DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

March 30, 2009

Gerald L. Talbot Jr.
Assistant Deputy Administrator for
Nuclear Safety and Operations
National Nuclear Security Administration
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Mr. Talbot:

Pursuant to the certification mandate provided in Section 3112 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, the Defense Nuclear Facilities Safety Board's (Board) staff responsible for certification activities has reviewed Chemistry and Metallurgy Research Replacement (CMRR) design data provided to date by the National Nuclear Security Administration (NNSA). The Board's staff is focusing its review on topics previously raised regarding the CMRR nuclear safety design strategy, the Preliminary Documented Safety Analysis, and design of safety-class and safety-significant systems. Those topics were provided electronically to NNSA on November 20, 2008. The Board's staff has documented specific technical issues on a Findings Form. For purposes of the certification review, the Board's staff considers a Finding a design topic related to a concern raised by the Board's staff regarding the CMRR design that has not been adequately resolved and that could preclude Board certification.

Enclosed is a Findings Form with respect to the issue of System Design Descriptions Do Not Incorporate Preliminary Documented Safety Analysis Requirements Adequately. We ask that you reply within seven calendar days from the date of Board's staff signature on the attached Findings Form, informing the Board's staff how long it will take to provide a complete NNSA response. The NNSA response should contain sufficient quantity and quality of technical information necessary for the Board's staff to determine whether the Finding can be resolved. The Findings Form contains a signature block for the NNSA individual with the authority and responsibility for addressing the Finding. Please ensure that this individual signs and dates the returned Findings Form.

Sincerely,

Roy E. Kasdorf

Roy E. Kasdorf
Nuclear Facility Design and
Infrastructure Group Lead

Enclosure

c: Mr. Mike Thompson
Mr. James McConnell
Mr. Patrick Rhoads
Mr. Herman LeDoux
Mr. Mark B. Whitaker Jr.

SEPARATION

PAGE

Board Findings
Chemistry and Metallurgy Research Replacement Facility: Congressional Certification Review

Topic: Design Control

Finding Title: System Design Descriptions Do Not Incorporate Preliminary Documented Safety Analysis Requirements Adequately

Finding: The Board CMRR certification review is evaluating the adequacy of the flow down of requirements from the Preliminary Documented Safety Analysis (PDSA) to the System Design Descriptions (SDDs). This includes SDD consistency with the PDSA and with DOE-STD-3024, *Content of System Design Descriptions*. The Board previously identified a Finding related to how the CMRR project documents and maintains design control of PDSA safety-related functions and requirements.

As stated in the introduction to DOE-STD-3024, "The SDD is a central coordinating link among the engineering design documents, the facility authorization basis, and implementing procedures." "Accordingly, the development of the SDD must be coordinated with the engineering design process and with the safety analysis development." It is critical that there is traceability between safety functions, functional requirements, performance criteria, and design requirements to ensure that the design of all safety-related structures, systems, and components is adequate. Two key attributes of the SDDs have been given in the Basis for Finding.

Review of several SDDs indicate that:

- The SDD safety functions and functional requirements are not consistent with the corresponding information in PDSA and do not have references back to the PDSA.
- In some cases PDSA functional requirements are identified as safety functions in the SDDs
- In some cases, safety functions are identified in the SDDs that are not identified in the PDSA.
- The PDSA functional requirements and performance criteria are not always included in the SDD.
- The SDD safety requirements are not consistently and explicitly correlated back to the PDSA functional requirements and performance criteria. The requirements are not sorted by importance with PDSA related requirements interspersed with requirements from other sources.
- The bases for the requirements are incomplete, with the PDSA bases behind the requirements not discussed, instead only order or standard bases related to the requirement are given. As a result the importance of the requirements cannot be determined without referencing back to the PDSA contrary to the purpose of the SDDs per DOE-STD-3024.

Attached to this Finding are several examples that document the inconsistencies discussed above. These examples are not intended to be complete, but indicate that systemic PDSA/SDD integration issues exist.

This finding is based on a review of the following SDDs: Nuclear Facility Laboratory Enclosure System (017, Rev 0A), Fire Protection System (019, Rev 0B), Uninterruptible Power Supply System (021, Rev 0B), Engine Generator System (022, Rev 0B), Security Category I Building HVAC System (029, Rev 0B), Security Category I Building (036, Rev 0B), Security Category I Vault Building (037, Rev0B), Instrument Air and Compressed Air System (045, Rev 0H), Facility Management System (048, Rev 0B), Fuel Oil System (059, Rev 0A), Electrical Power

System (062, Rev 0B), Electrical Distribution System (063, Rev 0B).
Basis for Finding: DOE-STD 3024-98, *Content of System Design Descriptions.* Section 2.1, "Statements of safety functions in the SDD shall be consistent with the corresponding information in the facility authorization basis and specific references to the authorization basis documents shall be provided." Section 3. "The safety requirements statements shall be consistent with, and be explicitly correlated back to, the corresponding statements of functional requirements and performance criteria in the facility FSAR, TSRs/OSRs, and other authorization basis documents."
Suggested Resolution or Path Forward: • **Pre-Certification:** The project must submit a plan for revising the SDDs to ensure consistency with the PDSA, including a schedule for SDD revisions. SDD revisions should be complete prior to award of the Final Design contract. • **Post-Certification:** Revise the System Design Descriptions to identify PDSA safety functions, functional requirements, and performance criteria in accordance with DOE-STD-3024 to ensure the SDDs serve their function in aiding the complete and efficient incorporation of the PDSA requirements into the final design.
NNSA Response:
DNFSB Final Resolution:

DNFSB: Roy E. Kasdorf 3/16/09 Roy Kasdorf Date	NNSA: _____ _____ Date

Attachment

CMRR PDSA and SDDs Crosswalk Comparison

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
NF Structure	1. Maintain structural integrity with expected PC-3 seismic criteria. 2. Maintains structural integrity of overhead SSCs (including anchors/supports for FSS and anchors/supports for the cranes in the storage vault) to PC-3 seismic criteria. 3. Maintain structural integrity to prevent SNM reconfiguration to a critically favorable geometry in a design basis earthquake. 4. All SS and SC fire barriers must be functional during and after a seismic event. This includes barrier around the SS diesel generator and associated switchgear rooms in the Auxiliary Building.	The latest NF SDD is Jan. 09 1. The NF shall provide horizontal and vertical load paths for accident loads. 2. The NF shall protect SC and SS SSCs from the effected of natural phenomena. 3. The Security Category I and Vault Buildings shall incorporate appropriate design measures to prevent criticality in normal operation and during and after a DBE. 4. Fire barriers covered under HVAC SDD and ENCL SDD.	1. The functional requirements do not directly align; the SDD speaks to load paths not structural integrity. SDD system functional requirements do not explicitly list PC-3. 2. The PDSA states that the crane lifting mechanism does not need to meet the safety function: the suspended load is not required to remain suspended by these performance criteria. Not clear given accident analysis requirement to protect containers. 3. The SDD interface tables do not clearly list all systems that will require in-structure spectra for seismic qualification. 4. The PDSA states that safety-related HVAC fire dampers and penetration seals will be designed to remain operational after the DBE.
Fire Protection System	1. The FPS water supply must be operational during and after a DBE.	The latest FP SDD is Jan. 09 1. There is no functional requirement in the SDD consistent with the PDSA. PC-3 design of FSS shows up under additional requirements and design requirements.	1. The PDSA performance criteria state that this includes the water supply tank, fire-water pumps, fire-water piping, and power supplies. Specific attention to SSCs that perform an active safety function is needed.

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
HEPA Filtered Active Ventilation Zones 1, 2, and 3	1. The HEPA-filtered HVAC system must be operational after a DBE by either operating in the normal Active Ventilation mode or the Reduced Flow Active Ventilation mode (Zones 1 & 2).	The latest HVAC SDD is Jan. 09 1. The Security Category I Bldg. HVAC system shall provide passive tertiary confinement during and after a PC-3 DBE. 2. The Security Category I Building shall be designed and qualified to ensure the integrity and operability to permit operation in the reduced ventilation mode following a PC-3 design basis earthquake. 3. All safety related HVAC fire barriers must be functional during and after a PC-3 DBE.	1. The PDSA states that the HVAC system must be capable of maintaining a cascading differential pressure after a DBE while operating in a reduced active ventilation mode. There is no explicit list of components to perform active HVAC functions. Functional requirements related to active confinement ventilation including what portions of the system require PC-3 seismic design need clarification. Specific attention to SSCs that perform an active safety function is needed.
Un-interruptible Power Supply	1. The UPS system must be operable during and after a DBE.	The latest UPS SDD is Jan. 09 The UPS SDD contains no functional requirements related to PC-3. However, the design requirements do state that portions of the system will be PC-3 designed.	1. The PDSA states that for most SS loads, the UPS must meet PC-2 requirements, but some of the SS loads will require PC-3 requirements. Functional requirements related to UPS PC-3 seismic design need clarification. Specific attention to SSCs that perform an active safety function is needed.
Engine Generator System	1. The EGS must be operable after a DBE.	The latest UPS SDD is Jan. 09 The EGS SDD contains no functional requirements related to PC-3. However, the design requirements do state that portions of the system will be PC-3 designed.	EGS includes generator, mechanical support systems, fuel tanks, exhaust and inlet components, electrical support systems. 1. PDSA states that 2 machines are SS PC-3 Functional requirements related to EGS PC-3 seismic design need clarification. Specific attention to SSCs that perform an active safety function is needed.

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
Electrical Power	1. Distribute power after a design basis seismic event.	The latest EP SDD is Jan. 09 The electrical power system SDD contains no functional requirements related to PC-3. However, the design requirements do state that portions of the system will be PC-3 designed.	1. The PDSA states that the SS portions of the Electrical Power System shall be capable of operating after a PC-3 seismic event. Functional requirements related to active confinement ventilation, including what portions of the electrical power system require PC-3 seismic design, need clarification. Specific attention to SSCs that perform an active safety function is needed.
Fuel Oil System	1. The Fuel Oil System will function after a design basis seismic event.	The latest FO SDD is Oct. 08 The fuel oil system SDD contains no functional requirements related to PC-3. However, the design requirements do state that portions of the system will be PC-3 designed.	1. The PDSA states that the Fuel Oil System will perform its safety functions after a PC-3 seismic event. Functional requirements related to active confinement ventilation, including what portions of the fuel oil system require PC-3 seismic design, need clarification. Specific attention to SSCs that perform an active safety function is needed.
Electrical Power	1. The Electrical Power System shall distribute offsite and onsite 480Y/277 power to SS loads. 2. The Electrical Power System shall automatically detect a loss of offsite power and switch to the onsite power source. 3. Distribute power after a design basis seismic event.	1. Same as PDSA 2. Same as PDSA 3. None	***PDSA and SDD do not align. However, design requirement for Civil and Structural include this requirement (DR.EP.1) "The Electrical Power System must supply power continuously during and after a Design Basis Seismic event. The SS portions of the Electrical Power System must meet PC-3 seismic criteria as required."

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
Engine Generator System	1. The engine generator system will start and supply electrical power to designated SS loads. 2. The engine generator system must be operable after a DBE.	1. Same as PDSA 2. None	***PDSA and SDD do not align. However, design requirement for Civil and Structural include this requirement (DR.DG.38) "The Engine Generator System must supply power continuously during and after a Design Basis Seismic event. The Engine Generator System must meet PC-3 seismic criteria as required."
Active Ventilation	HEPA-filtered ventilation airflow must be maintained to ensure cascading pressure differentials exist between confinement zones during: [F.1.4.1.1.1.1, F1.4.2.1.1.10, F1.4.2.1.1.1.2] • Normal and operational accident conditions such as facility fires, spills, etc. • Abnormal conditions (during system maintenance or in event of a single fan or component isolation damper failure or loss of a single source of offsite power) • During Reduced Flow Active Ventilation mode of operations (Zones 1 and 2 only).	**FR.HVACC.1** The Security Category I Building HVAC Systems (Zone 1, 2, and 3) shall prevent uncontrolled release of airborne radioactivity during normal operation by maintaining cascading differential pressures. **FR.HVACC.2.1.1** The Security Category I Building HVAC Systems (Zone 1 and 2) shall prevent uncontrolled release of airborne radioactivity during a complete loss of offsite electrical power by ensuring that a cascading differential pressure exists between primary confinement and the atmosphere.	The three requirement references are safety functions. Hierarchy of requirements labeled F, FR, DR, and PR are not clear due to inconsistent use. Vault requirements do not support the cascading flow FR.
	The HEPA-filtered HVAC system must be operational after a DBE [FR.HVAC.2.1.2] by either operating in the normal Active Ventilation mode or the Reduced Flow Active Ventilation mode (Zones 1 and 2 only) or in the passive confinement mode (Zones 1, 2 and 3)	**DR.HVACC.1.1.19** The Security Category I Building HVAC System shall be designed and qualified to ensure the integrity and operability to permit operation in the reduced ventilation mode following a PC-3 design basis earthquake.	FR.HVAC.2.1.2 is not referenced in the HVAC SDD. The example provided is not listed in the functional requirement section of the SDD.

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
	The HEPA-filtered HVAC system must be operational during and after design basis winds. [FR.HVAC.23]	**DR.CMRR.6.61** The HVAC system shall be protected from the effects of a design basis (PC-3) wind driven missiles.	FR.HVAC.23 is not referenced in the HVAC SDD requirement may not address pressure effects. The example provided is not listed in the functional requirement section of the SDD.
Active Ventilation (continued)	HEPA filtered HVAC system must provide passive tertiary confinement upon loss of active ventilation. [FR.HVACC.2.2]	**FR.HVACC.2** The Security Category I Building HVAC System shall provide passive tertiary confinement for public and environmental safety. **FR.HVACC.2.1.2** The Security Category I Building HVAC System shall provide passive tertiary confinement during and after a PC-3 design basis earthquake **FR.HVACC.2.3** The Security Category I Building HVAC System shall provide passive tertiary confinement during anticipated environmental conditions (temperature, wind, and precipitation). **FR.HVACC.23** The Security Category I Building HVAC PF-4 tunnel subsystem shall provide a cascading differential pressure between the PF-4 tunnel and atmosphere after a complete loss of offsite electrical power.	
	Where the HVAC ductwork penetrates SC fire barriers (e.g. Laboratory perimeter Fire Barriers (the HVAC dampers must meet the higher classification of the fire barriers to provide the safety function to prevent fire propagation consistent with the fire barrier function.	**FR.HVACC.11** All safety related HVAC fire barriers must be functional during and after a design basis earthquake (PC-3 /SC, PC-2/SS).	

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
	In addition, the following functional requirements are provided in the SDDs, but are not listed in the PDSA: **FR.HVACC.9** The Security Category I Building HVAC System exhaust airflows with the potential to contain contaminants must be injected into the stack in such a way that they are well-mixed with the bulk air stream. **FR.HVACC.7** The Zone 2 and Zone 3 bubbletight dampers shall close upon loss of ventilation air. **FR.HVACC.8** The Zone 2 and Zone 3 bubbletight dampers shall close upon trip of the exhaust fans. **FR.HVACC.18** The operable HEPA filtration unit isolation dampers shall open upon loss of electrical power. **FR.HVACC.17** The Security Category I Building HVAC System shall be capable of being manually started in reduced flow active ventilation mode after a complete loss of offsite electrical power. **FR.HVACC.19** The Security Category I Building HEPA-filtered ventilation system shall be designed to ensure an inward (to Zone 1) air flow at the most remote enclosure in the event of a glove failure, when operating in a reduced active ventilation mode. **FR.HVACC.3** The Security Category I Building HVAC System shall confine radiological hazards for worker safety.		
Facility Management System	Maintain cascading ΔPs to prevent building over pressurization and maintain confinement.	**IR.FMS.HVACC.3** The Facility Management System shall control ventilation fans to maintain differential pressures between ventilation zones as discussed in the system Sequence of Operation (SoO).	Requirement is in the Interface Requirement Section, not the FR section.
	Drive the HVAC system to passive confinement upon loss of active ventilation.	**IR.FMS.HVACC.4** The Facility Management System shall control the Security Category I Building HVAC System dampers and other components as discussed in the system Sequence of Operation (SoO).	Requirement is in the Interface Requirement Section, not the FR section.
	Protect 1st stage HEPA filters from blowout conditions.	None	No SDD requirement.

SSC	PDSA Functional Requirement	SDD Functional Requirement	Comments
	Control airflow through HEPA filter plenums to preserve filter efficiency.	None	No SDD requirement.
Facility Management System (continued)	Control temperature for rooms that contain SS SSCs as necessary to ensure equipment operability.	None	No SDD requirement.
	The FMS shall control the Fuel Oil Transfer Pumps. [IR.FMS.FO.1]	**IR.FMS.FO.1** The Facility Management System shall remotely control the FOTPs to ensure proper system operation.	Requirement is in the Interface Requirement Section, not the FR section.
	In addition, the following functional requirement is provided in the SDD, but is not listed in the PDSA: **DR.FMS.7** The safety significant portion of the Facility Management System shall meet the standards requirements for safety significant functions according to LANL Engineering Standards Manual (ESM), ISD 341-2, Chapter 8, D3060/F1050, Instrumentation and Controls (I&C) Section, Section 3.2 and Table 3-1. The safety significant portion of the Facility Management System shall be designed to be isolated from any adverse effects from the non-safety portion of the Facility Management System.		