DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

April 8, 2008

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: F. Bamdad, T. Spatz, and J. Plaue

SUBJECT: Documented Safety Analysis for the Plutonium Facility, Los Alamos National Laboratory

This report documents a review by the staff of the Defense Nuclear Facilities Safety Board (Board) of the Documented Safety Analysis (DSA) for the Plutonium Facility (PF-4) at Los Alamos National Laboratory (LANL). The initial on-site review was performed during the week of February 4, 2008, and was followed by an assessment of the National Nuclear Security Administration's (NNSA) review of the submittal. Staff members F. Bamdad, B. Broderick, C. Keilers, C. March, C. Martin, J. McFarland, J. Plaue, and T. Spatz participated in elements of the review.

Background. PF-4 is currently operating under a final Safety Analysis Report approved in 1997 and a set of interim Technical Safety Requirements (TSRs) generated in 2005. In April 2002, the laboratory submitted its first attempt at a DSA intended to comply with Title 10 of the Code of Federal Regulations, Part 830 (10 CFR 830). The rejection of this safety basis by NNSA led to an extensive effort to develop and approve the set of interim TSRs under which the facility is operating to this day. The laboratory's second attempt at generating a 10 CFR 830 compliant safety basis for PF-4 was submitted in November 2006. In March 2007, the safety basis was reviewed by NNSA and again determined to be noncompliant with 10 CFR 830, and therefore was not approved as submitted. A set of extensive workshops was held between NNSA and the laboratory to establish an agreed-upon framework for resolution of outstanding issues in the next submittal. The third proposed safety basis was submitted to NNSA in September 2007 and is the subject of this report.

Assessment of NNSA's Review. Overall, the Board's staff determined that NNSA performed a thorough and comprehensive review of the submittal. With the exception of the issues discussed below, the observations made by the Board's staff were adequately captured by NNSA's comment set. About a third of the more than 240 comments require action prior to federal approval, and a majority of the remaining comments require an agreed-upon path to resolution in future annual updates. The Board's staff believes this represents a reasonable

approach to achieving a meaningful improvement over the current interim TSRs in the near term while explicitly directing necessary improvements in the future.

Issues in Need of Further Consideration. Several issues identified by the Board's staff were not adequately captured by NNSA's comments and warrant additional attention.

Incomplete Hazards Analysis—The hazards analysis appears to have improperly screened out several events without adequate assessment or protection of assumptions. Examples include the following:

- Hydrogen gas is generated through radiolysis in a number of aqueous processing operations; however, it is identified as a hazard only for aqueous operations involving plutonium-238. An assessment has not been performed for operations involving weapons-grade plutonium to determine whether bounding operating parameters can create conditions warranting safety-related controls.

- The DSA screens out the hazards of shock-sensitive perchlorate salt formation because "perchlorate salts are typically not allowed to dry out over time, depending on the salt and particular chemical hazard associated with it." Either this hazard needs to be analyzed or the assumed condition appropriately preserved through a TSR.

All hazards that have been screened out need to be reevaluated to ensure that the assumptions involved are captured and/or appropriate safety-related controls are identified for inclusion in the TSR.

Poor Development of Controls from the Hazards Analysis—The hazards analysis correctly identifies a number of safety-significant structures, systems, and components (SSCs) and safety management programs. However, these controls are not adequately developed in the rest of the DSA to demonstrate clearly that their credited functions provide the protection assumed in the hazards analysis. This issue is illustrated by the following examples:

- The hazards analysis credits the glovebox system as a safety-significant SSC (protective feature) for several electrocution events; however, Chapters 3 and 4 discuss no electrical safety function for the glovebox system.

- The Hazardous Material Protection Program is credited for providing worker safety during a miscellaneous fire in a casting glovebox; however, it is unclear from Chapters 3 and 8 what safety function the program is providing for this event.

The full suite of safety functions for SSCs credited in the hazards analysis ought to be discussed in Chapter 3 and associated functional requirements and performance criteria developed in Chapter 4. Likewise, specific attributes of safety management programs ought to be clearly applicable to specific hazards analysis scenarios for which the programs are credited.

A good practice would be to briefly specify these functions and attributes directly in the hazards analysis to ensure that the full range of credited safety functions is explicitly captured. NNSA's comments identified a number of examples of this problem (e.g., failure to specify certain attributes for the quality assurance, maintenance, and pressure safety management programs), but did not explicitly address the global issue.

Software Quality Assurance—Department of Energy (DOE) Guide 414.1-4, *Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance*, provides guidance on grading the approach to quality assurance for software. Under this guidance, most software associated with the development of a DSA (i.e., software whose failure could result in nonconservative safety analysis or design or misclassification of a facility or SSC) would require the highest level of grading. The laboratory's Implementation Support Document, 114-7.0, *Safety Analysis Software Toolbox*, which identifies 13 software titles for use in the development of DSAs at LANL, is inconsistent with DOE's expectations because it designates all software titles as Category 3, the lowest level. LANL defines the failure of Category 3 software as not credibly leading to death, severe injury, occupational illness, major injury, chronic impairment or occupational illness, or even to minor injury or temporary impairment or occupational illness. The only requirements for Category 3 software are its registration and completion of a risk assessment worksheet to be maintained by the software developer's group or program office. While the laboratory performed some activities beyond its requirements for some of the Category 3 software used in the PF-4 DSA, it is clear to the Board's staff that the institutional software quality assurance processes incorporated in this DSA fail to comply with relevant DOE guidance. Notwithstanding any separate improvement initiatives in this area, these weaknesses in software quality assurance ought to be identified and addressed as part of the reworking of the DSA.

Fidelity and Pedigree of DSA References—The Board's staff identified a number of instances in which references cited in the DSA either were incorrectly applied or contained inaccurate information. Examples of these problems include the following:

- Reference 3-46 is cited as the source for a respirable airborne release fraction for an accident scenario involving ceramic fuels. While the reference is appropriate for this application, the value in the reference is a factor of 3 larger than the value used in the DSA.

- Reference 4-53 is cited as providing design and set point requirements for pressure relief devices for ion exchange columns; however, the full citation at the end of the chapter is for a criticality safety standard. It was therefore impossible for the reviewer to assess the validity of this key supporting reference.

Furthermore, references that were appropriately applied often did not meet the quality assurance requirements of the laboratory's *Safety Basis Division Calculation Procedure* (IMP 114-3.0). Commonly encountered issues included no clear evidence of an independent review

and no provision of input and output files for computer-generated calculations. When questioned, laboratory personnel indicated that there were no plans to upgrade references for compliance with this directive. While NNSA identified a few instances of these types of problems, there appears to be no global path forward for ensuring the validity and technical veracity of references cited in the DSA. The Board's staff believes such a plan to meet the laboratory's implementing directive for 10 CFR 830, Subpart A, *Quality Assurance*, is needed.

Weaknesses Associated with the Leak Path Factor Calculation—The review by Board's staff of the leak path factor and associated door closure strategy revealed significant issues regarding whether the controls adequately reflect the assumptions in the modeling. While many such issues exist, the following are two examples:

- The modeling assumes that the only time there is a direct flow path between the upper control volume of the fire room and the hallway is when the doors are completely open. Once the doors are closed, it is assumed that aerosols can only escape by transport from the upper control volume into the lower control volume followed by leakage through the doors. These assumptions imply the need for TSR-level controls to ensure that the top portion of the doors cannot leak and that the leakage rate from the bottom of the door is protected in accordance with the leak rate assumed in the model.

- Similarly, the model assumes that the doors between the room experiencing a fire and the two adjoining rooms stay closed throughout the entire scenario. Unless the doors are locked, this is an unattainable expectation for control of human behavior during an emergency situation.

NNSA made several significant comments in this area; however, it is not clear that the specified actions would effectively eliminate the overreliance on a low leak path factor that is difficult to justify with appropriately high confidence. The Board's staff believes a technically defensible approach to confinement consistent with the Board's Recommendation 2004-2, *Active Confinement Systems*, needs to be specified.

Additional Opportunities to Strengthen the DSA. The Board's staff has identified the following five areas that warrant additional consideration as the DSA evolves with future updates:

Active Confinement Ventilation—There are significant efforts under way to upgrade portions of the active confinement ventilation system to safety-class to address Recommendation 2004-2, as well as improve the facility's reliability and availability to support its programmatic mission. Greater discussion of and commitment to this effort are needed in the planned improvements section of the DSA.

Chemical Exposure Thresholds—The accident analysis uses the criterion of exceeding Emergency Response Planning Guideline (ERPG)-3 at the site boundary for the identification of safety-significant controls for chemical exposure events. As standard practice, the rest of the complex uses the lower ERPG-2 threshold for this purpose. Further, use of ERPG-2 was recently codified in DOE Standard 1189, *Integration of Safety into the Design Process*.

Assumption Tracking Database—The laboratory currently has no formal system for tracking analytical assumptions from the DSA and supporting references to ensure that they are preserved and the bounding analyses protected. Such a linking database would facilitate rigorous configuration management of these assumptions, the controls identified in the DSA and the associated TSRs, and the attributes of the safety management program.

Hazards Assessment Methodology—Many of the issues identified regarding the hazards analysis could have been avoided by the application of a more methodical and comprehensive hazards analysis methodology. As the facility's technical baseline matures (i.e., as process-level drawings and flow diagrams are developed), it may be appropriate to use a methodology such as hazard and operability analysis to reassess rigorously the more complex nuclear chemical operations conducted in the facility.

Criticality Safety Program—The criticality accident analysis and related discussion do not meet the expectations of DOE Standard 3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*. Specifically, this standard recommends a systematic and methodical approach for roll-up of criticality safety controls into the DSA and TSRs. Currently, the only safety-related criticality control identified in the DSA is the criticality alarm system. In addition, the criticality safety posture of the facility is being significantly enhanced under the Program Improvement Plan. This effort ought to be referenced in the DSA.

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

April 16, 2008

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: J. Kimball

SUBJECT: Review of Chemistry and Metallurgy Research Replacement Facility

This report documents a review by the staff of the Defense Nuclear Facilities Safety Board (Board) of the Chemistry and Metallurgy Research Replacement (CMRR) facility. This onsite review was held on March 4–6, 2008, and attended by CMRR federal and laboratory project personnel and representatives from the National Nuclear Security Administration's (NNSA) Chief of Defense Nuclear Safety. The purpose of the review was to examine the status of the overall project, review the draft Preliminary Documented Safety Analysis (PDSA), and determine the design status of several safety-related structures and systems. Staff members D. Andersen, F. Bamdad, B. Broderick, R. Kasdorf, C. Keilers, J. Kimball, and J. Plaue participated in the review.

Project Background. Current plans for the nuclear facility call for the preliminary design to be complete by the last quarter of fiscal year 2008. NNSA plans to complete a technical Independent Project Review in the August/September time frame in preparation for a decision to allow the project to enter into the final design stage. The Board's staff requested that the plan for this review be provided before the review begins. In addition, project personnel are developing a plan of action, in response to a February 14, 2008, letter from NNSA's Deputy Administrator for Defense Programs that provided direction on how to proceed with the execution of the CMRR project. This plan was provided to NNSA in March 2008.

To complete preliminary design, federal project personnel will need to complete a review of both the preliminary design and the draft PDSA. The project has entered an interim design phase that will enhance aspects of the preliminary design and further develop the draft PDSA. Project personnel expect that interim design efforts will result in improved integration of the draft PDSA and safety-related System Design Descriptions. The interim design stage will also allow the project to address technical challenges, such as the structural seismic design (discussed below). The Board's staff has focused on the following issues that are critical to developing a robust design.

Federal Oversight. The Board's staff noted that greater formality and independence in federal reviews of project design documentation is needed. Department of Energy (DOE) Order 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, states that the Federal Project Director, supported by the Integrated Project Team, is responsible for project reviews and for ensuring that safety is fully integrated into the design. When discussing these responsibilities, the CMRR Federal Project Director noted that the Los Alamos Site Office (LASO) currently has no formal process for completing design reviews other than participating in design reviews conducted by the CMRR contractors. The specific reviews of the final preliminary design package to be completed by federal personnel (federal Integrated Project Team members) were not clearly presented to the Board's staff. The staff anticipates that this matter will be the subject of continued discussion in the next several months.

Design Control. The Board's staff inquired about several topics, including what steps had been taken to ensure that software used remains within the limits established by validation and verification, and whether the project was developing design analysis procedures for safety-related system design. Design analysis procedures would provide the approach to design and would describe the proper use of models prior to the models' execution. Reaching agreement on the analytical approach makes it possible to avoid having to reanalyze the design should the approach be found deficient. Project personnel responded that the software verification and validation process should establish limitations and constraints for software.

The Board's staff noted that appropriate constraints were not established for use of the MELCOR code to model leak path factors. The contractor using MELCOR developed a model well beyond that established in guidance for the code (i.e., number of control volumes used), and as a result, the staff questioned the validity of the modeling results. Prior to its review, the Board's staff provided comments on the MELCOR modeling approach and assumptions for CMRR. LASO appear not to have explicitly assessed the validity of the MELCOR model for the facility, and has agreed to perform an independent review of the modeling approach.

To date, the project has focused on the completeness of requirements and has not required that analysis methods be documented before calculations proceed. While extensive calculations exist for safety-related structures and systems, LASO review of this material will need to ensure that analytical approaches used are appropriate. The Board's staff noted that for structural and seismic analysis, the lack of a design analysis procedure has often led to significant issues during design reviews, resulting in delays. Project personnel stated that Sargent & Lundy, the contractor completing the structural design, is currently preparing a document on the structural analysis approach that should address some of these concerns.

Draft Preliminary Documented Safety Analysis. The draft PDSA uses a what-if/checklist methodology to analyze the hazards of about a dozen different operational activities at the facility. While this methodology may be adequate for the conceptual stage of the design for CMRR, a more detailed process hazards analysis needs to be performed during the

preliminary design stage to ensure that all operational hazards are identified and adequately controlled. The following weaknesses were identified by the staff and discussed with project personnel:

- The criteria used for identification of safety-significant controls for the protection of workers may be inconsistent with DOE Standard 3009-94, *Preparation Guide for U.S. DOE Nonreactor Nuclear Facility Safety Analysis Reports*. The draft PDSA limits identification of safety-significant controls to those hazards whose unmitigated consequences would result in prompt fatality or major injury to a worker; this is inconsistent with the standard's criterion of protection against potentially significant radiological or chemical/toxicological hazards as well. Project personnel claimed this was a misstatement of the methodology that was actually applied. Given the significance of this issue, the adequacy of the selection of safety-significant controls needs to be confirmed.

- The safety functions of controls identified in the hazards analysis are insufficiently developed in the draft PDSA. This weakness could have a significant impact on the design of safety-related controls, especially at this stage of the design activities. For example, gloveboxes are relied upon for confinement of hazardous materials, as well as for protection of workers from potential missiles generated by some hazardous activities. The functional and performance requirements indentified for the gloveboxes in Chapter 4 of the draft PDSA refer only to confinement capabilities and do not include protection against missiles. Proper and comprehensive identification of safety functions is important to ensure the appropriate development of functional requirements for safety systems during the preliminary design stage.

- In Section 3.3.2.3.1, the draft PDSA states, "Any high or medium risk to the public or worker that remains after the imposition of safety SSC's [structures, systems, and components] (engineered controls) will be reduced by the implementation of administrative controls in the form of SACs [specific administrative controls], key elements of safety management programs (SMPs), or SMPs themselves." This statement is inconsistent with the tenets of DOE Standard 1189, *Integration of Safety into the Design Process*, which suggests that administrative controls should be relied upon only if engineered features are not practical. For example, the fire analysis calculations supporting the draft PDSA indicate there are certain small fires (about 0.8 megawatts or less) that would not actuate the safety-class fire suppression system in this facility. Engineered features, such as smoke detection, will need to be identified, and appropriately classified, for such events.

- Several hazards have not been identified and analyzed in the hazards analysis of the draft PDSA:

  - The potential exists for a criticality accident due to actuation of the room sprinkler system and flooding of the gloveboxes. This hazard may impose additional design requirements on the gloveboxes.

  - Large quantities of chemically or toxicologically hazardous material used in CMRR are to be stored in the adjacent Radiological Laboratory facility. The hazards associated with storage of these materials need to be analyzed as potential external events warranting controls in CMRR.

  - The hazards analysis fails to address the spectrum of accidents that could impact the design and that could be initiated by facility operations (e.g., maintenance activities and programmatic operations). Project personnel envision that such hazards will be adequately controlled by safety management programs and administrative controls to be developed in the final Documented Safety Analysis. The draft PDSA ought to analyze such hazards to ensure that engineered controls—especially those that may have significant costs—are not needed in the design stage of the project, and to validate that administrative controls will be adequate to prevent or mitigate the hazards.

Recommendation 2004-2, *Active Confinement Systems.* The Board's staff reviewed the approach to active confinement in the context of the draft PDSA and the design as presented. Several events analyzed in the draft PDSA require the identification of safety-class controls because their consequences challenge or exceed DOE's evaluation guideline. The Board's staff determined that, except for gloveboxes, the project's selection of safety-class controls was consistent with the methodology set forth in DOE Standard 3009 and clarified in Appendix A of DOE Standard 1189 (i.e., appropriate safety-class controls were assigned to mitigate consequences below 5 rem total effective dose equivalent [TEDE]). The draft PDSA takes credit for reduced airborne release and respirable fractions (thereby reducing the source term and offsite dose consequences) on the basis of the gloveboxes not toppling and spilling their contents during a seismic event. As a result, this glovebox safety function requires a safety-class functional classification. The classification of the active ventilation system is safety-significant and is being designed to Performance Category (PC-3) seismic requirements to ensure that it can perform its safety function under all credited operating environments. In the context of the current design and draft PDSA, the safety-significant functional classification is appropriate and meets the intent of Recommendation 2004-2.

The project is currently completing review of the active ventilation system as required under DOE's Implementation Plan for Recommendation 2004-2. As presented to the Board's staff, the confinement ventilation system is equipped with three stages of high-efficiency particulate air (HEPA) filters at the Zone 1 discharge and two stages at the Zone 2 discharge

plenums (gloveboxes and laboratory/room areas, respectively), along with three 50 percent capacity sets of fans that are powered from three different electrical buses. Each electrical bus is connected to the two offsite power sources and the two onsite emergency diesel generators. Zone 1 and 2 portions of the ventilation system and their support systems are designed to be operational after a PC-3 seismic event.

Project-specific analyses indicate that operation of one exhaust fan for Zone 1, one exhaust fan for Zone 2, and one supply fan for Zone 2 would be adequate to maintain a cascading flow and negative pressure with respect to the atmosphere during a fire event (with one door left open for emergency response activities). To protect the HEPA filters during a fire, the current design includes a deluge system and demisters, as well as a temperature sensor in the ductwork prior to the deluge spray that would shut down active ventilation on activation. The Board's staff expressed concern about the shutdown of active ventilation during a fire as a result of this temperature sensor. The staff will review the control logic and conditions under which the active confinement ventilation system would maintain negative pressure during a fire.

Preliminary Structural Design. The Board's staff received an overview of the current structural layout of CMRR. NNSA has mandated that the laboratories of the nuclear facility have a flexible, open floor plan to accommodate as-yet unknown future missions. This "hotel concept" prevents the addition of shear walls through the laboratory wings and has resulted in major seismic design challenges. Project personnel had been using a preliminary estimate of seismic motions for the facility until Los Alamos National Laboratory (LANL) completed its update of the probabilistic seismic hazards analysis; however, they did not anticipate that the final seismic motions, particularly vertical motions, would be in resonance with various sections of the nuclear facility. The laboratory portion of the nuclear facility has been most problematic, with the fundamental frequency for the floor and ceiling matching that of the input seismic motions.

The "hotel concept" has generated seismic amplifications in the CMRR facility; it is not clear whether the facility and equipment can be designed to accommodate such demands. To reduce the vertical seismic amplifications in the CMRR structure, the facility design was altered to thicken the basemat and slabs of structure. Few walls have been added in an effort to avoid disrupting the "hotel concept" or the systems layout. This change (stiffening of the structure) responds to recommendations of LANL's structural/seismic parametric studies.

Additionally, the project currently lacks a Structural Acceptance Criteria document to guide in the design of the facility; the Board's staff believes such a document is important for a successful design and encouraged the design team to develop one. As discussed above, project personnel noted that Sargent & Lundy are in the process of preparing a document on the structural analysis approach that may address some of the issues raised by the Board's staff. The staff does not yet have a clear understanding of the structural behavior of the nuclear facility and plans to perform a detailed review of this matter in the near future.