concerns and implementation of associated changes: (i) Operations Plan modifications, although these plans tend to be general in nature; (ii) the Program Manager's Periodic Report (PMPR); and (iii) technical direction, which may be requested by the CNWRA or unilaterally provided by the NRC. None of these vehicles was effectively used to identify or address perceived inaccuracies and inconsistencies in the planning process.

5.3   Communication and Dissemination of Information

It is clear in retrospect that communications were inadequate throughout the TPA Version 3.0 planning and development phases. Most of those interviewed cited inadequate communications as the greatest contributor to the TPA code development problem. The levels, effectiveness, and, perhaps, frequency of communication were not adequate for a project of this complexity. Regular ongoing discussions were taking place, however, at the PEM/EM and PO/PI level throughout the course of planning and implementing TPA Version 3.0 code development. These discussions were expanded to include the CNWRA TD during the December 1996 to January 1997 timeframe. Early indications of differences in perspective regarding the approach to TPA code development should have been raised up the management chains within the organizations, but this was not done for a considerable time.

Correspondence from the director of DWM to the president of the CNWRA indicates that at least some at NRC believe the CNWRA has not been forthright in its communications with the NRC. An alternative perspective on the apparent lack of forthrightness that the NRC reported may be gained from considering that (i) communications among the key CNWRA and NRC staff were limited to relatively few individuals; (ii) changes in management and lead technical staff took place within both organizations during the critical time of Operations Plan modification, SRD preparation, and early TPA code development; (iii) the understanding of the CNWRA PI and EM regarding what code modifications were required continued to evolve throughout this period; and (iv) different meanings were ascribed to terms that were central to developing a clear understanding of what was and was not being done (e.g., "architecture").

Taking into consideration the information provided in the context of both of these perspectives, this lessons learned analysis was unable to determine conclusively whether information was being deliberately withheld from the NRC, or whether the apparent lack of forthrightness was simply a reflection of evolving understanding on the part of the CNWRA EM and staff. Elements of both perspectives were clearly evident in the interviews and were undoubtedly contributors to the communications problem.

An attempt was made to identify factors that contributed to the inadequacy and an apparent lack of openness in communications between the staffs. Several contributing factors were identified through the interview process. These included (i) a lack of a common vision regarding both the changes required to the TPA Version 2.0 code and the fundamental approach to be used in developing Version 3.0; (ii) a sense that there was a lack of acceptance of new and different ideas; (iii) an unwillingness to involve a broad and diverse range of staff in the process; (iv) beginning in early 1997, a tendency to rapidly elevate matters to senior management before the issue was worked at the staff or section leader level; (v) time constraints on both staff and management at the NRC and CNWRA that allowed relatively little time for thoughtful interaction, exploration of new ideas, and consideration of alternative views and approaches; and (vi) inadequate documentation of verbal agreements.

A final factor that should be considered is the overall role of the CNWRA management in the identification and communication of budding problems and solutions to such problems. The late determination of the budget, delays in the planning process, and the press of business may have resulted in a de facto "management by exception" approach at the CNWRA. In addition, senior CNWRA management took a position early in 1997 of lessening day-to-day involvement in TSPA activities to foster a stronger

working relationship at the EM-PEM level. Both of those actions played a role in (i) diminishing the effectiveness of communication within the CNWRA and with the NRC and (ii) allowing things to progress to where a significant problem developed before the full attention of management was brought to bear.

5.4 Quality Assurance Practices and Procedures

All scientific and engineering software that is obtained, modified, or developed by the CNWRA and is also intended to be used to conduct analyses in support of regulatory reviews is required to be under configuration control in accordance with TOP-018 "Development and Control of Scientific and Engineering Software." The controls implemented through TOP-018 include requirements for (i) a software requirements description, (ii) design and development, (iii) design verification, (iv) installation testing, (v) configuration control, (vi) software problem reporting and resolution, and (vii) software validation. The specific controls applied depend on the software category. Any particular item of software is assigned to one of three such categories: (i) developed or modified software, (ii) acquired or existing and not to be modified by the CNWRA, and (iii) acquired or existing and to be modified by the CNWRA. The development of the TPA Version 3.0 code that is the subject of this analysis falls within the first category.

Designation and transmission of "beta" versions of the code. The CNWRA transmitted variations of the TPA Version 3.0 code on March 14, April 4, and April 16, 1997, the last date being the official release date of the code. Although QA Audit 97-01 reported that these versions were transmitted without proper discrimination among versions, this does not appear to be true upon further investigation. The lead code developer has since confirmed that the code output files indicate distinct version numbers (e.g., 3.0 beta, 3.xxx, etc.). Correspondence used to transmit these early versions was not clear, however, regarding either the alphanumerical designation or state of development of the code. This led to confusion and, to at least some degree, a sense among the NRC staff that the CNWRA was misrepresenting the product that was delivered.

The QA audit also questioned whether the approach of providing a client with incomplete versions of a code was wise from a contractual perspective. The independent analysis by the SwRI SED evaluator raised similar questions, and recommended against the practice. It is the view of the CNWRA, however, that early transfers of codes are essential when the CNWRA and NRC are jointly developing a code. This approach was used successfully during IPA-2 and was also pursued in developing TPA Version 3.0, although the NRC staff was not involved until much later in the process.

CNWRA staff interviewed as part of this lessons learned indicated that evolving requirements (particularly during 1997) and late inputs from participants (some were received on the ship date) were significant contributors to the quality assurance aspect of the problem. Although considerable module testing was accomplished, testing of the integrated code was minimal. These comments have merit. In the broader context, however, the changes directed by NRC staff were required because of inadequacies in communications, insufficient definition and agreement regarding the scope of required code revisions, and significant shortcomings in the delivered code.

Review and decision to transmit code. Although each version of the TPA code was properly and uniquely identified, a key concern of the QA audit, none of the early versions of the code met NRC requirements and expectations. A proper technical and programmatic review of the code following QAP-002 "Review of CNWRA Documents, Reports, and Papers," performed against an appropriate standard of acceptability should have identified shortfalls relative to both technical adequacy and contractual requirements. A QA "stop work" on the transmittal would have prevented transmittal of the initial and, perhaps, subsequent beta versions of the code.

Early evaluations of the appropriateness for a stop work order identified two factors that suggested that a stop work order may not have been an appropriate action in this case. First, TOP-018 is not explicit

7

regarding distribution and use of beta versions. Second, the NRC had specifically directed transmittal of the code so that it would be available for early test and evaluation by the NRC staff. As this lessons learned evaluation progressed and additional information was developed, however, it became increasingly clear that a stop work (i.e., stop delivery) was an appropriate action to consider. Although differing staff perspectives regarding the expected state-of-development of the code transmitted March 14th persisted throughout this evaluation, written documentation clearly establishes that this milestone did not meet the contractual requirements.

Development and content of the SRD. Several problems have been identified with the SRD development process and the SRD content. Aspects of some of these problems were identified during the annual QA audit, while others were identified during this lessons learned analysis. Key points include (i) although several draft versions of the SRD were provided in late 1996, a final SRD was not transmitted until January 28, 1997; (ii) substantial work was done before the SRD was approved and approval occurred only one month before the code was delivered; (iii) a parallel approach to SRD and code development was pursued because of the stringent schedule; (iv) some saw ambiguity in the TOP-018 requirement that an SRD should be "prepared prior to significant development or modification of computer codes;" and (v) the level of detail of the SRD was insufficient to fully inform the NRC of the extensive nature of the changes to the code that were envisioned by the CNWRA.

The SwRI software quality assurance expert involved in QA Audit 97-1 made strong statements regarding the lack of recognition by the CNWRA staff that "they are members of a software development organization." In addition, he implied that an approach such as the Capability Maturity Model (CMM) of the Software Engineering Institute (SEI) could provide more timely and less expensive software development. The CNWRA management maintains that its staff develops software as tools for problem-solving and, consequently, are not software developers in the model of the SEI. Furthermore, the CMM requires particular management structures, procedures, and protocols that are markedly different from those in use at the NRC. Because joint CNWRA/NRC code development is the preferred paradigm, the suggested approach could not likely be implemented, since it would drive organizational changes at the NRC as well as at the CNWRA.

ATTACHMENT 1

Brief Chronology of Events in Planning and Developing TPA Version 3.0

03/94	CNWRA submitted a report on input to the IPA-3 plan.
11/95	Completed IPA-3 planning; plan submitted by NRC PEM for management approval prior to implementation.
7/96	CNWRA Operations Plan Revision 8, Change 0 submitted 7/26/96; delivery date for TPA Version 3.0 established as 8/29/97. NRC approved the plan 9/3/96.
10/96	Development of TPA Version 3.0 began.
11/96	CNWRA staff noted significant changes were being made in Phase 2 code to make it easier to use. NRC staff believed that the Phase 2 architecture was still being used and had some reservations about some of the changes.
12/96	CNWRA Operations Plan Revision 9, Change 0 submitted 12/30/96, incorporating significant revisions in the scope and description but not the resources allocated to TPA code development; delivery date for TPA Version 3.0 revised to 3/17/97. NRC approved the revised plan 1/31/97.
12/96	The NRC PEM and Project Officer (PO) were changed.
12/96-1/97	NRC staff expressed concern to CNWRA about not being informed of major changes to the code and noted the programmatic significance of the code.
1/97	In an HLW Board meeting, the CNWRA staff informed NRC that the Phase 2 architecture had been abandoned. NRC indicated that they were not aware of the decision to develop a different code architecture. CNWRA provided rationale for using a different architecture.
1/97	In another HLW Board meeting, senior NRC management noted that the HLW Board had agreed to use the Phase 2 architecture and that any changes to that architecture were to be brought to the Board.
1/97	The CNWRA formally transmitted a Software Requirements Description (SRD) to the NRC for comment (note that one or more drafts were previously provided to the NRC).
1/97	Partial "beta" version of code informally delivered to NRC. Major components of analysis were not included in this version (e.g., NEFTRAN).
2/97	NRC cautiously agreed to move forward with TPA Version 3.0 architecture rather than returning to the Phase 2 architecture. CNWRA and NRC staff were questioned by the HLW Board about whether the 3/17/97 delivery date for a code capable of doing sensitivity studies was achievable; CNWRA did not raise any objection to that date when an affirmative answer was given by NRC staff.
2/97	NRC staff discovered in testing the "beta" version of the code that the SNL Latin hypercube sampling (LHS) module had been replaced with a code of lesser capability.

This action had not been discussed with NRC staff and was judged to be in direct contradiction to previous agreements.

2/97	NRC staff accepted the TPA Version 3.0 SRD with the stipulation that the code to be delivered on 3/17/97 would be sufficient to conduct sensitivity analyses.
2/97	The DWM director sent a letter to the CNWRA president that noted concerns about the lack of CNWRA communication of major changes to the code. The letter specifically identified removal of the LHS module as an example.
3/97	The CNWRA president sent a letter to the DWM director that noted and took responsibility for problems in communication, but suggested that significant changes in management of the program may have been a contributing factor.
3/97	TPA Version 3.0 was received by NRC on 3/17/97. The transmittal letter noted that TPA Version 3.0 had been run and the results checked for reasonableness. It also noted the CNWRA intention to freeze the code after shakedown tests were completed. There was no indication in the transmittal that this was a "beta" version of the code.
3/97-4/97	NRC staff carried out an extended acceptance review of the TPA Version 3.0 code, including functionality testing. Staff found that the code (i) had major functionality problems that led to indefensible results, (ii) was not sufficiently developed to perform sensitivity studies, and (iii) had not been adequately tested and verified. NRC staff also questioned the adequacy of implementation of the QA procedure TOP-018 "Development and Control of Scientific and Engineering Software."
5/97	NRC staff rejected the TPA Version 3.0 code because it did not meet the requirements in the operations plan and the expectations laid out in the NRC acceptance review of the SRD.
5/97	CNWRA responded to non-acceptance of the code, suggesting that the 3/17/97 deliverable was a "beta test code," indicating that controls had been put in place to eliminate the root cause of problems, and agreeing to a delivery date for a functional code on 8/8/97.
6/97	The annual internal QA audit of the CNWRA found that TOP-018 was not effectively implemented in TPA Version 3.0 code development, and CAR 97-03 was issued.
7/97	NRC staff visited the CNWRA to assist in testing the revised code. A consensus developed that the code would not be ready for sensitivity studies on 8/8/97.
7/97	NRC staff briefed the NRC management on the status of the code and noted that it believed a functional code could be available by 9/8/97.
7/97	In a document titled "Actions and Agreements for Completion of Total-System Performance Assessment Code", it was agreed that CNWRA would supply a functional TPA Version 3.1 code on 9/8/97 with a limited user's manual. Full testing and verification will be completed by 3/98 to support VA review activities.

7-8/97   CNWRA transmitted evolving beta versions of the TPA code for testing by NRC and CNWRA staff; ongoing code verification and associated modifications were conducted under TOP-018 using Software Problem Change Requests (SPCRs) to document changes.

9/8/97   Delivered the TPA Version 3.1 code to NRC, together with sufficient instructions to load and execute the code.

H\PATR\ASSMNT\LSSNLRNS TPA

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

October 21, 1997

0135 64 OCT 27

Dr. Robert G. Baca
Performance Assessment Element Manager
Center for Nuclear Waste Regulatory Analyses
6220 Culebra Road, Bldg. 189
San Antonio, Texas 78238-5166

SUBJECT CO⋯⋯
PROJECT NO.⋯

css (20-5705-761)

Dear Dr. Baca:

SUBJECT: ACCEPTANCE OF TPA VERSION 3.1 COMPUTER CODE (IM 5708-762-730)

On September 5, 1997, the CNWRA submitted the total system performance assessment code (TPA Version 3.1) as partial fulfillment of Intermediate Milestone (IM) 5708-762-730 (Updated User's Guide for TPA Code) which had been previously submitted and not accepted by the NRC staff. This is to inform you that we have tested and evaluated the TPA Version 3.1 code and find it acceptable to perform the process-level sensitivity studies and, therefore, consider it to be an acceptable deliverable based on the specifications in the CNWRA Operations Plan. This acceptance of the TPA Version 3.1 code is considered partial acceptance of IM 5708-762-730 because full acceptance of the IM must await submission of the User's Guide that accompanies the code. The User's Guide is now expected to be delivered to the NRC on December 12, 1997.

CNWRA staff within the Total System Performance Assessment and Integration Element are to be commended for their dedication and strenuous efforts in producing what we now believe is a code that provides NRC with considerable flexibility and significantly improves upon preexisting computational tools. Although continued testing of the TPA Version 3.1 code during the sensitivity studies could result in the identification of changes that need to be made to the code, this is considered part of the normal "debugging" associated with code verification.

I believe that the TPA Version 3.1 code reflects the excellent team effort that has taken place between NRC and CNWRA staff over the past 5 months. We should both strive to ensure that working relationships between NRC and CNWRA staff continue to improve. If you have any questions, please contact me at (301) 415-7289.

Sincerely,

Keith I. McConnell, Element Manager
Total System Performance Assessment and
  Integration KTI
Division of Waste Management
Office of Nuclear Material Safety
  and Safeguards

cc: W. Patrick
Directors
EMV
Ottakanta
Ron Janetzke

cc: J. Linehan, PMDA
B. Meehan, CMB1/ADM

DATE: September 23, 1997

TO: W. Patrick, B. Sagar, B. Mabrito

FROM: *PCL*   M. Ahola, P. Lichtner (Chairman), S. Mohanty, W. Murphy, and J. Stamatakos

SUBJECT: TOP-018 Revision Committee Recommendations

NOTE: Following Travel overseas by P. Lichtner, a meeting was held with W. Patrick, B. Sagar, P. Lichtner, B. Mabrito on 10/14/97 To discuss This memorandum and determine best next steps To change TOP-018.

P. Lichtner and Process Improvement Team will Take Action re TOP-018.

[signature] 10/14/97

Consensus was reached regarding recommended changes to TOP-018, Development and Control of Scientific and Engineering Software. These recommended changes are based on the results of the CNWRA internal audit described in Audit Report 97-1. Specifically, the audit report recommended that a team comprised of code developers and users should be established to better define TOP-018 requirements. The committee also took into consideration the contents of the letter to H. Garcia from S. Fortuna dated July 8, 1997 on the subject: Approval of CNWRA TOP-018, Revision 5. In this letter Ms. Fortuna recommended that the technical staff should assume "ownership" of TOP-018 to ensure effective implementation of the procedure. The recommended changes to TOP-018 follow the comments offered by S. Dellenback regarding Division 20 software development procedures in his memo dated August 10, 1997 to W. Patrick and R. Curtin.

Dellenback emphasized the need for a Software Development Plan (SDP) in addition to the Software Requirements Description (SRD) already required by TOP-018. In addition, he noted the need for an Acceptance Test Plan (ATP) not currently called for in TOP-018. The purpose of the ATP is to demonstrate to the client that the code development outlined in the SRD and SOW has in fact been fulfilled.

Dellenback raised 5 specific issues:

(i) Tailored software development procedures need to be identified for each software development project in a project-specific SDP.

(ii) Software requirements must be more thoroughly documented in the SRD and formally reviewed with the customer.

(iii) More documented testing needs to occur which should be formally documented in an ATP.

(iv) Quality of source code is inconsistent and does not adhere to generally accepted software engineering practices.

(v) Non-Computer Science trained staff are developing and delivering software.

Each of these items was addressed by the committee. The committee's recommendations are discussed below.

(i) The committee agreed that preparation of a SDP should be included in TOP-018. Dellenback noted that:

> *It is very difficult to write a single set of software development procedures with any substance that can logically apply to all software development projects. Each software project needs to tailor TOP-018 to best fit the requirements of the program.*

The committee felt that this was especially true of the CNWRA where a great variety of codes are being developed (TPA, MULTIFLO, 3DSTRESS, ...) or modified (VTOUGH/CTOUGH, EQ3/6, ...). Each code has a different purpose and different level of visibility with clients. The TPA code has input from many individuals both at the CNWRA and the NRC and a multitude of users. As such it requires special considerations to document changes in the code and to coordinate new releases to the users. MULTIFLO currently is being developed by two individuals, P. Lichtner and a consultant (M. Seth) and does not have the same level of visibility as does the TPA code. However, MULTIFLO is also being marketed in WFO and may have other requirements.

TOP-018 would be altered to provide general guidelines for developing a SDP. The SDP would provide an interface to TOP-018 for each code being developed or alteration of an existing code. The purpose of the SDP is to interpret how TOP-018 will be applied to a particular code. Future audits would need only refer to the relevant SDP, rather than TOP-018 itself. Each code developer would need approval from his/her element manager, QA, and the software development board to implement the SDP. The SDP appeared to be the most flexible approach to meet the needs of the CNWRA, where codes with widely varying requirements are being developed. The SDP would detail specifically for each code being developed at the CNWRA:

- style guideline

- configuration management

- code baselining

- changes to baseline

- change requests

- issuance of new releases

- Acceptance Test Plan (ATP)

Those parts of TOP-018 that refer to detailed requirements, such as preparation of an SPCR form, would be deleted as this function would be provided by the SDP tailored to each code's particular needs. Other suggestions made by Dellenback, such as the ATP, would be optional and would also be detailed in the SDP, rather than in TOP-018. Other recommendations were to include Cook et al. as an appendix to TOP-018 so that a copy is easy for the developer to locate.

(ii) The committee agreed that the SRD requirement as currently implemented in TOP-018 was adequate, but that the length of the SRD should not be restricted arbitrarily, but decided by the developer and project manager. In addition the committee agreed that the SRD should become an intermediate milestone and reviewed by the client (NRC) for appropriateness and buyoff.

(iii) In its present form TOP-018 does not call for an ATP document. Testing of code is documented in the developers scientific notebook. The committee felt that a formal ATP could be useful in certain instances to demonstrate to the client that what was stated in the SRD was actually carried out.

(iv) The committee agreed that style guidelines should be spelled out in the SDP and adhered to during code development and subsequent modifications. The tendency has been to consider code

2

"good enough" if it works. However, a recurring issue at the CNWRA has been code reusability and clean code could certainly help in this regard. As noted by Dellenback (private communication to P. Lichtner), however, writing "good" FORTRAN code seems to be a virtually impossible task. Object oriented programming languages have been specifically developed to deal with the issue of code reusability, but such languages in their present state of development may not be appropriate for number crunching codes such as MULTIFLO.

(v) The committee felt that this item was a management decision and fell outside the scope of TOP-018. It was agreed that CNWRA staff are primarily concerned with producing results useful for analyzing specific problems such as disposal of nuclear waste at Yucca Mountain. Codes are generally viewed as a means to an end and not an end in itself. Considerations of budget and time must be addressed as well because hiring a professional software developer would be expected to greatly increase the cost of software development and could prolong the time to complete coding.

The committee's next step, if management gives approval for the direction outlined in this memo, would be to modify TOP-018 in accordance with the suggested changes presented above. Much of TOP-018 can be left intact. Sections 5.4 Design and Development, 5.5 Design Verification, 5.6 Installation Testing, 5.7 Configuration Control, 5.8 Software Problem Reporting and Resolution, and 5.9 Software Validation, would be modified and/or replaced by guidelines for producing the SDP including optional development of an ATP. The SPCR form would be eliminated and replaced by guidelines for implementing change control as detailed in the SDP. The committee feels that implementing the plan to improve TOP-018 as outlined in this memo would provide a flexible approach to computer code management and would improve the quality of software developed at the CNWRA.

3

August 10, 1997

MEMORANDUM

TO: Wes Patrick
            Rich Curtin

FROM: Steve Dellenback $\mathcal{S}\mathcal{L}\mathcal{U}\mathcal{D}$

SUBJECT: Division 20 Software Development

I have had the opportunity to discuss Division 20 software development procedures with various personnel within Division 20. Additionally, I have been provided a variety of documents and source code to review. My primary contacts have been Peter Lichtner and Sitakanta Mohanty.

A summary of my insights would include:

- Software Development Procedures: Division 20 utilizes a document entitled "Development and Control of Scientific and Engineering Software" (aka TOP-018). This document provides an overview of how software should be developed within the Center. While this document presents some good concepts, the concepts need to be applied in a different fashion to different programs (i.e. the document is not a "cure all" for all projects). It is very difficult to write a single set of software development procedures with any substance that can logically apply to all software development projects. Each software project needs to tailor TOP-018 to best fit the requirements of the program.

  By contrast, the Software Engineering Department (SED) has a set of software development procedures that is currently several hundred pages long. These procedures are based on the Software Engineering Institute's (SEI) Capability Maturity Model (CMM). The goal of these procedures is to provide "development guidelines" and "best practices" which can be tailored to individual project requirements. The practice of having a set of software development procedures at an organizational level, which is tailored to specific project needs, is common in the industry today. The software development procedures are typically tailored via two mechanisms, tailoring guidelines (which are normally part of the procedures themselves) and a project specific Software Development Plan (SDP). Tailoring guidelines describe what must be done as well as what may be modified with suggestions as to "why" the tailoring might occur. It is controlled adaptation based on specific project needs and constraints. The

SDP details which parts of the software development procedures will be utilized and how they will be used.

One of the major issues that were identified during my review/discussions is that there was no consensus as to how "change control" should be implemented. While change needs to be carefully controlled to minimize "requirements creep" (which can impact cost and schedule), it is important to have a "change control" process that does not overwhelm the project. Generally accepted software engineering practices implement formal (i.e. written forms) "change control" once a product is delivered to the customer (termed the "baseline"). If modifications need to be made to the baseline, formal "engineering change request (ECR)" forms must be generated to document and track the changes. The number of changes that can be incorporated into a single ECR varies based on the development program requirements (the change control process is detailed in the SDP).

Issue: Specific software development procedures need to be identified for each software development project in a project specific SDP. This document needs to describe responsibility guidelines and provide significant detail on rules, practices, and conventions that will be applied on the project. This document should also describe how "change control" will be implemented.

Recommendation: Develop "tailoring" guidelines to accompany TOP-018 to specifically "customize" each software development effort. For significant development efforts, consider developing a document similar to a SDP; for small development efforts or software maintenance efforts, a "blanket tailoring guideline" should be developed.

Change control needs to be better defined. Because Division 20 has a variety of software development programs (in the sense that development activities widely vary), there needs to be more than one way to handle change control. The selected method for each project needs to be completely documented in the project SDP.

• Software Requirements Document: From a SwRI software development perspective, I believe the most important document that we produce is the Software Requirements Document (SRD). Although design documentation is important, from a contractual relationship with our customers, the SRD is the "defining" document for what SwRI is to perform. According to the software engineering literature, the most prominent cause of problems during software development projects is "mis-set" expectations, that is, the customer expects one product and the developer provides another. The SRD is a mechanism, which can formalize "what", the software is to do. In SED, we develop a significant amount of the contents of the SRD during the proposal stage (we have to in order to determine project costs). I realize Division 20 has a relatively unique contracting relationship but more effort needs to be spent on requirements.

Once the SRD is complete (this document could vary in size from very short for a simple project, to quite lengthy for a large, complex project), the contents of the SRD

Memorandum
August 10, 1997
Page 3.

need to be formally reviewed with the customer. Written customer feedback and/or concurrence with the SRD should be received from the customer. Once the SRD is approved, any requested changes must be formally submitted and considered for cost and schedule impacts. Note that even a well-written SRD will have "gray areas". There are always TBDs. Requirements may not be fully known until the project is complete. The software process needs to flag and monitor these TBDs to assure that the development is a controlled effort and not a chaotic effort. Processing of TBDs and change requests should be done in written correspondence (we use e-mail for this in many cases).

It should be noted that a complete and well-written SRD does not assure that no "issues" will arise with the customer. It does provide a "framework of expectations" which is important to be documented in the event that one of the project principles (either the customer or SwRI key team members) leaves the project.

Issue: Software requirements must be more thoroughly documented and formally reviewed with customer.

Recommendation: Initiate the development of a "classical" Software Requirements Document (SRD) whose "length" is not arbitrarily limited. Once the customer accepts the SRD, any change in requirements must be formally tracked using a well-documented procedure.

- Testing: At the heart of almost all "software problems" is a lack of testing. There are many reasons for this lack of testing, the most common is the lack of time. Software Engineering journals suggest that approximately 30% of the software development time should be spent "writing code". The balance of the time is in requirements, design, documentation and testing. Quality testing starts at well-defined requirements (see SRD above). In order to test, you have to fully understand what you are testing for. While "ad hoc" testing will identify problems, it should not be considered formal testing. Three levels of testing should occur on ANY software delivered to a customer:

  - Unit Testing: Testing performed by the developer at the "module" level to thoroughly exercise the "structure" of the code and to assure that individual subroutines/functions generate expected results. The unit tests themselves, as well as the results of the unit testing should be informally documented (hand written tests/results are acceptable).

  - Integration Testing: Combining "modules" to assure that an operational system has been put together. Integration test cases, as well as the results of the integration testing should be documented (the level of documentation depends on the complexity of the system being developed).

  - Acceptance Testing: The process of getting the customer's concurrence that the requirements (detailed in the SRD) have been successfully implemented. The

Acceptance Test Plan (ATP) needs to be a formal document that the customer reviews and approves prior to acceptance testing being initiated. The ATP should ONLY include tests to demonstrate that the requirements (detailed in the SRD) have been implemented. Failures during acceptance testing should be formally documented and corrective action needs to be detailed. At the conclusion of the acceptance test, the customer should "buy-off" the system.

Issue: More documented testing needs to occur.

Recommendation: Develop formal ATP procedures for ANY software to be delivered to a customer.

Software Implementation: It is my observation that the Institute's technical Divisions closely review reports/letters that are sent to our clients. We assure that these reports/letters adhere to standards that the Division has established. I spent time reviewing the software that has been produced; while some of the code was well documented and meets generally accepted software engineering practices, a vast majority of the code (over 75%) needs significant modification to make the source code "consistent" and "maintainable". I was not reviewing the code to see "if it works", rather I was reviewing the "style" of the code and trying to assess the "maintainability" (by either SwRI staff or the client's staff). While the "science" behind the software developed by Division 20 is complex, the style of implementation makes the code very difficult for anyone other than the author to modify. If we are delivering source code to a customer, software standards must be established and we must assure that software developed meets the same high standards we have established for SwRI generated reports/letters.

Issue: Quality of source code is inconsistent and does not adhere to generally accepted software engineering practices.

Recommendation: A "software style guideline" should be developed and all software delivered to the client should be reviewed by an independent reviewer to assure compliance with the style guideline. TOP-018 does reference guidelines but each project needs to select a style project specific guideline and adherence to the guideline should be independently evaluated.

- Computer Science Trained Staff: I realize that this is a sensitive issue but SwRI needs to assure that we are delivering quality software products. I realize that much of the software that is developed in Division 20 is done by scientists who understand the underlying problems they are trying to implement and trying to convey this information to a "programmer" would not be a feasible solution. There needs to be a "line" established in which there is a distinction made between software that is developed as a "tool" (and used internally to solve problems) and software that is a "product" (that is used by the client on a repetitive basis to solve problems).

Memorandum
August 10, 1997
Page 5.

I believe that a clear distinction can be drawn between the two types of software. There are many people who can "program" but the art of developing and delivering production quality source code is not a simple matter. If software is being used by SwRI employees to produce results that SwRI personnel are interpreting, we can be more lenient on the quality of the code (because anomalies in the code should be caught internally). However, in the cases where we are delivering code for customer execution (and validation of significant events), we should probably utilize more "formally trained" software professionals to assure that the software meets expected Institute quality standards. Another case that should be considered is the case of software that produces data that will be delivered, as a product, to a customer. In this case, software quality is also a significant issue since the customer may be making critical decisions based upon the data SwRI delivers, and the customer will expect that the data to be accurate.

As an analogy, if I need to connect two SwRI computers together, I might make my own cable (which will be functional but not "pretty"). If I am to deliver the cable to a customer, I will either purchase a commercially made cable or I will utilize a SwRI technician (who is trained in cable making) to make the cable. The Division 20 staff is clearly highly skilled in their technologies but Computer Science is a lot more than "programming".

Issue: Non-Computer Science trained staff are developing and delivering software.

Recommendation: Consider utilizing more Computer Science trained staff in the software development process or at least consider having a Computer Science trained staff member on the weekly/monthly review of all software development projects. Note that several members of the QA Department are trained in both Computer Science and QA so a single person may be able to fill several roles. If Computer Science personnel are not used on a full-time basis; consideration should be given to establishing a structured code walk-thourgh process (using trained software staff). This would provide independent insight into the software being developed and would more than likely greatly improve the delivered product.

Corrective action to improve the above areas will not be easily performed in several weeks; however, I do believe more rigorous testing could be accomplished before the August delivery of source code to the NRC. I hope that my insights prove to be helpful. If anyone within Division 20 wishes to further discuss my comments, please have them call me at the SwRI TransGuide offices at 737-2983.

cc: Susan B. Crumrine
        Peter Lichtner
        Sitakanta Mohanty

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

013420 JUL 14 ?

July 8, 1997

SUBJECT ....
PROJECT NO ....

Mr. Henry F. Garcia
Director of Administration
Center for Nuclear Waste Regulatory Analysis
6220 Culebra Road
PO Drawer 28510
San Antonio, Texas   78228-0510

SUBJECT: Approval of Center for Nuclear Waste Regulatory
           Analyses Technical Operating Procedure-018, Revision 5

Dear Mr. Garcia:

We have reviewed the subject technical operating procedure (TOP)
and have the following comments. The revision has accurately
incorporated the changes requested to revision 4, change 0, in my
May 11, 1995, letter to you. I have discussed the deletion of
the "Software Control Board" with Bruce Mabrito. It has been
agreed that we will closely monitor the new process, which relies
more heavily on the Director of Quality Assurance, to ensure it
will be as effective or more effective than use of the Board.

The changes which have been made in this revision are considered
acceptable. However, as you are aware, problems with the Total
System Performance Assessment (TPA) Software Development which
occurred during the last evaluation period were primarily due to
lack of effective implementation of TOP-018. This conclusion was
supported by the results of the CNWRA's internal audit and the
corrective action requests which resulted from that audit. For
this reason, it has been agreed that TOP-018 will be thoroughly
reviewed by CNWRA technical staff and the Quality Assurance
Director and revised, as appropriate, based on their recent
experience in code development. Further, to ensure effective
implementation of the procedure, the technical staff should
assume "ownership" of this technical procedure.

As part of the review consideration should be given to submission
of software requirements descriptions (SRDs) as intermediate
milestones which will be approved by NRC prior to the beginning
of code development. The level of detail to be included in the
SRDs, as well as when a modification to the design is significant
enough to require a revised SRD should also be evaluated and
agreed too by the Center Quality Assurance Director and the NRC
CNWRA Operations Program Element Manager and included in the
revised procedures.

The following editorial changes should also be included in the
next revision.

Center for Nuclear Waste Regulatory Analyses

6220 CULEBRA ROAD • P.O. DRAWER 28510 • SAN ANTONIO, TEXAS, U.S.A. 78228-0510
(210) 522-5160 • FAX (210) 522-5155

47a

May 1, 1998
Contract No. NRC-02-97-009
Account No. 20-1402-159

U.S. Nuclear Regulatory Commission
Attn: Ms. Deborah A. DeMarco
Office of Nuclear Material Safety and Safeguards
Program Management, Policy Development and Analysis Staff
Mail Stop 8-A23
Washington, DC 20555

Subject: Transmittal of Technical Operating Procedure (TOP)-018, Development
            and Control of Scientific and Engineering Software for NRC Review
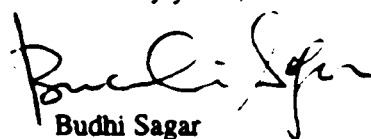   (AI-20-1402-159-801)

Dear Ms. DeMarco:

Enclosed is the Center for Nuclear Waste Regulatory Analyses (CNWRA) TOP-018, Revision 6. This
CNWRA operating procedure addresses the NRC comments of March 24, 1998. The changes requested
in the referenced correspondence have been made resulting in an improved procedure.

This deliverable is being carried in the Commitment Control Log as Administrative Item 20-1402-159-
801. After staff training with the revised TOP-018, the Quality Assurance Corrective Action Request No.
97-02 will be completed. We thank you for your assistance in revising TOP-018, which is important for
both our organizations.

Please contact me at (210) 522-5252 or Peter C. Lichtner at (210) 522-6084 if you have any questions.

Sincerely yours,

Budhi Sagar
Technical Director

HFG/lg
Enclosures
cc: B. Meehan   J. Thoma   P. Lichtner
      J. Linehan   K. McConnell   S. Boyanowski (SwRI Contracts)
      B. Stiltenpole   T. McCartin
      M. Federline   W. Patrick
      J. Greeves   CNWRA Directors/Element Managers
      K. Stablein

TOP-018 DEVELOPMENT AND CONTROL OF SCIENTIFIC ENGINEERING SOFTWARE
Revision 6, Change 0

CONTROLLED COPIES:

Theodore Carter, NMSS
Barbara Meehan, Contracts
Barbara Stiltenpole, NMSS & (20) Uncontrolled copies
Deborah DeMarco, NMSS
Rose Burn, NMSS
Christiana Lui, NMSS
Tim McCartin, NMSS
Keith McConnell, NMSS

UNCONTROLLED COPIES:

DCS
Tae Ahn, NMSS
Mike Bell, NMSS
John Bradbury, NMSS
David Brooks, NMSS
Kien Chang, NMSS
Richard Codell, NMSS
Neil Coleman, NMSS
Norm Eisenberg, NMSS
Margaret Federline, NMSS
Kim Gruss, NMSS
Philip Justus, NMSS
Bret Leslie, NMSS
Mysore Nataraja, NMSS
Jeff Pohle, NMSS
N. King Stablein, NMSS
John Thoma, NMSS
John Trapp, NMSS
Sandra Wastler, NMSS
Rick Weller, NMSS