

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

**DEFENSE NUCLEAR FACILITIES
SAFETY BOARD**

Washington, DC 20004-2901



February 28, 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:

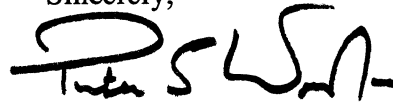
The staff of the Defense Nuclear Facilities Safety Board (Board) recently reviewed the safety basis, instrumentation and control systems, and quality assurance program (including software quality assurance) for the Annular Core Research Reactor (ACRR) at Sandia National Laboratories (SNL). The Board is concerned that the safety analysis is not bounding and that some safety systems may not be reliable enough to perform their safety functions; specific details are discussed in the enclosed report. Additional issues with quality assurance and software quality assurance will be addressed in a separate report.

The ACRR facility is authorized to store large quantities of experimental material, such as plutonium, and a moderate amount of explosives. The DSA does not evaluate operations and accidents using reasonably conservative or bounding values for these materials. Although the facility currently utilizes quantities of material that are orders of magnitude below the maximum values, the Board is concerned that the controls in place may not be adequate to protect the public and workers for the full scope of authorized operations that allow larger quantities of plutonium in the reactor cavity. Within the accident analyses of the DSA, the Board's staff noted several non-conservative assumptions applied to calculations of dose consequences. Examples of non-conservative values include those for deposition velocities, airborne release fractions, and respirable fractions. Finally, given the weaknesses associated with the ACRR safety analysis and recent sporadic occurrences involving the control system leading to uncontrolled rod motion, the Board is concerned that the reliability of the reactor protection and control systems may be inadequate.

The Board has learned that, following the recent issuance of two Potential Inadequacies in the Safety Analysis, SNL analysts embarked on a complete review of the accident analyses for the ACRR facility. This action is encouraging, and the Board suggests that the enclosed report may be helpful in this effort. Pursuant to 42 U.S.C. § 2286b(d), the Board requests a report and

briefing within 3 months of receipt of this letter describing the National Nuclear Security Administration's plans to review the accident analyses, modify the DSA, and evaluate the reliability of controls for the ACRR.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter S. Winokur". The signature is stylized with a large initial "P" and a long horizontal stroke at the end.

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mr. Glenn S. Podonsky
Mr. Richard Sena
Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

January 31, 2012

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: T. Spatz, D. Campbell

SUBJECT: Safety Basis for the Annular Core Research Reactor,
Sandia National Laboratories

This report documents a review by the staff of the Defense Nuclear Facilities Safety Board (Board) of the safety basis, instrumentation and control systems, and quality assurance program (including software quality assurance) for the Annular Core Research Reactor (ACRR) at Sandia National Laboratories (SNL). This review included two on-site discussions with SNL's technical staff and Sandia Site Office personnel during the weeks of July 25, 2011, and November 14, 2011. This report addresses issues related to the safety basis and the instrumentation and control systems for the ACRR; quality assurance and software quality assurance issues will be addressed in a separate report.

Background. SNL scientists use the ACRR to conduct radiation effects testing on weapon components and subsystems. The Sandia Site Office manager approved a major revision of the Documented Safety Analysis (DSA) for the ACRR facility in May 2007. This DSA revision was prepared using the Nuclear Regulatory Commission's (NRC) Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants*, which is the Department of Energy's (DOE) recommended safe harbor for nuclear reactors. For some chapters of the DSA, the contractor also incorporated the approach provided in DOE Standard 3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, DOE's safe harbor for nonreactor nuclear facilities.

The recent review by the Board's staff is the first comprehensive review of the DSA for the ACRR since the 2007 revision. The staff identified issues related to the technical justification for the large operating envelope authorized in the DSA. Considering the inherent risk associated with ACRR operations and sporadic operational occurrences involving the control system during the past several years, the staff is also concerned that the reliability of the safety-significant protection and control systems may be inadequate.

Issues Related to the Documented Safety Analysis. The staff believes the DSA is inadequate and does not conservatively evaluate the limits of the operating envelope. Therefore, it is not possible to determine whether the controls are adequate to ensure protection of the public and workers. Issues related to the DSA are summarized below.

Design Basis Accidents (DBAs) for Reactor Operations—The staff identified an issue with all the DBAs related to reactor operations. The most severe of these DBAs postulates significant reactor fuel melting. The issue is that the consequence analysis fails to account for the presence of experimental material-at-risk (MAR) in the central cavity during these DBAs. The DSA does not include a calculation of the amount of material that can be vaporized under DBA conditions. An administrative control limits the experimental MAR in the central cavity to 9,600 g of plutonium-239 (Pu-239) equivalent material. Another administrative control limits the material to less than 10 g Pu-239 equivalent material “when vaporization is credible.” During this review, the staff learned that “when vaporization is credible” had been intended by SNL safety analysts to mean that the experiment is *designed* to vaporize the material under normal operating conditions. The DSA does not specify the unmitigated consequences of the vaporization of quantities of material between 10 g and 9,600 g in an accident; therefore, it is impossible to determine whether the controls in place are adequate to ensure protection of the public and workers. In response, SNL personnel issued a Potential Inadequacy in the Safety Analysis on December 22, 2011.

Validation of Computer Code—The safety analysis relies on a computer code to determine the extent of fuel melting during accidents. Fuel melting would lead to significant water boiling at the surface of the fuel rods. SNL analysts failed to validate the code in that regime (where fuel melts under accident conditions). Failure to validate the code introduces uncertainty in the results. The analysts failed to report the uncertainty or error associated with the temperature calculations used to determine the extent of fuel and clad melting. The Board’s staff notes that small changes in temperature, if non-conservative, could result in more fuel and clad melting and increased dose consequences to the public and workers.

Fuel in the Storage Pool—The DSA does not contain limits on the amount of fuel in the storage pool, other than the geometric constraints of the racks in the pool. While the pool currently contains no fuel, the DSA authorizes such storage. None of the DBAs include the consequences from insults to the fuel in the storage pool.

Beyond Design Basis Accident (BDBA)—The discussion of the BDBA (seismic event with complete loss of reactor pool water) in the DSA concludes that no damage or release would occur as a result of the accident. The Board’s staff does not believe that the postulated BDBA scenario represents an appropriate BDBA for the facility. NRC Regulatory Guide 1.70 provides guidance for the analysis of BDBAs, as does DOE Standard 3009-94. The latter notes, “The [Title 10, Code of Federal Regulations, Part 830] requirement is that an evaluation be performed that simply provides insight into the magnitude of consequences of beyond DBAs (i.e., provide perspective on potential facility vulnerabilities). This insight from beyond DBA analysis has the potential for identifying additional facility features that could prevent or reduce severe beyond DBA consequences. . . . Operational beyond DBAs are simply those operational accidents with more severe conditions or equipment failures than are estimated for the corresponding DBA” (p. 54). The BDBA currently presented in the DSA is not consistent with either of these documents. It does not consider a release that exceeds that of a DBA, and it does not provide insight into the identification of facility features that could provide additional prevention or mitigation of accidents with severe consequences.

Non-Bounding Consequence Analysis—The staff identified several parameters in the consequence analysis that are non-bounding. A bounding unmitigated consequence analysis could lead to more robust controls.

- Pool release fractions—Two references used in the DSA recommend different pool release fractions.^{1,2} SNL analysts have chosen to use the less conservative pool release fractions given by Powers while offering a limited technical basis for that decision. During this review, the staff learned that SNL analysts had not considered the quantity of steam or vapor generated during the bounding DBA. Without knowledge of the quantity of steam generated by the accident, use of the less conservative pool release fraction has a weak technical basis.
- Dry deposition velocity—Powers and Restrepo provide the particle size distribution due to a postulated reactor accident. The particle size distribution following a reactor accident found in these references corresponds to a dry deposition velocity of 0.1 cm/s. This value is supported by DOE’s Office of Health, Safety and Security in Safety Bulletin 2011-02.³ SNL analysts used the less conservative value of 1 cm/s in the DSA. The staff notes the SNL analysts have not provided an adequate justification for using the less-conservative deposition velocity.
- Airborne release fraction and respirable fraction—The ACRR facility is authorized to store a large quantity of experimental MAR (20.6 kg of Pu-239 equivalent) and a moderate amount of explosives (500 g). SNL analysts calculated the consequences to the public due to the experimental MAR in the facility fire accident analysis (self-sustained oxidation of Pu metal), and applied the same consequences to the aircraft crash and earthquake accident scenarios. The staff disagrees that the airborne release fraction and respirable fraction for the facility fire are bounding for the aircraft crash and earthquake accidents. The analysis does not account for mechanical dispersion and blast effects. Also, an administrative control allows 1 g of Pu-239 to be stored contiguous with explosives in the facility. The consequence analysis does not account for this plutonium, which would yield a significantly higher airborne release fraction and respirable fraction in an explosion than it would under self-sustained oxidation. SNL analysts agreed with this observation and issued a Potential Inadequacy in the Safety Analysis on August 30, 2011.

Issues Related to the Adequacy of Reactor Controls. The staff reviewed the design criteria and safety functions for two safety-significant controls at the ACRR and identified issues associated with the reliability of each system. The Plant Protection System (PPS) is designed to

¹ D. A. Powers, *An Analysis of Radionuclide Behavior in Water Pools during Accidents at the Annular Core Research Reactor*, SAND91-1222, May 1992.

² L. F. Restrepo, *An Annular Core Research Reactor (ACRR) Postulated Limiting Event, Initial and Building Source Terms*, SAND91-0571, August 1992.

³ Safety Bulletin 2011-02, *Accident Analysis Parameter Update*, Office of Health, Safety and Security, U.S. Department of Energy, May 2011.

initiate a system scram (rapid insertion of negative reactivity) in response to high-power conditions. The Reactivity Control System (RCS) allows the operators to control the critical condition of the reactor through the movement of control rods.

Reliability of the Plant Protection System—The DSA for the ACRR invokes American National Standards Institute (ANSI)/American Nuclear Society (ANS) 15.15, *Criteria for the Reactor Safety Systems of Research Reactors*, for the design of the PPS. This standard specifies that the PPS must meet single-failure criteria and establishes additional independence requirements. The PPS, however, does not meet single-failure criteria. Specifically, it is vulnerable to a single failure of the mode select switch that could cause both PPS computer systems to bypass a scram channel simultaneously. SNL personnel justified the acceptability of this deficiency by noting that DOE Order 420.1B, *Facility Safety*, does not require redundancy for safety-significant systems (only for safety-class systems). Additionally, SNL personnel cited the exception in ANSI/ANS-15.15 that compliance with single-failure criteria is not mandatory for research reactors posing negligible risk. The staff concludes, however, that ACRR operations pose a non-negligible risk to workers and the public. This conclusion is based on the broadly defined experimental envelope for the ACRR, the potential for vaporizing of plutonium samples, allowance of the collocation of high explosives contiguous with special nuclear material, and the dose consequences of the postulated DBAs. Additionally, the approved safety analysis identifies DBAs with consequences that exceed the negligible-risk guidelines of ANSI/ANS-15.15. Therefore, the staff concludes that the PPS must fully meet single-failure criteria and independence requirements in order to comply with selected design criteria.

The DSA for the ACRR states that the control panel indications used to alert operators to the presence of a fault mitigate the significance of not meeting the single-failure criteria and independence requirements of ANSI/ANS-15.15 for the PPS. However, it does not define specific operator actions required in response to abnormal indications as part of a credited safety function.

Reliability of the Reactivity Control System—The safety-significant RCS for the ACRR was designed according to a tailored set of codes and standards that establishes design criteria to ensure that safety systems will perform their safety functions reliably. Since the Reactor Console/Rod Control Upgrade was completed in 2002, several problems with components within the RCS have arisen. Some of these problems resulted in a simple system lockup (at least five instances) with little safety impact. Others resulted in uncontrolled rod motion (at least two instances), effectively, but briefly, initiating the design basis rod withdrawal accident scenario. SNL personnel noted other deficiencies in the RCS, notably a “series of problems with the programmable multi-axis controller (PMAC)” that they characterized as “intermittent anomalies.”

Based on the observed component failure rates during the last 10 years, the staff does not consider the RCS to be sufficiently reliable to perform its safety-significant function. This assessment is supported by the following statement from the original 2005 project scope aimed at replacing the PMAC with an Allen-Bradley programmable logic controller: “The current PMAC rod control system has not demonstrated the operational reliability desired for reactor operations in the current Department of Energy climate, necessitating an upgrade to a new system with

demonstrated, improved reliability.” While system upgrades in 2006 appeared to resolve many of the issues associated with the reliability of the RCS, the recent instance of uncontrolled rod motion in 2011 indicates that the reliability of the RCS remains unsatisfactory. To date, the exact cause of the 2011 system problem remains unknown, and compensatory measures remain in place; unfortunately, these measures do not ensure improved system reliability.

Furthermore, SNL engineers have neither specified measurable criteria with which to judge the performance of the ACRR’s instrumented safety systems, nor performed a formal analysis to validate the system’s reliability. As a result, SNL analysts have failed to demonstrate that the as-built system is sufficiently reliable to perform its safety-significant functions. According to DOE Order 420.1B, “system assessments must include periodic review of system operability, reliability, and material condition.” Also, DOE Standard 1195, *Design of Safety Significant Safety Instrumented Systems Used at DOE Non-Reactor Nuclear Facilities*, recognizes and accepts methodologies used in the chemical process industry and the nuclear industry for the design and analysis of instrumented systems. For example, DOE Standard 1195 specifies ANSI/International Society of Automation (ISA)-84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, which formalizes a quantitative approach for determining target reliability goals and analyzing system reliability. For the commercial nuclear power industry, the Institute of Electrical and Electronics Engineers’ (IEEE) suite of standards defines deterministic requirements for achieving system reliability, and also identifies acceptable approaches for qualitative and quantitative analyses to provide additional confidence in system reliability. The Board’s staff notes the poor performance of the RCS presents compelling evidence of the need to consider a more formal analysis of system reliability and operability.

Adequacy of Safe Harbor Methodology. During this review, the Board’s staff determined that NUREG-1537, *Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors* (1996), may be a more appropriate safe harbor for test reactors such as the ACRR. NRC regulators use NUREG-1537 for licensing of new non-power reactors. Although the Nuclear Safety Management Rule (Title 10, Code of Federal Regulations, Part 830) provides the option of using a “successor document” to Regulatory Guide 1.70, the contractor did not exercise this option. Several of the issues related to the DSA for the ACRR could have been avoided if NUREG-1537 had been consulted at the time the DSA was developed. Given that SNL personnel have now committed to completing a review of the accident analyses and perhaps a significant revision of the DSA, it would be prudent for them to consider using NUREG-1537 as the safe harbor approach. The Board’s staff suggests it might be prudent for DOE to consider providing additional guidance to its contractors to use NUREG-1537 as the safe harbor for research and test reactors.