**DEFENSE NUCLEAR FACILITIES
SAFETY BOARD**

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004-2901
(202) 694-7000

00-0000022

January 20, 2000

The Honorable T. J. Glauthier
Deputy Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Mr. Glauthier:

Software quality assurance (SQA) is a process for the systematic development, testing, documentation, maintenance, and execution of software. The staff of the Defense Nuclear Facilities Safety Board (Board) has reviewed the status of SQA for software used to make safety-related design decisions and to control safety-related systems. The enclosed report, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities,* identifies deficiencies in SQA for both types of software. The report also describes problems with code execution resulting from a lack of guidance and training. The Board believes these problems are symptomatic of underlying deficiencies in the infrastructure supporting SQA at the Department of Energy (DOE), and they have a direct debilitating effect on safety activities in DOE.

The Board has been informed by its staff that the Quality Assurance Working Group within DOE has been aware of some of these issues since February, but that little progress has been made toward addressing these problems because no senior DOE leader has actively accepted responsibility for the function of SQA. The Board believes this to be precisely the type of important cross-cutting safety issue that could be resolved through actions by the DOE Safety Council.

Accordingly, pursuant to 42 U.S.C. § 2286b(d) the Board requests a report from DOE within 60 days of receipt of this letter that describes the actions that are needed to address the deficiencies and potential improvements identified in the enclosed report and the schedule for completing these actions.

If you have any questions on this matter, please do not hesitate to call me.

Sincerely,

John T. Conway
Chairman

c: Mr. Mark B. Whitaker, Jr.

Enclosure

00.22

DNFSB/TECH-25

QUALITY ASSURANCE FOR SAFETY-RELATED SOFTWARE AT DEPARTMENT OF ENERGY DEFENSE NUCLEAR FACILITIES

Defense Nuclear Facilities Safety Board

Technical Report

January 2000

QUALITY ASSURANCE FOR SAFETY-RELATED SOFTWARE AT DEPARTMENT OF ENERGY DEFENSE NUCLEAR FACILITIES

This report was prepared for the Defense Nuclear Facilities Safety Board by the following staff members:

Thomas Burns
Matthew Forsbacka
Charles R. Martin

with assistance from:

Farid Bamdad
Wallace Kornack
Joseph Roarty
Albert G. Jordan
William Yeniscavich

EXECUTIVE SUMMARY

The Department of Energy (DOE) relies upon numerous computer codes and associated control system software for safe operation of its facilities. Yet there is no adequate oversight mechanism or comprehensive set of standards in place for ensuring that the quality of software is in place. Software quality assurance (SQA) provides measures designed to ensure that computer software will perform its intended functions in a consistent and reliable manner and that software modifications will not result in unanticipated problems. As such, SQA is an essential part of the systematic development, testing, documentation, maintenance, and use of software. Because DOE depends on computer analysis embodying this software to ensure the safety of many of its operations, SQA is a necessary element of an overall safety program.

Deficiencies in computer software used in support of both safety analyses and machine control at DOE sites have been identified. Instances of inadequacies in the fundamental physical models encoded in the computer software for safety analyses have also been noted. In addition, there have been problems with implementation and use of software codes resulting from a lack of guidance and training of safety analysts on the use of codes for performing safety analyses. These problems are symptomatic of underlying deficiencies in DOE's quality assurance program for software and its supporting infrastructure.

Although there are many industry standards for SQA, DOE has not formally promulgated guidance that clearly defines which of those requirements are appropriate for use by its contractors. In addition, DOE has not developed an infrastructure capable of ensuring appropriate levels of training for analysts, or providing oversight and enforcement with regard to software widely used for authorization basis calculations. The staff of the Defense Nuclear Facilities Safety Board believes the evaluation documented in this report highlights the need for DOE to take steps to correct these deficiencies. To this end, the report proposes improvements in DOE's SQA infrastructure and provides specific suggestions for improving the quality of the software codes for both instrumentation and control and of accident analysis.

TABLE OF CONTENTS

Section Page

1 INTRODUCTION 1-1

2 RELATIONSHIP BETWEEN INTEGRATED SAFETY MANAGEMENT AND SOFTWARE QUALITY ASSURANCE 2-1

3 CURRENT STATUS OF SOFTWARE QUALITY ASSURANCE IN THE DOE NUCLEAR COMPLEX 3-1

3.1 Gaps in DOE's Infrastructure 3-1
3.1.1 Roles and Responsibilities of DOE Headquarters 3-2
3.1.2 DOE Office of Defense Programs Activities 3-2
3.1.3 Activities of DOE Albuquerque Operations Office 3-3
3.2 Examples of Issues With Accident Analysis Codes 3-5
3.2.1 MACCS2 Code 3-5
3.2.2 Other Codes of Interest 3-7
3.3 Examples of Issues With Instrumentation and Control Software 3-7
3.3.1 Los Alamos Critical Experiments Facility 3-8
3.3.2 Programmable Logic Controller: Various Incidents 3-9
3.4 Other Issues 3-10

4 POTENTIAL DOE IMPROVEMENTS IN SOFTWARE QUALITY ASSURANCE 4-1

4.1 Potential Improvements in DOE Software Quality Assurance Infrastructure 4-1
4.2 Potential Improvements to Software Quality Assurance for Instrumentation and Control Systems 4-2
4.3 Potential Improvements for Software Quality Assurance Associated with Accident Analyses 4-3

5 CONCLUSION 5-1

APPENDIX A A-1

REFERENCES R-1

GLOSSARY OF ACRONYMS AND TERMS GL-1

1. INTRODUCTION

The Department of Energy (DOE) and its contractors perform hazardous work necessary for national security and for restoration of the environment at former defense nuclear production facilities. The performance of this work is of paramount importance to our national interests, and it is equally important that this work be accomplished in a safe manner whereby the public, workers, and the environment are protected. A key and necessary tool adopted by DOE to accomplish this goal is Integrated Safety Management (ISM), which is simply a system designed to ensure that provisions for safety are fully integrated into planning and execution of work. Among the basic functions of ISM is the analysis of hazards entailed in performing work and the identification of controls to prevent adverse consequences.

Given the consequences of a major accident during the performance of many types of hazardous work, DOE has the significant responsibility of thoroughly investigating all pathways to an accident-initiating event and developing controls to prevent or mitigate such occurrences. Computer codes and their associated models and data are critical tools in fulfilling this important responsibility. Confidence in the adequacy of hazard analyses and the associated controls relies heavily on the integrity of such computational tools. Given the prominent role played by computer codes in ensuring the safe operation of DOE facilities, it is imperative that a thorough and effective approach to guaranteeing their quality be implemented. This is the goal of software quality assurance (SQA).

SQA provides measures designed to ensure that computer software will perform its intended functions in a consistent manner and that software modifications will not result in unanticipated problems. Such measures must be applied during the systematic development, testing, documentation, and execution of such software, and be maintained throughout the life cycle of safety-related computer software. Furthermore, an effective SQA program ensures that:

- The code numerical models are a valid representation of the physical phenomena of interest for the appropriate variables and within a defined applicable range (verification).

- The fundamental data used in the code are accurate.

- The results obtained when using the code within its established range of applicability are in reasonable agreement with available experimental benchmark data (validation).

- Codes are properly executed by safety analysts.

- Subsequent modifications and improvements of the codes be tracked and documented in a central registry so that users will be aware of the physical and mathematical assumptions and limitations of their analysis.

Although there are many adequate industry standards for SQA, DOE has not promulgated guidance that clearly defines those necessary for safety applications. Absent such guidance, some computer codes are not reviewed for the level of quality expected for operations at high-hazard facilities. In addition, DOE has not developed a formal program for training its contractors' analysts who implement SQA requirements or federal employees who perform safety oversight.

Specific deficiencies in software used in support of both safety analyses and machine control at DOE sites have been identified by both DOE and its contractors. Inadequacies in the fundamental physical models encoded in the computer software for safety analyses have also been noted. In addition, there have been problems with the use of codes in the performance of safety analyses because of the lack of guidance and training of safety analysts. These problems, which are symptomatic of underlying deficiencies in the infrastructure supporting software quality at DOE, are detailed in this report. Section 2 reviews the linkages among ISM, SQA, and the safety of defense nuclear facilities. Section 3 examines the current status of SQA in the DOE complex. In Section 4, the staff of the Defense Nuclear Facilities Safety Board (Board) proposes improvements in SQA. Conclusions are presented in Section 5.

2. RELATIONSHIP BETWEEN INTEGRATED SAFETY MANAGEMENT AND SOFTWARE QUALITY ASSURANCE

On October 11, 1995, the Board issued Recommendation 95-2, *Safety Management*, (Defense Nuclear Facilities Safety Board, 1995) which recommended that DOE restructure its safety management program to provide a more effective and integrated way of discharging its responsibilities for protecting the public, workers, and the environment. In support of this recommendation, the Board issued DNFSB/TECH-16, *Integrated Safety Management* (DiNunno, 1997), which sets forth a vision of what integrated safety management could offer. One of the guiding principles of ISM is the identification of safety standards and requirements. Before work is performed, the associated hazards must be evaluated, and an agreed-upon set of safety standards and requirements must be established that, if properly implemented, will provide adequate assurance that the public, workers, and the environment will be protected from adverse consequences.

Another concept important to safe operation of defense nuclear facilities is the authorization basis, as specified in DNFSB/TECH-5, *Fundamentals for Understanding Standards-Based Safety Management of Department of Energy Defense Nuclear Facilities,* (DiNunno, 1995). The authorization basis defines those aspects of the facility design basis and operational requirements that must be relied upon by DOE to authorize operation of facilities or activities. In addition, the authorization basis encompasses the information a contractor must provide in response to all environment, safety, and health requirements applicable to a facility or activity. Although assurance of quality of software used in quantitative analysis is important in general, it takes on a unique significance in safety analysis required for ISM.

A lack of clear direction on the appropriate standards and requirements for the quality assurance of software and its use leads to the potential for incorrectly or inadequately analyzing hazards. In addition, software-controlled systems with a safety function may not perform as intended. Indeed, most aspects of ISM are affected by software. For example:

- *Work definition and scope* may be prioritized on the basis of safety significance, which is often determined with the help of software tools.

- *Analysis of hazards* requires high-quality codes for estimating importance and consequence of potential accidents.

- *Identification of controls* requires high-quality codes to determine administrative controls and the safety significance of systems, structures, and components.

- *Safe conduct of work* requires high confidence that computer software and safety-related instrumentation and control (I&C) systems will operate reliably.

One element of ISM, hazard identification and analysis, is strongly dependent on software quality. DOE Order 5480.23, *Nuclear Safety Analysis Reports* (U.S. Department of Energy, 1992a), sets forth requirements for contractors to prepare a safety or hazard analysis report that identifies potential scenarios with high consequences to the public, workers, or the environment. Moreover, computer codes are often used to identify preventive and mitigative systems, which must function to eliminate or reduce any unacceptable consequences to acceptably low values. DOE is responsible for approving the selection of these special controls and the basis upon which the selection was made; this constitutes the authorization basis discussed earlier. Thus, confidence in the adequacy of controls, as well as the safety basis in general, depends on the quality of the software and the fidelity of its application.

3. CURRENT STATUS OF SOFTWARE QUALITY ASSURANCE IN THE DOE COMPLEX

An integrated and effective infrastructure for SQA implementation does not currently exist within DOE. An effective infrastructure would include ongoing research and development in improvement of the codes; a formal code configuration control program; standardized training; and formal program direction to provide guidance on the use of codes. Some elements of such an infrastructure do exist, but they are fragmented and isolated from one another. With modest support, these and other elements could be integrated into an infrastructure capable of correcting the SQA problems within the DOE complex.

This section presents an assessment by the Board's staff of the various elements of DOE's SQA infrastructure, as well as the impact of the lack of a unified structure to guide the development and use of safety analysis and I&C software. The focus is on the following:

- *Accident analysis codes*—These codes are used to calculate accident consequences in support of identification and classification of controls and hazard analysis. Many of these codes are extremely complex and have evolved during many years and under several uncoordinated development efforts. The result has been poor pedigrees and low levels of SQA, and a clear lack of adherence to current industry standards.

- *I&C control software*—This software either controls machinery or provides synthesized information about the physical state of a process or system. I&C software is generally associated with the implementation of controls. Although most sites in the DOE complex have applicable high-level standards and requirements that address SQA, the sound principles they embody often do not flow down to actual applications. In general, systems with software-aided control have independent hardware safety features. However, because I&C software adds to defense-in-depth, quality assurance (i.e., SQA) for this software is a safety concern.

3.1 GAPS IN DOE'S INFRASTRUCTURE

The Board's staff believes the root cause of many of the recent problems with SQA in the DOE complex is the absence of an effective infrastructure for executing SQA. The division of roles and responsibilities, as set forth in DOE's Functions, Responsibilities, and Authorities Manuals (FRAMs), defines general quality assurance functions. However, there is no overarching function to effectively integrate operational safety issues with technical aspects of the development of safety bases and software-related controls. In other words, there does not appear to be a formal linkage between individuals responsible for preparing safety bases and those who serve as the stewards of the software tools used in developing the safety bases. This situation has resulted in deficiencies in guidance, code maintenance, training, and new research initiatives. As noted above, some of the critical elements of an effective SQA infrastructure exist within DOE, and they are reviewed in the following subsections.

3.1.1 Roles and Responsibilities of DOE Headquarters

DOE has a set of Orders, guides, and manuals that could serve as a basis for SQA programs for both analytic software that supports safety basis definitions and I&C-related software. DOE Order 414.1, *Quality Assurance* (U.S. Department of Energy, 1998b) sets forth broad requirements for quality assurance programs. DOE Order 200.1, *Information Management Program* (U.S. Department of Energy, 1996) is the primary policy instrument for life-cycle management of software. These DOE documents contain general SQA objectives; however, they lack a practical focus. DOE Guide 200.1-1, *Department of Energy Software Engineering Methodology* (U.S. Department of Energy, 1997) provides generic guidance for developing and implementing quality software and reflects the requirements set forth in the canceled DOE Order 1330.1D, *Computer Software Management* (U.S. Department of Energy, 1992b). This guide also incorporates standards and preferred practices for software engineering, project management, and quality assurance that are advocated by the Institute for Electrical and Electronics Engineers (IEEE) and the Carnegie-Mellon Software Engineering Institute. Though more specific, this DOE guidance is focused primarily on the development of new software and does not address the problem of establishing SQA in existing software of poor pedigree.

Most DOE actions designed to address some aspects of SQA for safety-related software originate with DOE's Office of Defense Programs (DOE/DP). Discussions with personnel in various DOE Headquarters offices revealed scant evidence of involvement in SQA by other DOE Headquarters organizations, including the Office of Environmental Management (DOE/EM); the Office of Environment, Safety, and Health (DOE/EH); and the Chief Information Officer (CIO). Given the broad safety significance of SQA issues, the Board's staff believes all appropriate organizations within DOE that rely on software for safety systems should participate in a cross-cutting SQA program, and that this program should be integrated and given project management focus.

3.1.2 DOE Office of Defense Programs Activities

DOE/DP established the Accident Phenomenology and Consequence (APAC) methodology evaluation program in 1994 to address such vulnerabilities as inadequate SQA, improper code utilization, and inconsistent interpretations of parameter values used in bounding value calculations. The APAC evaluation program was undertaken to develop guides that would ensure appropriate use of codes for safety analyses and could be used in defining future code development activities. By late 1997, the program had published reports in three of its six focus areas; spills analysis (Brereton et al., 1997), in-facility transport analysis (Spore et al., 1996), and chemical dispersion and consequence assessment (Lazaro et al., 1997b). Final drafts in the remaining three focus areas of radiological dispersion/consequence analysis (O'Kula et al., 1999), fire analysis (Restrepo et al., 1996), and energetic events (Lazaro et al., 1997a) have been completed but not yet published due to funding limitations. These reports constitute a reasonable assessment of a select set of computer models, along with recommended hand-calculations for scoping analyses.

The APAC reports contain numerous recommendations for advancing the capabilities of the safety analysis community and increasing confidence in widely used computer codes. Substantive recommendations include the need for:

- Compiling a comprehensive list of codes useful for safety analysis, including outside resources such as those of the U.S. Department of Defense (DoD) and the North Atlantic Treaty Organization.
- Developing postprocessors to better integrate code outputs, thus enhancing the efficacy of follow-on safety analyses.
- Developing further recommendations on the use of computer codes for modeling explosion/deflagration phenomena.

Inherent in these recommendations is the notion that computer codes need to be subjected to a rigorous quality assurance program. However, the characteristics of such a program are not defined in the APAC reports.

3.1.3 Activities of DOE Albuquerque Operations Office

The DOE Albuquerque Operations Office (DOE/AL) currently supports an organization that is dedicated to the promotion of SQA. A Software Quality Assurance Subcommittee (SQAS) was formally established in 1988 to serve as a technical advisory group to the DOE Nuclear Weapons Complex (NWC) Quality Managers. The charter of the SQAS is to promote an understanding and awareness of software quality and its assurance, and to identify and share tools, techniques, and methodologies for improving software quality. SQAS comprises both DOE and NWC contractor personnel. Since 1988, SQAS has issued numerous reports, covering such topics as the following:

- Definitions of software engineering terminology
- Software process assessment
- Software measurement
- Guidelines for software quality audits
- Status reports on licensing and certification of software professionals
- Guidelines for resources and responsibilities in software quality management

A common theme of SQAS documents is that management plays a pivotal role in the development of quality software, and that it is only through management support that the programmatic elements required to perform all aspects of quality software development and implementation can be adequately accomplished. In addition, SQAS reports provide comprehensive guidance relating to software requirements, design, implementation, and testing.

Through biannual meetings and triennial Software Quality Forums, SQAS appears to have the potential to serve as an effective mechanism for disseminating software engineering methodologies. However, the parent NWC Quality Managers group has questioned the need for SQAS. To provide greater value to the NWC Quality Managers group, SQAS self-identified the need to (1) generate fewer but higher-quality documents, (2) support the Accelerated Strategic Computing Initiative more directly, and (3) play a role in the electronic integration of the NWC (U.S. Department of Energy, 1998c).

At this time, there is evidence that the SQAS capabilities available to the complex are not being utilized effectively. For example, when the Board's staff contacted the Radiation Safety Information Computational Center (RSICC) at Oak Ridge National Laboratory to assess the impact of SQAS, knowledgeable RSICC staff members professed no knowledge of the group or its products. (It should be noted that RSICC is the primary distributer of radiation transport and reactor analysis codes.)

All of the DOE sites assessed by the Board's staff have quality assurance plans related to software. These plans appear to meet the minimum requirements of DOE Order 414.1 (U.S. Department of Energy, 1998b); thus the lack of widespread knowledge of SQAS does not preclude the possibility of achieving some degree of SQA. However, the efficiencies achieved by an NWC-wide infrastructure would greatly enhance the rigor of SQA and ensure a common understanding of the limitations of software packages used throughout the NWC.

To meet the intent of SQA, a realistic model of the process by which software is developed and implemented is essential for the validation and verification of software performance. Of particular interest is the wide range of ad hoc software development activity across the defense nuclear complex that eventually results in useful software. One recent example which is a preprocessor for the widely used Monte Carlo N-Particle (MCNP™) code is a code called MCNP-VISED. This preprocessor was developed at Pacific Northwest National Laboratory by summer students working under the supervision of an MCNP™ expert from Battelle Pacific Northwest Laboratory (R. Schwarz, personal communication, March 1999). There was no specific programmatic support. The code conforms to the RSICC standards for format, but underwent no formal, auditable validation and verification process. The code contains numerous errors, although none found to date appear to have safety implications. The errors are reported to the developer by the user community, and trouble reporting and corrections to the code therefore depend on an ad hoc symbiotic relationship between the users and the developer. It should also be noted, however, that an overly onerous quality assurance process would likely have prevented development of this useful code.

To ensure that SQA is performed at all levels of software development, a graded approach needs to be considered by reviewers, who should be capable of understanding the physical phenomena or I&C function associated with a code, the safety ramifications of code malfunctions or misapplications, and the mechanics of the code itself. Some central body could disseminate SQA methodologies and provide appropriate reviews to ensure the proper functionality of safety-relevant software. This body would be most effective if its support were provided on a programmatic basis so that development of new codes or improvements to existing ones would not be stymied by a funding burden attributed to SQA.

3.2 EXAMPLES OF ISSUES WITH ACCIDENT ANALYSIS CODES

APAC evaluations of the current tools available to safety analysts are excellent sources of data on code utilization in support of safety analysis reports. Fewer than 4 percent of codes surveyed by the APAC program meet current industry standards for SQA. Appendix A provides a brief synopsis of the APAC results. MELCOR Accident Consequence Code System 2 (MACCS2), a code that is known to have software deficiencies, is discussed in detail below. Of particular importance is the degradation of the fidelity of safety bases that can be attributed to a poor SQA pedigree.

3.2.1 MACCS2 Code

The MACCS2 code is used to calculate the health and economic consequences of accidental airborne releases of radioactive material, typically in the form of a plume carried by wind (Sprung et al., 1990; Chanin et al., 1993).[1] This code has been found to contain systematic errors. Such errors can lead to invalidation of the authorization basis for a nuclear facility, potentially causing disruptions in operations and necessitating expensive backfits to safety systems.

The MACCS2 code is an evolutionary descendent of a code known as Calculation of Reactor Accident Consequence (CRAC) that was developed as part of the WASH-1400 study (U.S. Nuclear Regulatory Commission, 1975). MACCS2's more recent predecessor, MELCOR Accident Consequence Code System (MACCS) (Chanin and Young, 1997), was used to perform calculations for NUREG-1150, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants* (U.S. Nuclear Regulatory Commission, 1990), and was used by DOE to support a risk-based authorization basis for the K-Reactor at the Savannah River Site. The level of SQA with the MACCS code is relatively good.

MACCS2 was developed to expand the range of facilities to be analyzed beyond reactors and make it possible to address a variety of DOE non-reactor nuclear facilities. MACCS2

[1] The earlier version of the MACCS2 code (MACCS for MELCOR Accident Consequence Code System) was developed by Sandia National Laboratories for the Nuclear Regulatory Commission for use in calculating off-site consequences of severe accidents at nuclear power plants.

employs a number of enhancements, among them an increase in the number of radionuclides included and the number of daughters permitted in the decay chains, a look-up table option for dispersion coefficients, emergency response and food pathway models, and additional types of output. There are documented problems with the MACCS2 code, however, in all areas of SQA concern, including issues of numerical model adequacy, source code fidelity, and proper end-user execution. Despite these identified SQA problems, MACCS2 has been widely used in safety analyses that support authorization bases throughout the DOE complex.

In communications with one of the MACCS2 code developers, the Board's staff determined that there was no formal SQA program for the MACCS2 code. In the first phase of development, modifications were made to the MACCS code to provide the desired new features for use at DOE facilities. Individuals other than those making the original changes evaluated the revised code for correctness using both line-by-line inspection and testing. The results of these evaluations were documented, but apparently were later lost. In a subsequent phase of the code development, there was inadequate independent inspection and testing. Sandia National Laboratories later contracted with the University of New Mexico in an attempt to correct this deficiency (Chanin, 1997 and O'Kula, 1999). The report of that effort, however, was never published (Westinghouse Savannah River Company, 1998).

It would appear that additional effort is needed to bring the MACCS2 code into compliance with sound principles of SQA if it is to continue to be used for analyses to support authorization bases at DOE facilities. Such an effort would satisfy the intent of the consensus standards for SQA of the IEEE, the American Society of Mechanical Engineers (ASME),1997, the American Nuclear Society, 1987 and 1995, and the Institute of Electrical and Electronics Engineers, Incorporated, 1983 and 1989. These standards contain provisions for bringing software not developed under a formal SQA program up to a reasonable level of compliance.

The Board's staff has identified a number of concerns with MACCS2 that are a result of inadequate SQA. These concerns include the following:

- *Phenomenology*—One of the authors of the code has indicated that the model in the code underpredicts the dose to the maximally exposed off-site individual in the case of releases from fires (D. I. Chanin, personal communication, November 1997).

- *Coding errors*—An error in the source term looping function was found to produce erroneous results when four plumes were specified. This particular error was discovered during the preparation of the Safety Evaluation Report for a facility at the Pantex Plant in Amarillo, Texas. As noted earlier, such errors can lead to invalidation of the authorization basis for a nuclear facility, potentially causing possible disruptions in operations and necessitating expensive backfits to safety systems. Apparently, this error was introduced when the number of dose conversion factors in the database was increased. The dimensions of the independent variables associated with this change had been properly modified, but not the dependent variables. This error led to a preliminary review of the MACCS2 SQA program in 1997.

- *End-user quality assurance problem*—Westinghouse personnel at the Savannah River Site reported in July 1998 that the default value in the code for dose conversion factors is based on plutonium oxide, but the limiting radionuclide at the H-Canyon facility is plutonium nitrate. Westinghouse analysts determined that the dose consequences rose by 50 percent when the proper dose conversion factors were used in the code. In this particular case, the increased dose rates are due to the different chemical and biological effects of plutonium nitrate versus oxide; i.e., the nitrate goes into solution in the lungs, reaches critical organs more rapidly, and stays in the body longer (U.S. Department of Energy, 1998a). The analyst should have been aware of the relationship between solubility class and dose conversion factors.

- *Poor documentation*—Quality assurance problems stem from difficulties in using the code. The code is poorly documented, and the input streams are difficult to construct, so errors can easily be introduced. Considerable effort is required to assemble the MACCS2 input decks without errors. The Board's staff has a made a number of suggestions to the developers for improving the ease of use of the code and minimizing errors during input preparation. These suggestions include eliminating redundant inputs, relaxing unnecessary constraints on input parameters, creating a user-friendly interface and postprocessor, and integrating the modules more closely.

3.2.2 Other Codes of Interest

Some of the systemic SQA issues noted for MACCS2 have also been noted with respect to the Explosive Release Atmospheric Dispersion (ERAD) (Boughton and DeLaurentis, 1992) and the Fire Analysis and In-Facility Transport (FIRAC) (Spore et al., 1996) codes. ERAD, developed by Sandia National Laboratories to model explosive dispersal of hazardous materials, has SQA problems that could adversely impact the conservatism of safety analysis results. These problems, which are not described in the code documentation, include grid instability and generic use of the meteorological input file approach as a substitute for site-specific meteorological data (Steele et al., 1998; Hills et al., 1998). FIRAC, a code that models dispersal of hazardous materials by fire, has no formal SQA plan, although some validation documentation is available. Users have indicated that the code can fail without any meaningful error messages, and it does so regularly. The use of both of these codes for safety-basis-related work at defense nuclear facilities in support of safety analyses should be reevaluated.

3.3 EXAMPLES OF ISSUES WITH INSTRUMENTATION AND CONTROL SOFTWARE

In the case of I&C software, there have been instances in which requirements for rudimentary SQA have been contractually stipulated, but do not flow down to implementation at the floor level. As noted earlier, while computer-driven I&C systems are generally backed up by hardwired safety systems, I&C software does play a significant safety role in defense-in-depth for a facility. This section describes instances of deleterious impacts on facility operations that have been the result of inadequacies in SQA for I&C software.

3.3.1 Los Alamos Critical Experiments Facility

At the Los Alamos Critical Experiments Facility (LACEF), software can be used to control the approach to nuclear criticality during experimental work on critical assemblies, such as the Critical Experiments Machines at LACEF (Planet, Sheba, and Comet). In a February 1998 event involving the Planet critical assembly, a failure of the control system software combined with a spurious hardware failure caused an uncontrolled reactivity insertion. This problem was traced back to a software programming error that allowed for a high-speed insertion of reactivity when the hardware sent a spurious signal. This event resulted in a positive Unreviewed Safety Question determination.

This issue, along with others, contributed to an extended shutdown of LACEF. During the restart process, a review of SQA requested by the Los Alamos National Laboratory (LANL) Reactor Safety Committee, which independently reviews assembly operation, identified a number of deficiencies in SQA. These deficiencies included the following:

- The requirements documents typically described functions at the system level, but not specific software functions.
- Reviews of software revisions were conducted by personnel familiar with the system, but not by software professionals.
- The software test plans were not sufficiently detailed to test the functionality of individual modules and did not have acceptance criteria for each step.
- Documentation of testing was not complete.
- No quality assurance review was performed.

LANL subsequently identified short- and long-term plans to address the above deficiencies. Short-term plans included identifying and upgrading the safety-related functions of the software; describing the method of implementation for each requirement; upgrading the test plan to test the safety functions, including defining the test method and the acceptance criteria; performing and documenting the testing; obtaining reviews of the documentation and testing; and freezing the software configuration until an acceptable change control program is developed. Long-term plans include recruiting an external consultant with expertise in quality assurance for software and control systems, selecting a process or standard for conducting SQA, and preparing and implementing the SQA process. The new SQA process is expected to be applied during the upgrade of the software descriptions and the development of new computer-controlled systems.

3.3.2 Programmable Logic Controllers: Various Incidents

Additional examples of software quality control problems with DOE-owned control systems have been found with programmable logic controllers (PLCs). Many PLCs play an important role in the control of safety-related equipment. A scoping search of the DOE occurrence reporting system yielded more than 150 reportable occurrences involving PLC issues. More than 27 percent of these occurrence reports involved some type of PLC failure. The following are examples of the more significant PLC failures:

- Unexpected and spurious change of PLC internal software coding, resulting in unexpected behavior of the PLC and the PLC-controlled equipment.

- Unexpected behavior of PLCs and PLC-controlled equipment (including continuous air monitors [CAMs]) due to inadequate software programming verification and validation. This failure indicates the possibility of common-cause failure mechanisms.

- Potential for worker fatality (steam explosion or exposure to 1400°F steam) due to a hardware wiring error and PLC operation in accordance with its programming logic.

- Failure of a uranium hexafluouride leak detection system alarm due to a single point of failure in a PLC alarm circuit resulting from an unexpected interaction lockup of two redundant PLCs performing routine automatic circuit-checking routines. This reported failure indicates the possibility of common-cause failures of redundant equipment and hence the potential for complete loss of a safety function.

- Dual PLC failure due to inadequate testing of PLCs in the expected normal operating temperature environment.

- Release of radioactive material due to PLC module failure.

- Unexpected ventilation fan speed changes and stoppage in a nuclear facility due to incorrect activation of a PLC module during a maintenance activity. This could result, for example, in backflow of contaminated air from vented hoods, thus presenting a hazard to workers.

The above PLC failures caused systems to behave erratically as a result of driver or embedded software problems that in some instances caused common-mode failures, even when redundant PLCs were used. This list of actual failures demonstrates that PLCs can introduce new types of malfunctions and attendant challenges to safety beyond those previously considered in the authorization basis. Indeed, the list presented here is but a limited selection of examples of a much larger problem. SQA protocols can be an important contributor to identifying and preventing safety-related control system failures.

3.4 OTHER ISSUES

The Board's staff believes that DOE should take action to identify the breadth and depth of deficiencies in computer software used in both support of safety analyses and machine control at DOE sites. Such a program should assess current operational deficiencies, as well as the root causes of these deficiencies. The objectives should be to assess the current status of SQA, to develop a reasonable and cost-effective path forward for correcting the identified deficiencies, and to implement compensatory measures that would bring critical software to an acceptable level of conformance with standard industry practice. It may be noted that many elements of an effective SQA program already exist, but those elements have yet to be integrated into an effective whole. The identification of appropriate SQA requirements promulgated through a DOE standard or equivalent mechanism, along with a means to enforce their use, would ensure the appropriate level of SQA for safety-related software.

Improvements to quality assurance of existing I&C software and accident analysis codes can be tailored. Rather than formal backfitting of existing codes, alternative methods and expert judgment could be used, when appropriate. Formal verification and validation for existing codes should be limited to those codes that are and will continue to be widely used. In addition, special-purpose software, such as that used in safety-related I&C systems, should meet a level of SQA formality appropriate to the safety significance of the control feature.

4. POTENTIAL DOE IMPROVEMENTS IN SOFTWARE QUALITY ASSURANCE

The previous sections outlined numerous problems with SQA in the DOE nuclear weapons complex. The root cause of these deficiencies appears to be an inadequate infrastructure for SQA. Specific concerns identified by the Board's staff include insufficient guidance and training on the use of codes and unclear ownership for SQA problems within DOE, as well as concerns about the robustness of the research program to improve understanding of the application of first principles and develop code benchmarks. These concerns led the staff to develop the suggested corrective actions presented in this section. These actions are aimed at achieving potential improvements to address the root and contributing causes to the identified deficiencies in SQA within DOE.

4.1 POTENTIAL IMPROVEMENTS IN DOE SOFTWARE QUALITY ASSURANCE INFRASTRUCTURE

The activities of the various DOE offices and projects that perform SQA-related functions need to be coordinated with a project management focus if a strong SQA infrastructure is to be established. Furthermore, an effective approach to the development of a productive SQA infrastructure should include, but not be limited to, the following actions:

- Take advantage of the expertise and findings of the APAC program. Establish a centralized safety analysis support group that, among other responsibilities, would assume stewardship of accident analysis codes accepted for use in DOE safety basis analyses. Funding should be stabilized for this high-visibility and cross-cutting effort. The SQA responsibilities of this group should include the following:

  - Performance of postdevelopment verification and validation reviews of extant accident analysis codes and certification of those found acceptable for use in DOE safety basis analyses.

  - Maintenance (including configuration control) and distribution of certified accident analysis codes.

  - Identification of areas of accident analysis in which current codes are inadequate or nonexistent, and new tools and techniques are needed.

  - Direction of adequate research and development focused on development of new codes to meet the needs of the accident analysis areas identified as deficient, and assurance that adequate SQA is integrated into the development of these codes. Consideration should also be given to the identification and development of benchmark data, where appropriate.

  - Promulgation of guidance on code use and best practices for the certified set of codes through a robust official Web site and periodic training seminars.
  - Development and implementation of a qualification program for performing safety basis analyses of DOE facilities and activities.

- Integrate the DOE/AL SQAS efforts with all DOE sites and programs affected by SQA, such that productive impacts are realized complex-wide. Measures to this end would include, but not be limited to, the following:

  - Development or identification of a postdevelopment verification and validation standard and acceptance criteria appropriate for use in assessing and certifying codes for DOE safety basis analyses. In addition, appropriate standards should be developed or cited for new code development.
  - Assistance to individual DOE sites in determining which SQA standards are appropriate for their operations. Areas addressed should include, at a minimum, local installation and checkout, end-user verification and validation guidance, and I&C systems.
  - Assistance to individual DOE sites in assessing their level of compliance with the SQA standards identified as applicable to their operations, and in implementing corrective actions where deficiencies are found.
  - Verification that the SQA principles comprising the SQA standards identified as applicable at individual DOE sites flow down and are properly applied in actual software-related activities.

4.2 POTENTIAL IMPROVEMENTS TO SOFTWARE QUALITY ASSURANCE FOR INSTRUMENTATION AND CONTROL SYSTEMS

I&C software utilization is highly site-dependent. Most sites address SQA at a high level with references to standards in their contractual documents, but there is little evidence that high-level SQA principles flow down to practices in actual applications. Furthermore, in some instances the referenced standards are not well suited to the I&C software profile of the site. A logical general paradigm for correcting this situation is a case-by-case approach for each site that would consist of, but not be limited to, the following actions:

- Assess the software profile with regard to I&C. These assessments should be aimed at determining: the level of reliance on software for I&C purposes, the applicable standards addressing SQA, and verification of hardwired safety systems.

- Determine whether the applicable SQA standards are appropriate for a given site, considering the nature of that site's operations and the findings of the software profile assessment. If current standards are inappropriate, identify an acceptable set, and incorporate that set into contractual documents that are part of the authorization basis.

- Verify that the principles comprising the acceptable set of applicable SQA standards flow down and are implemented in actual I&C systems. Where it is determined that the high-level principles are not being applied, institute corrective actions to bring the I&C systems into compliance.

For the specific case of the I&C software problems at LANL, a prudent corrective action would be to execute immediately a postdevelopment SQA program aimed at increasing confidence in the three reactor assemblies that have software-controlled I&C systems with known deficiencies, and to develop a more rigorous SQA process designed to minimize future software problems.

Finally, as was indicated in Section 4.1, the Board's staff believes an enhanced DOE/AL SQAS operation would be effective in supporting the sites' efforts to improve the level of SQA associated with I&C systems throughout the complex.

4.3 POTENTIAL IMPROVEMENTS FOR SOFTWARE QUALITY ASSURANCE ASSOCIATED WITH ACCIDENT ANALYSES

Under the approach to SQA infrastructure development discussed in Section 4.1, potential improvements in SQA for accident analysis code could be achieved primarily through a centralized safety analysis group with coordinated support from an enhanced SQAS. The general pathway for realizing improvements in this regard is centralization. The accident analysis codes with the best combinations of technical robustness and existing SQA would be identified, with consideration for their degree of use within the complex. These codes would then be consolidated into a standard "tool-box" to be certified, under a postdevelopment verification and validation program, for use in DOE's safety basis analyses. The following are some specific actions the staff believes would improve the state of SQA with regard to accident analysis codes (it should be noted that a significant amount of the ground work for these actions has been covered under the APAC project):

- Determine which codes have been or will be used to assess hazards and their consequences, identify controls, or support other ISM safety-critical activities at defense nuclear facilities. Assess the adequacy of these codes in the following areas: model fidelity and appropriateness for various accidents, code pedigree and level of SQA, confidence in local installation at sites using the codes, and ease of use (including user interface, user documentation, and guidance on input parameters).

- Since the MACCS2 code is widely used for authorization basis calculations and is known to have deficiencies, immediately conduct a postdevelopment verification and validation program for this code to bring it into a reasonable level of compliance with accepted standards.

- Assess the degree of use of codes determined to have inadequate pedigrees, determine the safety significance for each case, and take the following actions:

  - For codes that will comprise the standard tool box and be used for authorization basis calculations, conduct postdevelopment verification and validation in accordance with standards and guidance provided by SQAS.

  - Develop and implement compensatory measures, as appropriate (based on Unreviewed Safety Question evaluations), for all cases in which authorization basis deficiencies have been identified. Compensatory measures might consist of independent analysis using other codes or hand-calculation methods, expert judgment of reasonableness, or imposition of additional controls.

  - Once tool box codes with an inadequate pedigree have been brought into reasonable compliance with appropriate SQA standards, place them into a configuration management program to maintain the pedigree during future code evolutions.

- Develop and institute an intensive training program, including best practices and other guidance, for safety analysts who use such codes in the performance of safety analyses, emergency preparedness, or other safety-related activities. This training course should also emphasize conditions under which hand-calculations are adequate. It should serve as one of the key elements of a broader program of instruction leading to formal qualification of safety engineers.

- Consider a modest program of experimental research designed to validate calculations used to develop the safety basis for nonreactor nuclear facilities. The scope of this program should be limited to the most safety-significant aspects of such calculations and should yield a safety benefit commensurate with the cost of the experiments. In some cases, efforts to develop new models may also be appropriate.

- Develop a Web site to (1) promulgate lessons learned from the application of codes in safety analyses; (2) share benchmark data and test problems; (3) permit rapid communication of code problems and fixes; (4) share databases needed for execution of these codes, such as meteorological and population data; and (5) provide a forum for discussion of common problems.

- Identify a core group of safety analysis experts to advise on the above actions and resolving future technical issues.

5. CONCLUSION

The observations documented in this report led the Board's staff to conclude that there is no adequate SQA program for DOE's defense nuclear complex. Deficiencies exist in the infrastructure for programmatic support of SQA, technical outputs from software used in safety analyses, and I&C for safety systems. Section 4 presented a number of specific suggestions for improvements in SQA; however, these are merely illustrative of a larger set of issues that need to be addressed by DOE and its contractors. These broader issues include the need to:

- Develop a DOE standard with a practical focus on SQA.
- Identify all organizational elements of the defense nuclear complex that should be involved in the systematic development, testing, documentation, maintenance, and execution of software—especially as regards safety.
- Provide adequate funding support for SQA.
- Provide a project management focus and leadership for the integration of all disparate SQA efforts into a single comprehensive program.

APPENDIX A

Status of Software Quality Assurance and Verification and Validation (SQA/V&V) for Software Employed by DOE Defense Nuclear Facilities

The format and content of this appendix are in accordance with the APAC program. A table summarizing the SQA/V&V status for the APAC identified codes is presented for each of the six primary analysis areas. The tables contain information regarding the code developer and sponsoring organization, the current owner/technical support contact point, and the status of code SQA/V&V. Text comments regarding SQA/V&V that appear in regular type are derived from the APAC program, while bolded comments are those of the Board's staff. Though not complete, this list of codes captures a significant portion of the tools used in each of the six most common areas of accident consequence analysis. Furthermore, the list should provide a representative picture of the current state of SQA/V&V for the cadre of codes used predominantly in support of DOE authorization bases.

RADIOLOGICAL DISPERSION

Code	Code Developer/ Sponsor	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
AI-RISK	Los Alamos National Laboratory	Pat McClurc Los Alamos National Laboratory MS K557 Los Alamos, NM 87545 (505) 667-9534	Unknown	
ARAC (MATHEW/ ADPIC)	Lawrence Livermore National Laboratory (U.S. Department of Energy/DP)	Connee Foster Lawrence Livermore National Laboratory (L-262) P.O. Box 808 Livermore, CA 94551 (510) 422-1867	No formal SQA program was in effect during development; however, this code has been subjected to the most extensive V&V work of any of the dispersion codes considered by the APAC group. **The code is probably still short of accepted industry standards with regard to SQA/V&V.**	The APAC group judged this code to be the most technically sophisticated and robust for general atmospheric transport of radionuclides.
AXAIRQ	Westinghouse Savannah River Company	Ali Simpkins Westinghouse Savannah River Company Savannah River Site 773-A Aiken, SC 29808 (803) 725-9643	Local Savannah River Site code owners have performed verification testing of code modules since its inception. **The SQA/V&V plan associated with this code is ad hoc and incomplete.**	
BNLGPM	Brookhaven National Laboratory	Paul Michael Brookhaven National Laboratory, Building 318 P.O. Box 5000 Upton, NY 11973-5000 (516) 344-2264	Unknown	Development was site-specific for use with High Flux Beam Reactor. The code is limited to releases of noble gases and radionuclides.
COSYMA	CEC Code developed by KfK (Germany) and NRPB (U.K.)	Jan van der Steen KEMA Nederland B.V. Postbus 9035 NL-6800 ET Arnhem, The Netherlands 31.26.356.33.70	Unknown	

RADIOLOGICAL DISPERSION

Code	Code Developer/ Sponsor	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
ERAD	(U.S. Department of Energy)	Bruce Boughton Sandia National Laboratory Albuquerque, NM 87185 (505) 844-8545	This code's predictions have been compared with 1963 Nevada Test Site Operation Roller Coaster dose and deposition data. Agreement was generally within 50%, thus APAC believes thc models representation of physical processes has been validated. **Though the validation efforts associated with this code are relatively more substantial than others, in an absolute sense the V&V efforts are ad hoc and are not part of a systematic SQA plan.**	
ETMOD		G. L. Ogram Ontario Hydro Research Division Ontario Hydro Toronto, M5g 1X6, Canada	A verification and validation report is provided with the code.	This code is for tritium transport only.
GENII	Pacific Northwest National Laboratory	Bruce Napier Pacific Northwest National Laboratory P.O. Box 999 Richland, WA 99352 (509) 375-3896	This code has thorough documentation and quality assurance and has been accepted by DOE for use in accident consequence calculations for safety analyses. **It is unclear what criteria apply to DOE "acceptance." Although the SQA plan is certainly more thorough in a relative sense than those for other codes considered by APAC, it probably still falls short of conventional industry standards.**	Numerous model attributes are either nonfunctional or inconsistent with various regulatory guide recommendations.

RADIOLOGICAL DISPERSION

Code	Code Developer/ Sponsor	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
GXQ	Westinghouse Hanford Company (U.S. Department of Energy)	Britt Hey Westinghouse Hanford Company P.O. Box 1970 Richland, WA 99352 (509) 376-2921	Validation is implied for this code because it uses models similar to those in other "validated" codes. Verification is in the form of a series of documented test cases, which were independently checked and reviewed. **The acceptance criteria for "validation" are not clear. The test cases, though a good beginning, likely do not comprise an SQA plan commensurate with conventional industry standards.**	Error checking is minimal for this code; an experienced user is required.
HOTSPOT	Lawrence Livermore National Laboratory	Steven G. Homann Lawrence Livermore National Laboratory 7000 East Ave L-380 Livermore, CA 94551 (510) 490-6379 (501) 423-4962	No software development plan was identified. The model is based on experimental results of the 1963 Nevada Test Site Operation Roller Coaster. Westinghouse Savannah River Company reviewed the SQA/V&V status and issued a set of reports. **Though this code derives from empirical models, the approach to SQA/V&V is not commensurate with current industry standards.**	This code is generally appropriate only as a first-response tool for computing first-order approximations in response to accident situations in which quick computation time is paramount.
MACCS2	Sandia National Laboratories and Idaho National Engineering and Environmental Laboratory (U.S. Nuclear Regulatory Commission and U.S. Department of Energy/DP)	Julie Gregory Sandia National Laboratories P.O. Box 5800 MS 0748 Albuquerque, NM 87185 (505) 844-7539	**The MACCS2 predecessor code MACCS was developed within a well-considered SQA/V&V plan for Nuclear Regulatory Commission applications. However, the upgrades and extensions of the MACCS2 code did not follow the same regimen; hence there are significant concerns, both identified and postulated, with regard to the quality of this code's SQA/V&V.**	This is one of the most extensively used codes for authorization basis consequence analyses in the DOE complex.

RADIOLOGICAL DISPERSION

Code	Code Developer/ Sponsor	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
PAVAN	Pacific Northwest National Laboratory	Leta Brown U.S. Nuclear Regulatory Commission Rockville, MD (301) 415-1232	**Unknown. However, considering the code was developed for Nuclear Regulatory Commission commercial licenses, the SQA/V&V program may be sound.**	This code is considered "on-the-shelf" software as APAC did not identify continuing Nuclear Regulatory Commission sponsorship for development.
RSAC-5	Idaho National Engineering and Environmental Laboratory (U.S. Department of Energy)	D. R. Wenzel Lockheed Idaho Technologies Co. P.O. Box 1625 Idaho Falls, ID 83415 (208) 526-3463	This code was subjected to a rigorous SQA/V&V plan. **The SQA/V&V approach for this code appears to be rigorous and consistent with current industry standards.**	The code has an associated input preprocessor, RSAC+, with significant error-checking features to minimize user errors.
TRAC RA/HA	Alpha-TRAC Inc. (Rocky Flats Environmental Technology Site)	C. Reed Hodgin AlphaTRAC Inc. Sheridan Park 8 Suite 120 8670 Wolff Court Westminster, CO 80030 (303) 428-5670	The code was formally evaluated and approved for use by the State of Colorado. An adequate SQA/V&V approach was applied. **Colorado approval criteria are currently unknown; however, it is likely that the SQA/V&V for this code is consistent with current industry standards.**	
UFOTRI	KfK (Germany)	Wolfgang Raskob Forschungszentrum Karlsruhe, Abt. INR, Potsfach 3640 76021 Karlsruhe, Germany 49-7247-82-2480	Some experimental validation studies have been performed. Some instances showed nonconservatism in the code estimates. **The degree of nonconservatism in the test cases is not clear. The test cases, though a good beginning, likely do not comprise an SQA plan commensurate with conventional industry standards.**	This code is for tritium transport only.

SPILLS

Code	Code Developer/ Geneology	Current Owner/ Tech. Support	Status of SQA/V&V	General Comments
ADAM	Phillips Laboratory (U.S. Air Force)	Capt. Michael Jones AL/EQS 139 Barnes Dr. Tyndall AFB, FL 32403 (904) 283-6002	No SQA plan was identified for this code, and no validation effort was documented. **The SQA/V&V approach is not commensurate with current industry standards.**	
ALOHA	(U.S. Environmental Protcction Agency, National Oceanographic and Atmospheric Administration, and National Safety Council)	Mary Evans (206) 526-6325 National Safety Council P.O. Box 558 Itasca, IL 60143 (708) 285-0797	No SQA plan was identified for this code, and no validation effort was documented. **The SQA/V&V approach is not commensurate with current industry standards.**	
CASRAM-SC	Argonne National Laboratory and University of Illinois (U.S. Department of Transportation and U.S. Department of Energy)	M. Lazaro ANL-EAD 9700 S. Cass Ave. Building 900 Argonne, IL 60439 (708) 252-3447	The developers have conducted a thorough verification effort on the source code. No validation work has been documented to date. The code is stated to be "benchmarked" against ALOHA; however, ALOHA has not been subjected to a documented validation effort. **The ad hoc nature of the SQA approach is not commensurate with current industry standards.**	
EMGRESP	Ontario Ministry of the Environment/Air Resources Branch	Ontario Ministry of the Environment Air Resources Branch 880 Bay St., 4th Floor Toronto, Ontario M5S 1Z8	No SQA plan was identified; however, several references regarding validation are documented. **The ad hoc nature of the SQA approach is not commensurate with current industry standards, and more development work is necessary.**	

SPILLS				
Code	**Code Developer/ Geneology**	**Current Owner/ Tech. Support**	**Status of SQA/V&V**	**General Comments**
HGSystem	Shell Research Limited (U.K.) (Industry Cooperative HF Mitigation/Assessment Program, Ambient Impact Technical Subcommittee [20 chemical and petroleum companies])	Howard Feldman American Petroleum Institute 1220 L St., NW Washington, DC 20005 (202) 682-8340	The SQA plan status is unknown; however, a significant validation effort was performed. **The SQA/V&V approach is likely not commensurate with current industry standards, and more development work is necessary.**	
HOTSPOT/ Resuspension	See evaluation under Radiological Dispersion.			
KBERT	Sandia National Laboratories (U.S. Department of Energy/EH)	K. Washington MS0722 Org. 6913 Sandia National Laboratories Albuquerque, NM 87185 (505) 844-0231	No SQA plan was identified for this code; however, it derives from the extensively validated Mishima release database. **The SQA/V&V approach is likely not commensurate with current industry standards, and more development work is necessary.**	The code has a rather unique approach. It does not rely on a robust computational engine, but rather incorporates data from the Mishima release database (basis for DOE-HDBK-3010-94) directly.
MISM	U.S. Department of Defense	Department of Defense Civil and Environmental Engineering Development Office Tyndall Air Force Base Panama City, FL 32403	No SQA plan was identified for this code. No systematic validation effort was documented. **The SQA/V&V approach is not commensurate with current industry standards.**	The code is currently capable of handling ground spills of only three chemicals: N_2H_4, MMH, and UDMH.

SPILLS

Code	Code Developer/ Geneology	Current Owner/ Tech. Support	Status of SQA/V&V	General Comments
ORG40/TP10	U.S. Army Chemical Research and Development Engineering Center (U.S. Army)	Commander, U.S. Army CRDEC Aberdeen Proving Ground, MD 21010	No SQA plan was identified for this code; however, validation efforts included comparisons with other computational models and experiments. **The ad hoc nature of the SQA approach not commensurate with current industry standards.**	
Pspill	Pacific Northwest National Laboratory (Nuclear Regulatory Commission)	M. Ballinger Pacific Northwest National Laboratory P.O. Box 999 Richland, WA 99352 (509) 373-6715	No SQA plan was identified for this code. The code is simple, and the source code is short. This code might be better classified as an "engineering aid." The model is empirical and based on experimental data. No formal validation efforts were conducted. **The ad hoc nature of the SQA approach is not commensurate with current industry standards; however, the simplicity of the code may make these concerns moot.**	
Tscreen	(U.S. Environmental Protection Agency)	Jawad Touma US EPA, OAQPS, TSD (MD-14) Source Receptor Analysis Branch Research Triangle Park, NC 27711 (919) 541-5381 .	No SQA plan was identified for this code, and no validation efforts have been documented. **The SQA/V&V approach is not commensurate with current industry standards.**	The model is very simplistic.

IN-FACILITY TRANSPORT

Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
CONTAIN	Sandia National Laboratories (U.S. Nuclear Regulatory Commission)	Richard Griffith Org. 6421 MS-0739 P.O. Box 5800 Sandia National Laboratories Albuquerque, NM 87185 (505) 844-8232	A SQA plan exists for this code, and an independent peer review is documented. Also, numerous validation studies have been performed and documented. The SQA/V&V status of this code is likely commensurate with current industry standards. **Maintenance and change control may be an issue for this code as it appears that nonstandard features have been added to some versions in an ad hoc fashion.**	
FIRAC	Los Alamos National Laboratory, Westinghouse Hanford Company, New Mexico State University, Pacific Northwest National Laboratory (FIRIN Module), and National Institute of Standards and Technology (CFAST Module) (U.S. Nuclear Regulatory Commission and U.S. Department of Energy/EH)	William Gregory MS K575 Los Alamos National Laboratory Los Alamos, NM 87545 (505) 667-1120	No formal SQA plan was documented for this code. Some validation documentation is referenced. They indicated that the code can fail without any meaningful error message and regularly fails. They reported that interaction with the original code developers is typically required to complete calculations. Though one of the most technically robust tools available, this code is not recommended for safety basis usage due to the poor status of SQA, specifically with regard to error handling. **The SQA/V&V status of this code is poor, and there are significant concerns about its use for safety basis analyses.**	The FIRAC Module of this code system handles gas dynamics, material transport, and heat transfer. The FIRIN and CFAST Modules are independent options for handling fire modeling.

IN-FACILITY TRANSPORT

Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
GASFLOW	Los Alamos National Laboratory (U.S. Department of Energy/DP&EM and U.S. Nuclear Regulatory Commission)	Kin Lam MS K575 Los Alamos National Laboratory Los Alamos, NM 87545 (505) 665-3362	No SQA plan was identified for this code; however, there has been some work on validation. The SQA/V&V status of this code is not commensurate with current industry standards. **Though some effort regarding SQA/V&V has taken place, it is likely that the approach is not commensurate with current industry standards.**	This is the only code considered by APAC with the capacity for handling multidimensional effects. However, it does not account for agglomeration.
KBERT	See evaluation in Spills table			
MELCOR	Sandia National Laboratories (U.S. Nuclear Regulatory Commission)	K. Bergeron Org. 6421 MS 0739 P.O. Box 5800 Sandia National Laboratories Albuquerque, NM 87185 (505) 844-2507	No SQA plan was identified for this code; however, extensive validation has been performed. **Though significant effort with respect to validation has taken place, it is likely that the SQA/V&V approach is not commensurate with current industry standards.**	

FIRE

Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
FIRAC/ FIRIN	Pacific Northwest National Laboratory (FIRIN Module) (U.S. Nuclear Regulatory Commission and U.S. Department of Energy/EH)	William Gregory MS K575 Los Alamos National Laboratory Los Alamos, NM 87545 (505) 667-1120	No formal SQA plan was identified for this code. Some validation documentation is referenced. Users indicated that the code can fail without any meaningful error message and regularly fails. Users reported that interaction with the original code developers is typically required to complete calculations. Though one of the most technically robust tools available, this code is not recommended for safety basis usage due to the poor status of SQA, specifically with regard to error handling. **The SQA/V&V status of this code is poor, and there are significant concerns about its use for safety basis analyses.**	The focus of evaluation here is on the FIRIN Module, which handles fire modeling. The FIRAC Module, which handles gas dynamic, material transport, and heat transfer, was evaluated by the In-Facility-Transport Working Group.
CFAST	National Institute of Standards and Technology (CFAST Module) (U.S. Nuclear Regulatory Commission and U.S. Department of Energy/EH)	FIRAC/CFAST: William Gregory MS K575 Los Alamos National Laboratory Los Alamos, NM 87545 (505) 667-1120 CFAST: Walter Jones Building and Fire Research Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899 (301) 975-6887	No formal SQA plan was documented for this code. Some validation documentation is referenced. **The SQA/V&V status of this code is not commensurate with current industry standards.**	Following the APAC review, a version of CFAST was incorporated as a fire-handling submodule of the FIRAC system. There is concern about proliferation of multiple versions of this code.

FIRE

Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
COMPBRN III	University of California at Los Angeles (U.S. Nuclear Regulatory Commission)	COMPBRN 3-e: EPRI COMPBRN III: G. Apostolakis Mechanical Engineering Department University of California at Los Angeles Los Angeles, CA	No SQA plan was identified for this code; however, a limited number of validation efforts are documented. **Though some effort regarding SQA/V&V has taken place, it is likely that the approach is not commensurate with current industry standards.**	
FPETool	National Institute of Standards and Technology (General Services Administration and Public Building Service/Office of Real Property Management)	Walter Jones Building and Fire Research Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899 (301) 975-6887	No formal SQA plan exists for this code; however, some validation has been performed and documented. **Though some effort with respect to validation has taken place, it is likely that the SQA/V&V approach is not commensurate with current industry standards.**	
VULCAN	SINTEF (Norway) and Sandia National Laboratories (Norwegian Oil and Gas Industries and Defense Nuclear Agency)	SINTEF Sandia National Laboratories	It is unknown whether a formal SQA plan exists. The code developers make code verification information available, and some validation efforts are documented. **The SQA/V&V status of this code is presently unclear.**	This code represents the state of the art fire-modeling science.

EXPLOSIONS AND ENERGETIC EVENTS

Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
EXPAC	Los Alamos National Laboratory	William Gregory MS K575 Los Alamos National Laboratory Los Alamos, NM 87545 (505) 667-1120	No SQA plan was identified for this code, and no validation efforts have been documented. **The SQA/V&V approach is not commensurate with current industry standards.**	
GASFLOW	See evaluation under In-Facility-Transport.			
HOTSPOT	See evaluation in Radiological Dispersion table			
CHEETAH	Lawrence Livermore National Laboratory	Laurence E. Fried Lawrence Livermore National Laboratory P.O. Box 808 Livermore, CA 94551	No SQA plan was identified for this code; however, extensive validation has been performed. **Though significant effort with respect to validation has taken place, it is likely that the SQA/V&V approach is not commensurate with current industry standards.**	
KIVA-3	Los Alamos National Laboratory	Energy Science and Technology Software Center P.O. Box 1020 Oak Ridge, TN 37831	An SQA plan exists; however, its status is unclear. Documentation of verification and validation efforts may be available from the code developer. **The status of SQA/V&V for this code is unclear.**	This is a complex CFD code.
DYNA2D/3D	Lawrence Livermore National Laboratory	Energy Science and Technology Software Center P.O. Box 1020 Oak Ridge, TN 37831	An SQA plan exists; however, its status is unclear. Documentation of verification and validation efforts may be available from the code developer. **The status of SQA/V&V for this code is unclear.**	This is a complex hydrocode.
CALE	Lawrence Livermore National Laboratory	Dr. Robert Tipton Lawrence Livermore National Laboratory, L-170 P.O. Box 808 Livermore, CA 94550	An SQA plan exists; however, its status is unclear. Documentation of verification and validation efforts may be available from the code developer. **The status of SQA/V&V for this code is unclear.**	This is a complex hydrocode.

CHEMICAL DISPERSION				
Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
ADAM	See evaluation under Spills.			
ALOHA	See evaluation under Spills.			
CALPUFF	Earth Tech (U.S. Environmental Protection Agency)	Unknown	Unknown	
CASRAM-SC	See evaluation under Spills.			
DEGADIS	University of Alaska (U.S. Environmental Protection Agency)	Unknown	Unknown	
FEM3C	Lawrence Livermore National Laboratory (U.S. Army)	Unknown	Unknown	
HGSystem	See evaluation under Spills.			
HOTMAC/RAPTAD	Los Alamos National Laboratory (U.S. Air Force)	Unknown	Unknown	
INPUFF	(U.S. Environmental Protection Agency)	Unknown	Unknown	
HASCAL/SCIPUFF	Aeronautical Research Associates of Princeton (Defense Special Weapons Agency)	Unknown	Unknown	

CHEMICAL DISPERSION				
Code	Code Developer/ Geneology	Current Owner/ Technical Support	Status of SQA/V&V	General Comments
SLAB	Lawrence Livermore National Laboratory (U.S. Department of Energy)	Unknown	Unknown	
TSCREEN	See evaluation under Spills.			
VLSTRACK	Naval Surface Warfare Center (U.S. Navy)	Unknown	Unknown	This code was designed for chemical/biological munitions damage assessment. It currently lacks the capability to handle most chemicals of interest to DOE.

REFERENCES

American Nuclear Society, 1995, *Documentation of Computer Software,* ANSI/ANS-10.3-1995, La Grange Park, IL.

American Nuclear Society, 1987, *Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry*, ANSI/ANS-10.4-1987, La Grange Park, IL.

American Society of Mechanical Engineers, 1997, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*, NQA-1-1997, Subpart 2.7.

Boughton, B. and J. DeLaurentis, 1992, *Description and Validation of ERAD: An Atmospheric Dispersion Model for High Explosive Detonations*, SAND92-2069, Sandia National Laboratories, Albuquerque, NM, October.

Brereton, S., D. Hesse, D. Kalinich, M. Lazaro, V. Mubayi, and J. Shinn, 1997, *Final Report of the Accident Phenomenology and Consequence (APAC) Methodology Evaluation*, UCRL-ID-125479 APAC Methodology Evaluation Program Spills Working Group, August.

Chanin, D, J. Rollstin, J. Forest, and L. Miller, 1993, *MACCS Version 1.5.11.1 - A Maintenance Release of the Code*, NUREG/CR-6059INZ (SAND92-2146), Sandia National Laboratories, Albuquerque, NM.

Chanin, D. and M. Young, 1997, *Code Manual for MACCS2: Volume 1, User's Guide*, SAND97-0594, Sandia National Laboratories, Albuquerque, NM, March.

Defense Nuclear Facilities Safety Board, 1995, *Recommendation 95-2: Integrated Safety Management,* Washington, D.C., October 11.

DiNunno, J. J., 1995, *Fundamentals for Understanding Standards-Based Safety Management of Department of Energy Defense Nuclear Facilities*, DNFSB/TECH-5, Defense Nuclear Facilities Safety Board, Washington, D.C., May 31.

DiNunno, J. J., 1997, *Integrated Safety Management*, DNFSB/TECH-16, Defense Nuclear Facilities Safety Board, Washington, D.C., June.

Hills, C., D. Chanin, and C. Dickerman, 1998, *Validation Study of Available Models for Consideration of Explosive Releases at Pantex Plant*, Mason and Hanger Corporation Report, RPT-30 Amarillo, TX, February.

Institute of Electrical and Electronics Engineers, Inc., 1983, *IEEE Standard for Software Test Documentation,* ANSI/IEEE STD829-1983, New York, NY.

Institute of Electrical and Electronics Engineers, Inc., 1989, *IEEE Standard for Software Quality Assurance Plans*, ANSI/IEEE STD730-1989, New York, NY.

Lazaro, M., G. Melhem, D. Aldis, D. Hesse, J. Mishima, S. Mohindra, D. Price, and K. Thomas, 1997a, *Draft Explosive Event Modeling Guidance for Accident Consequence and Safety Analysis*, (Unpublished Report), APAC Methodology Evaluation Program Explosions and Energetic Events Working Group, May.

Lazaro, M., K. Woodard, S. Hanna, D. Hesse, J. Huang, J. Lewis, and C. Mazzola, 1997b, *Model Review and Evaluation for Application in DOE Safety Basis Documentation of Chemical Accidents - Modeling Guidance for Atmospheric Dispersion and Consequence Assessment*, ANL/EAD/TM-75, APAC Methodology Evaluation Working Group Program Chemical Dispersion and Consequences Working Group, September.

O'Kula, K., J. East, A. Weber, A. Savino, and C. Mazzola, 1999, *Draft Evaluation of Current Computer Models Applied in the DOE Complex for SAR Analysis of Radiological Dispersion and Consequences (U)*, (Unpublished Report), WSRC-TR-96-0126 Rev. 2, Accident Phenomenology and Consequence (APAC) Methodology Evaluation Program Radiological Dispersion and Consequence Working Group, June.

Restrepo, L., D. Hesse, D. Kalinich, V. Nicolette, W. Gregory, and R. O'Neill, 1996, *Draft Report of the Accident Phenomenology and Consequence (APAC) Methodology Evaluation*, (Unpublished Report), Accident Phenomenology and Consequence Methodology Evaluation Program Fire Working Group, April.

Spore, J., B. Boyack, W. Bohl, R. Gasser, L. Hamm, and J. Saunders, 1996, *In-Facility Transport Code Review*, LA-UR-96-2952, APAC Methodology Evaluation Program In-Facility Transport Working Group, July.

Sprung, J., L. Ritchie, and H. Jow, 1990, *MELCOR Accident Consequence Code System (MACCS), User's Guide*, NUREG/CR-4691-V1 (SAND86-1562), Sandia National Laboratories, Albuquerque, NM, February.

Steele, C., T. Wald, and D. Chanin, 1998, *Plutonium Explosive Dispersal Modeling Using the MACCS2 Computer Code*, Los Alamos National Laboratory Report LA-UR-98-1901, Los Alamos Area Office, June.

U.S. Department of Energy, 1992a, *Nuclear Safety Analysis Report*, DOE Order 5480.23, Washington, D.C., April 30.

U.S. Department of Energy, 1992b, *Computer Software Management*, DOE Order 1330.1D, Washington, D.C., May 18.

U.S. Department of Energy, 1996, *Information Management Program*, DOE Order 200.1, Washington, D.C., September.

U.S. Department of Energy, 1996, *Software Engineering Methodology*, DOE Guide 200.1-1, Washington, D.C., March.

U.S. Department of Energy, 1998a, *Operating Experience Weekly Summary July 24–July 30, 1998*, Summary 98-30, Office of Nuclear and Facility Safety, Washington, D.C., July 30.

U.S. Department of Energy, 1998b, *Quality Assurance*, DOE Order 414.1, Washington, D.C., November 24.

U.S. Department of Energy, 1998c, *Software Quality Assurance Subcommittee Meeting #22*, Software Quality Assurance Subcommittee of the Nuclear Weapons Complex Quality Managers Group, Pleasanton, CA, November 30.

U.S. Nuclear Regulatory Commission, 1975, *Reactor Safety Study - An Assessment of Accident Risks In U.S. Commercial Nuclear Power Plants*, WASH-1400 (NUREG-75 (014), Washington, D.C., October.

U.S. Nuclear Regulatory Commission, 1990, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, Volume 1, NUREG-1150, Washington, D.C.

Westinghouse Savannah River Company, 1998, *Independent Evaluation of the MACCS2 Software Quality Assurance Program,* (Unpublished Report), WSRC-RP-98-00712, August.

GLOSSARY OF ACRONYMS AND TERMS

AC	alternating current
ANSI	American National Standards Institute
APAC	Accident Phenomenology and Accident Consequence Project
ASME	American Society of Mechanical Engineers
Board	Defense Nuclear Facilities Safety Board
CAM	continuous air monitor
CIO	Chief Information Officer
COMET	Critical Experiments Machine at LACEF
CRAC	Calculation of Reactor Accident Consequence
DOE	U.S. Department of Energy
DOE/AL	Department of Energy Albuquerque Operations Office
DOE/DP	Department of Energy Office of Defense Programs
DOE/EH	Department of Energy Office of Environment, Health and Safety
DOE/EM	Department of Energy Office of Environmental Management
DoD	Department of Defense
ERAD	Explosive Release Atmospheric Dispersion
FIRAC	Fire Analysis and In-Facility Transport Computer Code
FRAM	Functions, Responsibilities, and Authorities Manual
I&C	instrumentation and control
IEEE	Institute for Electrical and Electronics Engineers
ISM	Integrated Safety Management
LACEF	Los Alamos Critical Experiments Facility
LANL	Los Alamos National Laboratory
MACCS	MELCOR Accident Consequence Code System
MACCS2	MELCOR Accident Consequence Code System 2
MCNP™	Monte Carlo N-Particle
MCNP-VISED	Preprocessor for MCNP Computer Code
MELCOR	In-Facility Transport Computer Code
NWC	Nuclear Weapons Complex
PLANET	Critical Experiments Machine at LACEF
PLC	programmable logic controller
RSICC	Radiation Shielding Information Computational Center
SHEBA	Critical Experiments Machine at LACEF
SQA	software quality assurance
SQAS	Software Quality Assurance Subcommittee
V&V	verification and validation