

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-96SR18500 with the U. S. Department of Energy.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Progress in Addressing DNFSB Recommendation 2002-1 Issues: Improving Accident Analysis Software Applications (U)

Kevin R. O’Kula
Washington Safety Management Solutions LLC
P. O. Box 5388, Aiken, SC 29804-5388;
Phone: 803.502.9620
Email: kevin.okula@wsms.com

Richard (Chip) H. Lagdon, Jr.
Acting, Chief of Nuclear Safety
U.S. Department of Energy
1000 Independence Ave., S.W.
Washington, D.C. 20585-0270
Phone: 301.903.4218/202.586.9174
Email: chip.lagdon@eh.doe.gov

Abstract

Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1 (*Quality Assurance for Safety-Related Software*) identified a number of quality assurance issues on the use of software in Department of Energy (DOE) facilities for analyzing hazards, and designing and operating controls to prevent or mitigate potential accidents. Over the last year, DOE has begun several processes and programs as part of the Implementation Plan commitments, and in particular, has made significant progress in addressing several sets of issues particularly important in the application of software for performing hazard and accident analysis. The work discussed here demonstrates that through these actions, Software Quality Assurance (SQA) guidance and software tools are available that can be used to improve resulting safety analysis. Specifically, five of the primary actions corresponding to the commitments made in the Implementation Plan to Recommendation 2002-1 are identified and discussed in this paper. Included are the web-based DOE SQA Knowledge Portal and the Central Registry, guidance and gap analysis reports, electronic bulletin board and discussion forum, and a DOE safety software guide. These SQA products can benefit DOE safety contractors in the development of hazard and accident analysis by precluding inappropriate software applications and utilizing best practices when incorporating software results to safety basis documentation.

The improvement actions discussed here mark a beginning to establishing stronger, standard-compliant programs, practices, and processes in SQA among safety software users, managers, and reviewers throughout the DOE Complex. Additional effort is needed, however, particularly in: (1) processes to add new software applications to the DOE Safety Software Toolbox; (2) improving the effectiveness of software issue communication; and (3) promoting a safety software quality assurance culture.

Introduction

Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1 (*Quality Assurance for Safety-Related Software*) identified a number of quality assurance issues on the use of software in Department of Energy (DOE) facilities to analyze and guide safety –related decisions, the quality of software applied to design or develop safety-related controls, and the proficiency of personnel using the software.¹ DOE accepted the DNFSB Recommendation in November 2002, and developed an Implementation Plan in the ensuing months to address the key areas of concern.² The Implementation Plan includes:

- Identification, documentation and communication of roles, responsibilities and authorities for software quality assurance (SQA)
- Identification of federal personnel that have responsibility related to safety software
- An assessment of safety system software to determine its current status and an assessment of the effectiveness of SQA programs for safety analysis and safety design software
- Identification of a set of safety analysis “toolbox” codes that are commonly used in the DOE complex, the upgrade of those codes to a prescribed qualification, and the establishment of a Central Registry to facilitate maintenance, technical support, configuration management, training, and notification to users of problems and revisions to these codes
- Identification and development of requirements and guidance for safety SQA based on existing industry or federal standards, and
- A continuous improvement process that includes the identification of SQA experts across the DOE Complex who will provide input to management regarding SQA programs.

A set of twenty-six commitments are described in the DOE Implementation Plan (IP) for resolving the Recommendation issues. Of these commitments, several have particular significance to safety analysis contractors for supporting safety basis documentation. The deliverables meeting these specific commitments have been recently developed for use throughout the DOE Complex, and can greatly improve software quality critical for sound, technically robust hazard, accident, and consequence decision-making. They include:

- (1) Establish and implement a Central Registry for the long-term maintenance and control of the safety analysis “toolbox” codes (Commitment 4.2.2);
- (2) Perform a gap analysis of the toolbox codes to determine the actions needed to bring the code into compliance with the SQA qualification criteria, and develop a schedule with milestones to upgrade each code based on the gap analysis results (Commitment 4.2.1.3);
- (3) Issue code-specific guidance reports on use of the “toolbox” codes identifying applicable regimes in accident analysis, default inputs, and special conditions for use (Commitment 4.2.1.4);
- (4) Identify methods for capturing and clearly communicating SQA lessons learned, new technology, innovative techniques, and areas in software development in which research and development is needed to ensure software quality (Commitment 4.4.2); and
- (5) Establish a schedule to develop, revise, approve, and issue SQA directives (Commitments 4.3.2.1 and 4.3.2.2).

The remainder of this paper discusses the five specific deliverables that support this set of commitments.

SQA Tool Development

Specific products/processes that were completed or begun in the past year are the DOE Central Registry, gap analyses and guidance reports for designated toolbox software, web-based sharing of information, and safety software guidance. These products are directly applicable to safety analysts and the application of software in support of safety basis documentation. All products are available through the (DOE SQA Knowledge Portal - <http://www.eh.doe.gov/sqa/>).

1. DOE Central Registry

The cornerstone to the completion of an appreciable portion of the IP commitments has the development and completion of a web-based DOE/EH SQA Knowledge Portal. The DOE/EH Knowledge Portal was started in mid-2004 with the purpose of promoting continuous improvement and the sharing of knowledge of safety software quality assurance among interested parties across the DOE Complex. It consolidates information and contains links to subject matter experts, procedures, training material, program descriptions, good practices, lessons learned and the Central Registry of Toolbox Codes. The Portal also provides capabilities for member collaboration in product development and threaded discussions. It is found at (http://www.eh.doe.gov/sqa/central_registry.htm). A portion of the screen image upon addressing the Knowledge Portal is shown in Figure 1.

As noted above, an information link available from the Knowledge Portal is the Central Registry. The Central Registry provides information about Department of Energy (DOE) toolbox codes. The toolbox codes are, in principle, a small number of standard computer codes having widespread application. The Codes are routinely used by DOE to perform calculations and develop data used to establish the safety basis for DOE facilities and operations, and to support the variety of safety analyses and safety evaluations developed for these facilities.

The Central Registry assists users in configuration control and serves as a point of contact for resolving user issues. To date, six codes have been identified as toolbox codes: ALOHA, CFAST, EPIcode, GENII, MACCS2, and MELCOR. A general description of each code is provided along with the respective code owner. Code-specific guidance reports have been issued identifying applicable regimes in accident analysis, default inputs, and special conditions for using each of the six toolbox codes. In addition, a gap analysis was performed on each toolbox code to determine the actions needed to bring the code into compliance with SQA criteria. However, code owners are responsible for ensuring that the codes are maintained in accordance with established requirements. The Office of Quality Assurance Programs (EH-31) works closely with the code owners to ensure that adequate technical support and training are available.

The screenshot shows the homepage of the Software Quality Assurance Knowledge Portal. The header includes the U.S. Department of Energy logo and the text 'ENVIRONMENT, SAFETY AND HEALTH'. Navigation links include 'HOME', 'Department of Energy', 'Site Map', 'Search ES&H', 'Security and Privacy Notices', and 'Disclaimer'. A left sidebar contains links for 'About Us', 'ES&H Program/Topics', 'ES&H Corporate Reporting Databases', and 'Resources/Tools'. A central banner features a photo of three workers and the title 'Software Quality Assurance Knowledge Portal'. The main content area welcomes visitors and describes the portal's purpose: to promote continuous improvement and knowledge sharing of safety software quality assurance. It lists key features: 'Central Registry' (a library of DOE 'Toolbox' Codes), 'Site Assessments and CRADS' (product development and threaded discussions), and 'Hot Topics' (Accident Type A and B Investigations, Electrical Safety Campaign). A right sidebar lists 'Latest News' (OE Summary 2005-06, OE Summary 2005-05) and 'Events' (2005 Pollution Prevention Workshop). A bottom sidebar lists 'Software Quality Assurance Home' and various resources like 'Central Registry', 'CRADS', 'Discussion Forum', 'SQA Directives', 'SQA Library', and 'SQA Links'.

Figure 1. The Knowledge Portal is the cornerstone of SQA Information network (found at <http://www.eh.doe.gov/sqa/>).

While DOE is listing the toolbox codes for information in the Central Registry, most of them were developed outside of DOE (e.g., in the private sector or other Federal agencies), and access to these codes or their use may be subject to agreements, conditions and restrictions established by the code owners or Federal agencies. In most cases, the most current versions accepted for use by DOE are listed in the Registry, although other versions may be in use or available in archives or from code owners.

2. Gap Analyses for the DOE Toolbox Software

Safety analysis software for the DOE “toolbox” was designated by DOE/EH in March 2003.³ Software for toolbox status, and its version and area of applicability are listed in Table 1. Discussion of SQA deficiencies and the actions required to upgrade designated toolbox software (ALOHA, CFAST, EPIcode, GENII, MACCS2 and MELCOR) into compliance with NQA-1 and other consensus software standards are documented in six individual reports. The reports provide safety contractors with a programmatic understanding of the SQA pedigree of toolbox software.

Table 1. Software Designated for DOE Safety Analysis Toolbox

Code	Version or Revision	Area of Applicability
ALOHA	5.2.3	Chemical Release/Dispersion and Consequence
CFAST	3.1.6	Fire Analysis
EPIcode	6.0	Chemical Release/Dispersion and Consequence
GENII	1.485 and 2.0	Radiological Dispersion and Consequence
MACCS2	1.12	Radiological Dispersion and Consequence
MELCOR	1.8.5	Leak Path Factor

The Implementation Plan for Recommendation 2002-1 recognized that the designated toolbox software, while widely used in the DOE Complex for safety analysis applications, have uncertain SQA pedigree. The Implementation Plan contains commitment 4.2.1.2 to address this situation:

- A plan for evaluating the SQA characteristics of the programs, procedures, and practices for the designated safety-related toolbox codes
- The requisite criteria for evaluating the SQA adequacy of the DOE toolbox safety analysis computer codes.

Each of these six codes and their respective development programs was evaluated on their SQA attributes relative to present-day, documented software quality standards and is termed a SQA evaluation, or gap analysis. The SQA evaluation assessed those measures requiring action, i.e., areas of improvement, before the individual codes meet current SQA-compliant standards. Primary criteria and implementing criteria were identified on which to base the individual gap analyses.

An over-arching framework of primary criteria to conduct assessments was established early in the SQA evaluation program for the designated toolbox software. The primary criteria are those in the Quality Assurance rule, Subpart A to 10 CFR 830.⁴ Subpart A establishes quality assurance requirements for DOE contractors conducting activities including providing items or services, that affect, or may affect, the nuclear safety of DOE nuclear facilities. Section 830.121 describes a requisite quality assurance program (QAP) its applicability, frequency of updates, and directs the contractor to describe how criteria (Section 830.122) are met. It also specifies integration with the Safety Management System and recommends use of voluntary consensus standards.

While several national and international sets of software quality assurance partially meet the needs of assuring software quality in the nuclear sector and provide guidance to following the

Quality Assurance rule, it is concluded that the ASME NQA-1-2000⁵ requirements best address safety analysis software and cover the full spectrum of needs for this type of software. NQA-1 is referenced in 10 CFR 830 Subpart A, and it provides guidance for complying with Nuclear Safety requirements. It incorporates the basic criteria from 10 CFR 50, Appendix B,⁶ 10 CFR 830 Subpart A and references key criteria from Institute of Electronics and Electrical Engineers (IEEE) standards. A major theme to changes in NQA-1 has been protecting the health and safety of the public while performing work that meets requirements. This goal is consistent with nuclear safety directives and guidance from the Department of Energy, including DOE-STD-3009-94⁷ and other “safe harbor” methodologies listed in Table 2 in Subpart B to 10 CFR 830. In summary, 10 CFR 830 Subpart A, and the NQA-1-2000, Subpart 2.7 and related Part I requirements, primarily Requirements 3 (*Design Control/Section 800 Software Design Control*) and 11 (*Test Control/Section 400 Computer Program Test Procedures*), were the primary set of SQA criteria for the evaluation of safety-related computer software.

Requirements from NQA-1-2000 are not met directly, but require implementing procedures with sufficient detail to guide appropriate actions for each computer code. The implementing procedures for meeting NQA-1-level requirements from the Savannah River Site (SRS), Sandia National Laboratories (SNL), and the Yucca Mountain Project (YMP) were reviewed as part of the SQA Implementation Plan project for application in the evaluation methodology. While the final procedural basis discussed is a merged set composed of procedures from these sources, it primarily draws upon procedures from SRS.

Detailed gap analysis then proceeded based on an evaluation of each of the six designated computer codes. The requirement and specific documents to help determine compliance are listed in Table 2.

Table 2. SQA Topical Area and Corresponding Documentation for Demonstrating Compliance

<u>Requirement No.</u>	<u>SQA Requirement</u>	<u>SQA Document</u>
1	Software Classification	-
2	SQA Procedures/Plans	SQA Plan
3	Requirements Phase	Software Requirements Document
4	Design Phase	Software Design Document
5	Implementation Phase	3, 4, 6
6	Testing Phase	Test Case Description and Report
7	User Instructions	User’s Manual
8	Acceptance Test	User Instructions
9	Configuration Control	Software Configuration and Control Document
10	Error Notification.	Error Notification and Corrective Action Report
11	Training and Qualification of Users	Training Package and User Qualification

Figure 2 is a schematic of the process followed in the gap analysis for each of the designated toolbox codes.

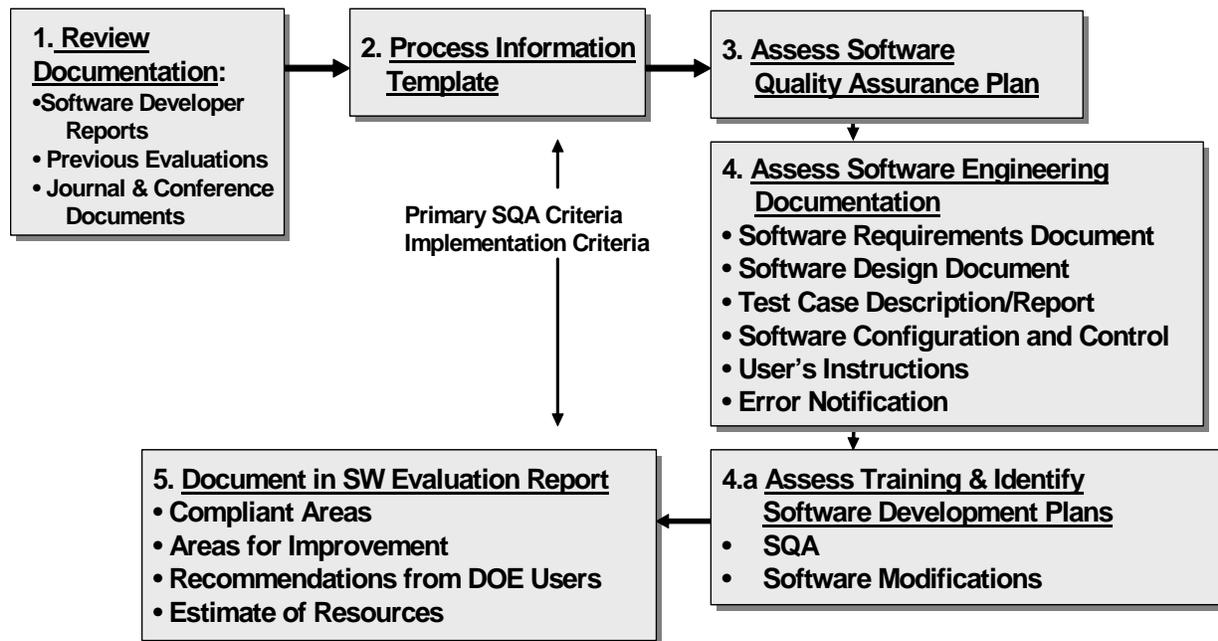


Figure 2. Gap analysis process followed for designated toolbox codes.

Evaluations and preparation of draft documentation for review took place from October 2003 through May 2004. Of the six codes evaluated, only one fully met the majority of the eleven SQA requirements. The other five were found to meet most requirements at best “partially” or and many were in the “not at all” category. Nevertheless, while this outcome is not satisfactory, it did not suggest that existing safety analysis supported by this software is non-conservative. It does indicate however, that remedial steps should be taken to better document past and current SQA development and maintenance processes, establish the software baseline, and improve software user/owner/sponsor communications.

Final gap analysis documentation was prepared and posted at the Central Registry link during the May - June 2004 time frame. Copies can be reviewed at the Central Registry website (http://www.eh.doe.gov/sqa/central_registry.htm).

3. Guidance Reports for the Designated Toolbox Software

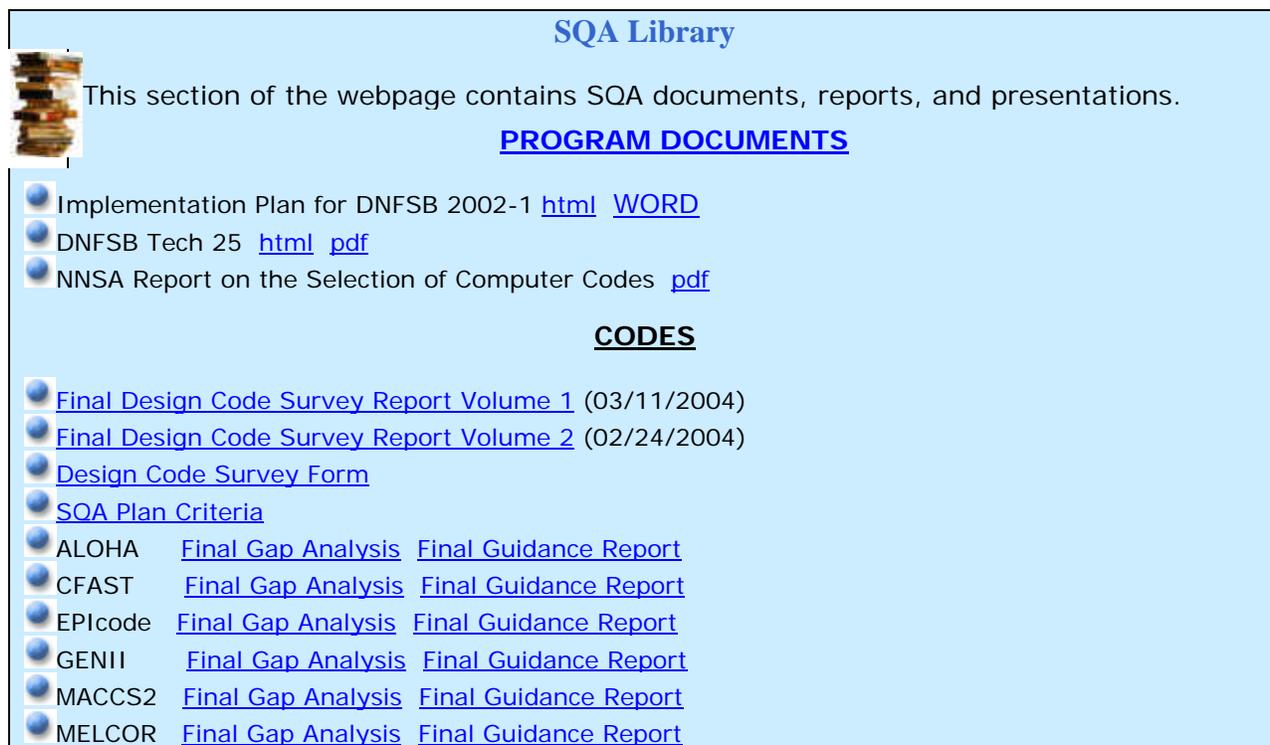
The toolbox software will require completion of quality assurance improvement measures before meeting current SQA standards. In some cases, technical model modifications are strongly suggested. In the interim period before these changes are completed, the six software applications are still considered useful assets in the support of safety basis calculations. To ensure appropriate application of the designated toolbox software, the Implementation Plan has committed to sponsoring a set of code-specific documents to guide informed use of the software,

and supplement, rather than replace, the available user's manual information. The guidance reports include the following:

- Applicability information for DSA-type analysis, specifically tailored for DOE safety analysis
- Code development information and SQA background
- Appropriate regimes and code limitations
- Valid ranges of input parameters consistent with code capability and DOE safety basis applications
- Default input value recommendations for site-independent parameters, and
- Examples of code applications for specific accident sequence analysis.

These reports will guide DOE analysts in the qualified use of these toolbox codes to support safety analysis consistent with 10 CFR 830, Subpart B Safety Basis Documentation. It is expected that due to an extended, prioritized schedule for improvement of the designated toolbox codes, that many of the code guidance reports may need to be updated to remain both consistent with latest improvements to the SQA of the software and version changes.

Final code guidance documentation was prepared and posted at the Central Registry link in June and July, 2004. Copies can be obtained at the Central Registry website (http://www.eh.doe.gov/sqa/doc_library.htm). A partial listing of the available documentation in the virtual SQA Library, including the final guidance reports (ALOHA, CFAST, EPIcode, GENII, MACCS2, and MELCOR) is shown in Figure 3.



The screenshot shows a webpage titled "SQA Library" with a light blue background. On the left, there is a small image of a stack of books. The main text reads: "This section of the webpage contains SQA documents, reports, and presentations." Below this, there are two sections: "PROGRAM DOCUMENTS" and "CODES".

SQA Library

This section of the webpage contains SQA documents, reports, and presentations.

PROGRAM DOCUMENTS

- Implementation Plan for DNFSB 2002-1 [html](#) [WORD](#)
- DNFSB Tech 25 [html](#) [pdf](#)
- NNSA Report on the Selection of Computer Codes [pdf](#)

CODES

- [Final Design Code Survey Report Volume 1](#) (03/11/2004)
- [Final Design Code Survey Report Volume 2](#) (02/24/2004)
- [Design Code Survey Form](#)
- [SQA Plan Criteria](#)
- ALOHA [Final Gap Analysis](#) [Final Guidance Report](#)
- CFAST [Final Gap Analysis](#) [Final Guidance Report](#)
- EPIcode [Final Gap Analysis](#) [Final Guidance Report](#)
- GENII [Final Gap Analysis](#) [Final Guidance Report](#)
- MACCS2 [Final Gap Analysis](#) [Final Guidance Report](#)
- MELCOR [Final Gap Analysis](#) [Final Guidance Report](#)

Figure 3. Partial listing of documentation from SQA Library.

4. Web-Based Sharing of SQA Information

A communication capability has been established recently, including an internet web-based discussion forum and a sharing information/lessons learned site. Both are accessible through the SQA Knowledge Portal.

The SQA Discussion Forum provides a virtual workspace for end users to post information regarding SQA including general issues, toolbox code usage, and lessons learned. The SQA Discussion Forum link is <http://www.eh.doe.gov/sqa/discussionforum.htm>).

The lessons learned feature of the SQA Knowledge Portal is established to promote the sharing of knowledge across the DOE complex with specific emphasis on lessons learned relevant to SQA. The sharing of lessons learned can potentially reduce risk, improve efficiency, and enhance the cost effectiveness of DOE processes and operations. This is a feedback mechanism for the Quality Assurance community to use and promote continuous improvement in the application of SQA.

Sites have been asked to provide lessons learned from safety software assessments as well as recent experience from implementing other SQA requirements for posting. Initial examples that have been contributed include:

- [Insights from 2004 Safety SQA Assessments at DOE Hanford, January 2005](#)
- [British Nuclear Fuels Fissile Tracking System at the Advanced Mixed Waste Treatment Facility \(DOE-ID\) Special Report, October 2004](#)
- [Idaho Operations Office Assessment Best Practices, May 2004](#)

The link also notifies DOE and DOE contractors on SQA training. For example, EH sponsors Software Quality Engineer Courses offered by the American Society for Quality (ASQ). This type of training allows attendees to satisfy several of the competency requirements in the Safety Software Quality Assurance Functional Area Qualification Standard.⁸

The Sharing Information and Lessons Learned link is found at http://www.eh.doe.gov/sqa/lessons_learned.htm.

5. Safety Software Guide

A final illustration of the progress made in the past year in addressing Recommendation 2002-1 is specific SQA guidance. DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance* provides the safety analysis professional with information and acceptable methods useful for implementing the safety SQA requirements of the Order, DOE O 414.1C, *Quality Assurance*.

The guide provides information and acceptable methods for implementing the SQA requirements of DOE O 414.1C. DOE O 414.1C requirements supplement the quality assurance program (QAP) requirements of Title 10 Code of Federal Regulations (CFR) 830, Subpart A, Quality Assurance, for DOE nuclear facilities and activities. The safety SQA requirements for DOE, including the National Nuclear Security Administration (NNSA), and its contractors are necessary to implement effective quality assurance (QA) processes and achieve safe nuclear facility operations.

DOE promulgated the safety software requirements and this guidance to control or eliminate the hazards and associated postulated accidents posed by nuclear operations, including radiological operations. Safety software failures or unintended output can lead to unexpected system or equipment failures and undue risks to the DOE/NNSA mission, the environment, the public and the workers. Thus DOE G 414.1-4 has been developed to provide guidance on establishing and implementing effective QA processes tied specifically to nuclear facility safety software applications. DOE also has guidance¹ for the overarching QA program, which includes safety software within its scope. This Guide includes software application practices covered by appropriate national and international consensus standards and various processes currently in use at DOE facilities. This guidance is also considered to be of sufficient rigor and depth to ensure acceptable reliability of safety software at DOE nuclear facilities.

The guide is intended to be used by organizations to help determine and support the steps necessary to address possible design or functional implementation deficiencies that might exist and to reduce operational hazards-related risks to an acceptable level. Attributes such as the facility life-cycle stage and the hazardous nature of each facility's operations should be considered when using this Guide. Another objective of the guide is to encourage robust software quality methods to enable the development of high quality safety applications.

The guide and the order are scheduled to be available by May 2005. Upon issuance, copies may be downloaded from <http://www.directives.doe.gov>. A preliminary version of the table of contents of the document is shown in Table 3.

¹DOE G 414.1-2, *Quality Assurance Management System Guide for use with 10 CFR 830.120 and DOE O 414.1*, dated 6-17-99.

Table 3. DOE Safety Software Guide (Near-Final Outline)**1. INTRODUCTION**

- 1.1 Purpose
- 1.2 Scope
- 1.3 Responsibility for Safety Software
- 1.4 Safety Software Quality Assurance
- 1.5 Software Quality Assurance Program

2. SAFETY SOFTWARE TYPES AND GRADING

- 2.1 Software Types
- 2.2 Graded Application

3. GENERAL INFORMATION

- 3.1 System Quality and Safety Software
- 3.2 Risk and Safety Software
- 3.3 Special-Purpose Software Applications
 - 3.3.1 Toolbox and Toolbox-Equivalent Software Applications
 - 3.3.2 Existing Safety Software Applications
- 3.4 Continuous Improvement, Measurement, and Metrics
- 3.5 Use of National/International Standards

4. RECOMMENDED PROCESS**5. GUIDANCE**

- 5.1 Software Safety Design Methods
- 5.2 Software Work Activities
 - 5.2.1 Software Project Management and Quality Planning
 - 5.2.2 Software Risk Management
 - 5.2.3 Software Configuration Management
 - 5.2.4 Procurement and Supplier Management
 - 5.2.5 Software Requirements Identification and Management
 - 5.2.6 Software Design and Implementation
 - 5.2.7 Software Safety
 - 5.2.8 Verification and Validation
 - 5.2.9 Problem Reporting and Corrective Action
 - 5.2.10 Training Personnel in the Design, Development, Use, and Evaluation of Safety Software

6. ASSESSMENT AND OVERSIGHT

- 6.1 General
- 6.2 DOE and Contractor Assessment
- 6.3 DOE Independent Oversight

APPENDICES AND REFERENCES

Case Studies

Two examples are given below of recent use of the Central Registry in support of the DOE safety analysis process.

Chemical Dispersion Code Algorithm Impact

One of the primary improvements with the availability of the Central Registry and its categories of information is timely communication of Complex-wide SQA issues, and improving subsequent resolution. An example of the change brought about by the availability of the DOE SQA Knowledge Portal and the links discussed here is in disseminating information on an algorithm modification in chemical dispersion software in one of the designated toolbox codes, i.e., a new liquid evaporation model used in EPIcode.

As noted previously, DOE/EH issued the final guidance reports in mid-2004 for the six designated toolbox codes used in conducting calculations to support Safety Analysis. Section 2.0 of the EPIcode (Version 7) guidance report described a revision that was made to the code based on EPA guidance for Offsite Consequence Analysis (EPA-550-B-99-009).⁹ The change models evaporation from liquid spill scenarios by a factor of 2.68 higher relative to older EPIcode version results. The EPA-550-B-99-009 model is intended to provide a conservative estimate for evaporative spills for screening purposes. A concern was raised whether there was an impact to sites that used previous versions of EPIcode as part of their Accident Analysis, Emergency Action Levels or Emergency Planning Hazard Assessments.

The new communication links made available through the Central Registry and the SQA Knowledge Portal allowed quick dissemination of the issue in July 2004. Through this and other communication mechanisms, including the Energy Facility Contractors Group (EFCOG), safety contractors became aware of the EPIcode change and the need to review potential impacts in their safety basis documentation. In particular, sites were asked to answer the following:

1. Could this change result in a non-conservative impact with respect to your DSA? Is this a significant change in the effects of liquid evaporation cases that would really matter to the safety analysis? Would the new information (increase by factor of 2.68 in evaporation rate) impact the safety decisions made at your facility?
2. Were your users notified of the EPIcode changes? (If so, how?).
3. What have your EPIcode users done? Were safety analyses reviewed to update appropriate documentation? Did the results change and if so how?
4. What version of EPIcode are you presently using?

The results of the EPIcode review found that by late September, only one DOE site potentially had facilities that were affected. Upon review of the situation, the site took the appropriate compensatory actions to disposition the issue.

While it could be argued that notification, review, and disposition phases of the EPIcode non-conservatism issue would have been the same regardless of Knowledge Portal, discussion forum, and the Central Registry availability, it is equally valid to recognize that the process was expedited. Had the Central Registry infrastructure not been established, the overall process would have been inefficient, uncertain, and easily longer in duration.

Safety Analyst and Software Developer Use of the Central Registry

As a second example, it is estimated that Central Registry documentation access has averaged several “hits” per day among DOE safety analysts since guidance reports have been released. Most of the use has to:

- Become aware of software versions, improvements, and new capabilities
- Understanding appropriate domain applications and technical limitations
- Access examples to base site-specific applications.

Several of the designated toolbox software developers have utilized the Central Registry, Discussion Forum, and other features of the DOE/EH web site to expand contact with DOE code users, and in supporting priority setting. Prior to the establishment of the Central Registry, many of developers had little if any contact with the DOE user community. It is now recognized as a key “constituency” group that justifies frequent and timely developer-user contact.

What’s Past is Prologue: SQA Improvement Program

As part of the Implementation Plan to Recommendation 2002-1, DOE/EH has initiated several processes to improve safety SQA practices, procedures, and programs among its contractors in the DOE Complex. The activities that are underway address several sets of issues particularly important in the application of software for performing hazard and accident analysis. Particularly noteworthy are the web-based DOE SQA Knowledge Portal and its Central Registry, guidance and gap analysis reports, electronic bulletin board and discussion forum, and a DOE safety software guide. These SQA products can benefit DOE safety contractors in the development of hazard and accident analysis by promoting appropriate software applications for the tasks in question, and especially when incorporating software results to safety basis documentation.

While software development, maintenance and application should be standardized and applied consistently with DOE O 414.1C (*Quality Assurance*) and the DOE G 414.1-4 (*Safety Software Guide*), the areas outlined in this paper mark only a beginning. The limited successes achieved in communications on SQA issues, providing software developer feedback, and improving user guidance, then are preface to subsequent actions and decisions are likely to be required in the near term. Included are:

1. **Adding new software to the DOE Safety Software Toolbox** – New software applications and new versions of currently designated toolbox software should be examined in a standard manner for adding to the DOE Toolbox. Processes to submit and to evaluate software have been introduced, but will need testing to confirm readiness for the types of application that are anticipated. Draft procedures for standardizing and managing this process will be tested in the near future.
2. **Increasing the effectiveness of software issue communications** – The example cited earlier on changes to a chemical dispersion code demonstrated the usefulness of the new website and the Central Registry. Although the initial notice, communication, and actions by the safety contractors took place on the order of weeks, the overall process can be streamlined. A more centralized system, able to alert all potentially affected sites within hours should be the goal. Nonetheless, the initial “posting” and dispositioning of the

software issue was a good exercise in establishing an effective communication infrastructure.

To better notify users on software issues, DOE/EH is working on concepts to make more transparent the locations at which specific software is applied. A system such as this, presumably integrated with the Central Registry, would allow near-immediate contact to be made with sites and contractors on code-specific issues.

3. **Instilling and furthering a safety software quality assurance culture** – Recognition of SQA processes and their value in DOE safety software applications has been improved among developers, analysts, users, and reviewers. However, for the most part, the designated toolbox codes have no ties to DOE support and their developers are not formally required to execute their development programs under stronger SQA procedures described by the Safety Software Guide in support of the DOE O 414.1C (*Quality Assurance*). Additional planning is needed to encourage more cooperation on the part of software developers even when there is no contractual obligation.

In parallel with this cultural step change on the part of the developer is a similar need affecting software users and their management. Users should ensure that if a designated toolbox code is not applied, that they select software that has achieved at least the minimum required SQA credentials and that it is suited for the intended application. The user of any selected software is encouraged to understand the limitations and capabilities, use appropriate inputs and qualified data, and consult the Central Registry for current information. The managers of software users should establish sound training programs (Work Practice #10 in the Safety Software Guide) to preclude occurrences of incomplete and faulty software applications.

Acknowledgements

The authors are indebted to comments and recommendations from those throughout the DOE Complex towards improvements of SQA practices in general, and the Knowledge Portal/Central Registry, in particular. We especially wish to thank Bob Quirk and Chip Martin of the Defense Nuclear Facilities Safety Board staff, and Bud Danielson, Tony Eng, Pranab Guha, Shiv Seth, Debra Sparkman, and Charlie Thayer of DOE.

References

1. Defense Nuclear Facilities Safety Board, *Recommendation 2002-1, Quality Assurance for Safety-Related Software*, (September 2002).
2. U.S. Department of Energy, *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1: Quality Assurance for Safety Software at Department of Energy Nuclear Facilities*, Report, (March 13, 2003).
3. U.S. Department of Energy Office of Environment, Safety and Health, *Designation of Initial Safety Analysis Toolbox Codes*, Letter, (March 28, 2003).
4. Code of Federal Regulations (CFR). 10 CFR 830, Nuclear Safety Management Rule.
5. American Society of Mechanical Engineers, ASME NQA-1-2000, *Quality Assurance Requirements for Nuclear Facility Applications*.
6. 10 CFR 50, Appendix B, *Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants*.
7. U.S. Department of Energy, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Reports*, DOE-STD-3009-94, Change Notice 2 (April 2002).
8. U.S. Department of Energy, *Safety Software Quality Assurance Function Area Qualification Standard*, DOE-STD-1172-2003, (December 2003).
9. U.S. Environmental Protection Agency, *Risk Management Program Guidance for Offsite Consequence Analysis*, U.S. EPA, Chemical Emergency Preparedness and Prevention Office, EPA-550-B-99-009. (April 1999).