Peter S. Winokur, Chairman
Jessie H. Roberson, Vice Chairman
John E. Mansfield
Joseph F. Bader

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

April 18, 2012

The Honorable Donald L. Cook
Deputy Administrator for Defense Programs
National Nuclear Security Administration
U. S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0104

Dear Dr. Cook:

The Defense Nuclear Facilities Safety Board (Board) is concerned that the approach taken by Sandia National Laboratories (SNL) to implement Title 10, Code of Federal Regulations, Part 830, Subpart A, *Quality Assurance Requirements* (Rule), is insufficiently rigorous with regard to the scope and nature of the work being conducted at the Annular Core Research Reactor (ACRR). The Board's concern arises from four significant issues requiring attention: (1) lack of compliance with the requirement for independent assessments specified in the Rule and Department of Energy (DOE) Order 414.1C, *Quality Assurance*; (2) use of an inadequate quality assurance consensus standard; (3) serious deficiencies in the site procedures for safety software quality assurance; and (4) improper application of the selected software quality assurance consensus standard.

The Board's staff performed two on-site reviews of the safety basis, instrumentation and control system, and quality assurance program, including software quality assurance, for the ACRR at SNL. The Board letter to DOE dated February 28, 2012, addresses issues identified by the staff concerning the ACRR safety basis and instrumentation and control systems. The enclosed report details the quality assurance and software quality assurance issues identified during these reviews and subsequent discussions with SNL personnel.

The Board has learned that SNL personnel initiated corrections for several of the identified quality assurance and software quality assurance issues. This action is encouraging, and the Board suggests that the enclosed report may be helpful in this ongoing effort. Pursuant to 42 U.S.C. § 2286b(d), the Board requests a report and briefing within 90 days of receipt of this letter describing the plans and schedule for actions to be taken to address the issues at ACRR detailed in the enclosed report.

Sincerely,

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mr. Geoffrey Beausoleil
Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

March 7, 2012

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: W. S. Horton

SUBJECT: Quality Assurance and Safety Software Quality Assurance, Annular Core Research Reactor

This report documents issues with quality assurance (QA) and software quality assurance (SQA) related to the Annular Core Research Reactor (ACRR) at Sandia National Laboratories (SNL). The staff of the Defense Nuclear Facilities Safety Board (Board) performed on-site reviews of the safety basis, instrumentation and control systems, and QA and SQA programs for ACRR during the weeks of July 25, 2011, and November 14, 2011. Several follow-up discussions on ACRR QA and SQA occurred with SNL's technical staff and Sandia Site Office personnel in December 2011 and March 2012. This report addresses the most significant QA and SQA issues identified during the staff's reviews. A separate issue report addresses the ACRR safety basis and instrumentation and control systems.

Background. The ACRR is a Hazard Category 2 defense nuclear facility within Technical Area V (TA-V) at SNL; consequently, it follows the TA-V and SNL approaches to compliance with QA requirements. This organizational relationship is important because the staff identified shortcomings at ACRR that may affect other SNL facilities and organizations. In January 2011, TA-V personnel incorporated their existing QA program into a new Management System. The Management System consists of 16 separate programs including QA. As part of the new Management System, ACRR personnel selected two consensus QA standards to meet the requirements of Department of Energy (DOE) Order 414.1C, *Quality Assurance*: (1) American National Standards Institute/American Nuclear Society (ANSI/ANS) 15.8-1995 R2005, *Quality Assurance Program Requirements for Research Reactors* (ANSI/ANS 15.8); and (2) Part II, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*, of the American Society of Mechanical Engineers NQA-1-2000, *Quality Assurance Requirements for Nuclear Facility Applications* (Subpart 2.7).

Issues Related to the Quality Assurance Program. The Board's staff noted issues related to the QA program. The most significant issues are:

Lack of Compliance with Criterion 10, Assessment/Independent Assessment— Criterion 10, *Assessment/Independent Assessment* of Title 10, Code of Federal Regulations, Part 830, Subpart A, *Quality Assurance Requirements* (Rule), and DOE Order 414.1C impose three

requirements: plan and conduct independent assessments, establish sufficient independent authority from line management, and ensure technical qualification of assessors. The Sandia Independent Audit and Advisory Service Center (SIAASC) provides independent assessment services for SNL. During the Board's staff review, representatives of SIAASC confirmed that their assessors are not qualified in and do not base their assessments on the QA standards invoked for ACRR. Consequently, the staff is concerned that ACRR and other activities at SNL do not comply with Criterion 10 of the Rule and DOE Order 414.1C. This concern extends to SQA, as described below.

Use of Inadequate Quality Assurance Consensus Standard—The ACRR facility is authorized to house significant quantities of special nuclear material and explosives. ANSI/ANS 15.8 provides "criteria for quality assurance in the design, construction, operation, and decommissioning of research reactors," but does not provide adequate or sufficient quality assurance criteria for the scope of activities conducted in the ACRR facility. DOE Order 414.1C allows for the use of a non-NQA-1 quality standard at DOE's existing defense nuclear facilities, but requires a documented equivalency to NQA-1-2000. The staff noted that SNL personnel have not documented equivalency and have not addressed gaps between ANSI/ANS 15.8 and NQA-1-2000.

Issues Related to Software Quality Assurance. The Board's staff identified several issues related to the SQA program. The most significant of these issues are discussed below.

Improper Application of NQA-1-2000—The application of NQA-1-2000 in SNL's SQA procedures is improper:

1. Part I of NQA-1-2000 provides the requirements for establishing and executing QA programs in nuclear facilities. NQA-1-2000 Subpart 2.7 specifies the SQA requirements for computer programs used in nuclear facilities and supplements the applicable requirements of Part I of the standard. A common failure when using Subpart 2.7 is not addressing the Part I requirements that remain applicable. Subpart 2.7 explicitly requires implementation of the following Part I requirements, which were not implemented at ACRR:

    - Requirement 3, "Design Control,"
    - Requirement 4, "Procurement Document Control,"
    - Requirement 7, "Control of Purchased Items and Services,"
    - Requirement 11, "Test Control,"
    - Requirement 16, "Corrective Action," and
    - Requirement 17, "Quality Assurance Records."

2. Other requirements in Part I are not explicitly identified in Subpart 2.7, but are important and applicable nonetheless. NQA-1-2000 requires organizations to specify and comply with other applicable requirements of Part I. The staff believes ACRR failed to consider using these implied Part I requirements:

- Requirement 1, "Organization,"
- Requirement 2, "Quality Assurance Program,"
- Requirement 6, "Document Control," and
- Requirement 18, "Audits."

In the corporate SQA program document, the table mapping the NQA-1-2000 Part I requirements to the SNL corporate SQA procedures omits Requirement 18, "Audits." This omission may be a consequence of the noncompliance with Criterion 10 discussed above.

Deficiencies in Software Quality Assurance Procedures—The Board's staff noted that SQA procedures for TA-V and ACRR have improved since SNL's recent addition of a software professional to its staff. However, the Board's staff identified a number of deficiencies:

1. While TA-V and ACRR personnel identified and documented a number of computer programs as safety software as defined in DOE Order 414.1C, they failed to characterize several other computer programs as safety software, including:

   - A computer program used to aid in the design of explosive confinement, and

   - Embedded safety software (instrumented control systems have embedded software components performing safety-significant functions).

2. The SQA procedures at ACRR are an amalgamation of DOE directives, corporate policies, and diverse SQA standards. These procedures include a complex prioritization process for software used onsite. SNL personnel use the results of the prioritization process to assign a Practice Level to the software. The Practice Levels range from 0–4, with 0 being the lowest level of rigor and formality. A responsible individual, who may not have any software engineering experience or training, applies software engineering actions associated with the assigned Practice Level to the safety software. The complexity of these SQA procedures poses a challenge to SNL personnel for implementation, and to DOE personnel for review and approval, which is required by DOE Order 414.1C. Specific problems include:

   - The ACRR Safety Software Inventory, a required listing of all safety software, reflects the fact that all current computer programs are Practice Level 1, the second lowest level of rigor and formality. DOE Order 414.1C identifies and requires the application of ten different Work Activities for safety software. At Practice Level 1, there are no actions to meet the requirements for the safety software Work Activities "Procurement and Supplier Management" and "Problem Reporting and Corrective Action." In accordance with DOE directives, these two Work Activities apply to all software types at all grade levels. Consequently, the safety software procedures at ACRR and SNL are noncompliant with DOE Order 414.1C.

- In comparing the Practice Level tables of the ACRR procedures to the SNL procedures, there is a consistent reduction in Practice Levels assigned to software at ACRR. There is no documented rationale for the reduction.

- ACRRMain is a computer program loaded onto the programmable multi-axis controller (PMAC) used to operate the instrumentation and control system for the reactor. A recent failure of the PMAC highlights continuing problems with this safety software. ACRR personnel stated that the method used to correct the failure was to power down and then power up (hard reboot) the computer. ACRR personnel indicated that the cause of the failure remains unknown, and there are no ongoing efforts to identify or correct it. The Board's staff believes that for a safety significant computer system and safety software, hard rebooting to correct a failure is an inappropriate mitigation strategy and an unacceptable corrective action. ACRRMain is designated Practice Level 1 safety software so ACRR personnel were not required to apply the Work Activities "Procurement and Supplier Management" and "Problem Reporting and Corrective Action" under SNL SQA processes. As noted above, these work activities are required by DOE directives.

Conclusion. The issues described in this report concerning QA and SQA at ACRR and its parent organization demonstrate noncompliance with the Rule, DOE directives, and self-imposed consensus standards. In the aggregate, these issues challenge the assurance that structures, systems, and components or processes at ACRR will perform their safety function.