Department of Energy
National Nuclear Security Administration
Washington, DC 20585

April 21, 2009

Mr. Roy Kasdorf
Nuclear Facility Design and
Infrastructure Group Lead
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW., Suite 700
Washington, D.C. 20004-2901

Dear Mr. Kasdorf:

This letter is in response to your March 16, 2009, letter which contained the Finding Form documenting the Defense Nuclear Facilities Safety Board's issues on the topic entitled "PDSA and Safety Strategy – Inadequate Identification of Safety-Related Controls, Functional Requirements, and Performance Criteria".

As you requested, we have completed this Form and have attached it to this letter with the applicable supporting documentation.

We look forward to continuing to work with you during your review of the design of the Chemistry and Metallurgy Research Replacement Facility (CMRR) design needed to support the Board's CMRR Certification to Congress as specified in Section 3112 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009.

If you have any questions, please contact me or have your staff contact Patrick Rhoads (202) 586-7859.

Sincerely,

Gerald L. Talbot Jr.
Assistant Deputy Administrator
for Nuclear Safety and Operations

Attachment

cc:
M. Whitaker, HS-1.1
D. Nichols, NA-2.1
J. McConnell, NA-171
M. Thompson, NA-172
H. LeDoux, LASO

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

Topic: PDSA and Safety Strategy

Finding Title: Inadequate Identification of Safety-related Controls, Functional Requirements, and Performance Criteria

Finding:

The Hazard Analysis (HA) section of the Preliminary Documented Safety Analysis (PDSA) is to identify the spectrum of hazards potentially posed by the operations, and identify an adequate set of controls to protect the public and the workers. This HA has been documented in Appendix 3B of the PDSA. It appears to be relatively comprehensive for this stage of the PDSA (the project has made a commitment to perform a process HA for the next revision of the PDSA). Appendix 3B highlights (in blue) the "safety-related" controls that are needed to protect the public or the workers from significant consequences.

Section 3.4 of the PDSA quantitatively evaluates the unmitigated consequences of major accidents from the HA, and identifies the "safety-class" (SC) controls for events potentially exceeding 5 rem Total Effective Dose Equivalent (TEDE) at the site boundary. The quantitative analysis should also evaluate the unmitigated consequences to the Collocated Workers (CLW) at 100 meters for comparison with the DOE criterion. This evaluation is not presented in this PDSA (the project has committed to provide that information in the next revision to the PDSA). Chapter 4 of the PDSA collectively lists all the safety-related controls (i.e., safety-significant (SS) structure, systems, and components (SSC) from Appendix 3B and safety-class SSCs from Section 3.4), and identifies functional requirements (FR) and performance criteria to ensure that the controls meet their intended functions.

The following deficiencies have been identified (the Attachment to this Finding provides examples for demonstration purposes only, and by no means is expected to be an all inclusive list):

(1) The set of safety-class and safety-significant controls identified in the PDSA have not been demonstrated that they will ensure adequate protection of the public and the workers.

(2) The functional requirements and performance criteria identified for safety-related controls in Chapter 4 of the PDSA do not support the credit given to them in the Chapter 3 analysis.

Basis for Finding:

10 CFR 830, 202(b): "(4) Prepare a documented safety analysis for the facility; and (5) Establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment."

10 CFR 830, 204(b)(4): "Derive the hazard controls necessary to ensure adequate protection..., demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards."

10 CFR 830, G.3: "Safety structures, systems, and component require formal definition of minimum acceptable performance in the documented safety analysis...by first defining a safety function...then placing functional requirements."

DOE O 420.1B, 3.a.(1): "(a) Safety analyses must be used to establish the identity and function of safety class and safety significant SSCs, and (b) the significance to safety of functions performed by safety class and safety significant SSCs."

Suggested Resolution or Path Forward:

- **Pre-certification:** The project must (1) submit a process plan for addressing the PDSA deficiencies, and (2) prepare a document that briefly, but thoroughly and comprehensively, describes all safety-class and safety-significant controls and their support systems that envelope the identified events in the PDSA, including its Appendix 3B. This document should also identify the functional requirements for all those SSCs, along with their performance categorization, to ensure appropriate credit can be given to them in the hazard or accident analysis. This document should be place in a configuration control system as this document will be part of the Board's certification.

  The process plan should include commitment to:

  - Revise Chapter 2 to describe safety-related SSCs and their support systems as portrayed in the SDDs and credited in the PDSA.
  - Revise Chapter 3 to include the process HA and CLW dose calculations, identify any new controls from these analyses, and implement/incorporate Board specific comments.
  - Revise Chapter 4 to capture all SS and SC controls from Chapter 3 and Appendix 3B including their support SSCs, and clearly identify the FR for all those SSCs along with their performance categorization to demonstrate the credit given to them in the hazard and accident analyses.

- **Post-certification:** Within 6 months of the certification, the PDSA must be revised to (1) address the identified deficiencies, (2) implement the results of the Process hazards analysis, (3) evaluate unmitigated dose consequences to the collocated workers, (4) incorporate the above list, as well as any new safety-related SSCs from the process HA and the CLW dose calculations, and their corresponding performance criteria and system evaluations, and (5) notification of any deviation from the above document of safety SSCs.

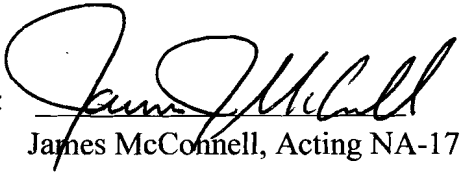
NNSA Response: The NNSA commits to completing a revision to the PDSA to ensure the safety function and functional requirement descriptions thoroughly and comprehensively describe all safety-class and safety-significant controls and their support systems that envelope the identified events in the PDSA hazard analysis scenarios (in appendix 3B). NNSA will develop internal documents that will show these relationships, which would ultimately be embedded in the PDSA Revision G4. As the work proceeds, the results of the process will be shared with the DNFSB. Similar requirements were identified in Condition of Approval 8 in the PSVR, R0.

This finding identifies two elements – first it identifies in the attachment specific examples where the documented system response to a hazard analysis scenario might not be complete. Similar comments to these were identified by the NNSA review team during the NNSA review of PDSA revision G3. The resolution of the specific set of comments included in COA 1 and 2 to the PSVR (R0) are intended to ensure the demands imposed on systems are complete. To this point, the PDSA (in multiple revisions) has been through multiple reviews with comments incorporated. The schedule for completion of the resolution of the identified issues is included in the response to DNFSB finding #3.

The second element is the adequacy and completeness of the safety function and functional requirement descriptions in the PDSA given the demands identified in the hazard analysis. The NNSA commits to performing a systematic re-evaluation of the defined safety functions and functional requirements to ensure that in a complete and comprehensive fashion, they are consistent with hazard and accident analysis as credited. This is documented in COA 8 of the PSVR.

The project team has developed a work instruction for the completion of this effort, a copy of which is attached. The schedule for the completion of this work is included in the schedule previously provided in the NNSA response to finding #3 and 5. The specific activities are included under COA 6 and 8 as we view the efforts here are linked with the commitments for consistency in the documentation of safety functions and functional requirements between the documentation within the PDSA and the implementing System Design Descriptions (SDDs).

DNFSB Final Resolution:

DNFSB: _____ _____ Roy Kasdorf Date	NNSA:  4/21/2009 James McConnell, Acting NA-17 Date

Los Alamos
NATIONAL LABORATORY
EST. 1943

CHEMISTRY & METALLURGY RESEARCH REPLACEMENT

NNSA LASO Draft PDSA Rev. G3 Preliminary Safety Validation Report Condition of Approval # 8

Document Number: CMRR-DSK-SAB-001, R0
Authorization for Use Date:
Supersedes: Initial Issue

Action		
☒ New Document	☐ Major Revision	☐ Minor Revision

Classification Review

118663	4/17/09	☐ UCNI	☐ Classified
ADC/RO Signature and Z#	Date	☐ OUO	☒ Unclassified

Marking Information / Special Instructions:

	Organization	Signature	Date
Document Owner			
Brad Gallimore SAB Manager	CMRR-SAB	Brad Gallimore	4.17.09
Approved			
Brad Gallimore SAB Manager	CMRR-SAB	Brad Gallimore	4.17.09

History of Revisions

Document Number	Effective Date	Action	Description
CMRR-DSK-SAB-001, R0	April 2009	Initial Issue	New Document

Table of Contents

1.0 Introduction

1.1 Purpose

This desktop guide serves as a layout as to how the Chemistry and Metallurgy Research Replacement (CMRR) Project will address Condition of Approval (COA) #8 from the National Nuclear Security Administration (NNSA) Los Alamos Site Office (LASO) Preliminary Safety Validation Report (PSVR) Rev. 0, issued to approve the CMRR Project Preliminary Documented Safety Analysis (PDSA), Draft, Rev. G3.

1.2 Scope

The scope of this process is to provide the information necessary to address the requested information in the LASO COA #8

1.3 Requirements

NNSA LASO, CMRR PSVR Rev. 0, COA #8.

2.0 Steps

2.1 Develop a PDSA Table 3-27 to Address COA #8 Information

This step expands the existing PDSA Table 3-37, "Summary of Safety Class and Safety Significant Controls," to provide the additional information requested by COA #8. (See Attachment 1, Example Table 3-37 with revised format and content)

Steps 2.1-2.3 are intended to be completed together. The product of step 2.1 is a table to address the LASO COA, but is dependent on data developed by steps 2.2 and 2.3.

Step	Action
2.1.1	For safety significant (SS) controls, in column 3 "Basis for Designation", provide the rationale (i.e., specific accident types) for the SS designation from the HA scenario tables developed below in step 2.2. Provide a reference to each HA scenario table in Chapter 3 (see step 2.2) or DBAs (see step 2.3) for which the safety significant designation is made.
2.1.2	For safety class (SC) controls, in column 3 "Basis for Designation", provide specific accidents from Chapter 3 PDSA, Section 3.4 (see step 2.3 below) for which the SC designation was made (per STD 3009, p 57, Section 4.3, SC SSCs).
2.1.3	For each SC and SS control, coordinate with engineering staff the validation and/or revision of the safety function and/or functional requirements to be complete for each

Step	Action
	accident or accident type referenced in step 2.1.2 and 2.1.3 above.
2.1.4	Add Performance Category (seismic), Functional Requirements, and Support Systems, Structures and Components (SSCs)/Design Features to the information in the table. Coordinate this information with the project engineering staff.
2.1.5	For each SC and SS control, coordinate with the engineering staff the identification of the specific support systems required for the identified control to perform its safety function.

2.2 Develop HA Scenario Summary Tables in PDSA Section 3.3 for each Accident Type

These are congruent to the existing Section 3.3.2.3 tables that designate controls at the SS level. These tables should provide a link to the SS controls selected for each HA scenario within the 8 accident categories listed in Table 3-37 (step 2.1). See Attachment 2, Table 3-9a, HA Scenarios for Radiological Spills (example format and content) as an example of the table to be developed for each of the 8 accident types.

Step	Action
2.2.1	Develop an HA scenario summary table for PDSA section 3.3 that is a companion to each accident type represented by existing table 3-9 through 3-16. The summary tables are to include, • Each HA scenario from Appendix 3B that has an unmitigated consequence of 'A' or 'B' for the Public, Collocated Worker, or Work for the 'accident type' being considered. • Provide a summary description for each scenario listed. • Cross check with an 'X' the SS control for each HA scenario listed. *Note*: These tables are congruent to the existing section 3.3.2.3 tables. For example, Table 3-9 is for Evaluation of Controls for Radiological Spills. Table 3-9a is proposed to be the "HA Radiological Spill Scenarios that Require SS Coverage". Tables 3-9a through 3-16a are for Radiological Spills, Chemical Spills/Fires, Radiological Fires, Radiological Explosions, Natural Phenomena, External Events, Criticality, High Radiation Accidents, respectively.
2.2.2	Work with the PDSA team lead to group the results of each table developed in 2.2.1 into similar types of accidents within the overall accident type. For example, for spills listed in Table 3-9a this could include, (1) all radiological spills outside on the loading dock, (2) spills involving glovebox enclosures, or (3) spills outside of enclosures, etc. (see example table Attachment 2).
2.2.3	Incorporate into Table 3-37 (step 2.1) the data in each table as information is available. See example format and content attached (Attachment 2)

2.3 Validate SC and SS Controls from each Design Basis Accident in PDSA Section 3.4

Step	Action
2.3.1	Validate each section 3.4 DBA, SC and/or SS control and incorporate into Table 3-37 (step 2.1).

2.4 Transfer Table 3-37 Information into the Chapter 4 Safety SSC Tables

Step	Action
2.4.1	Transfer Safety Function and Functional Requirements 'verbatim' into Chapter 4 for each SC and SS Control.
2.4.2	Coordinate with CMRR Engineering and Design Team. *Note*: This coordination may be done periodically as individual control information is available.

2.5 Update Remainder of PDSA

Step	Action
2.5.1	Update remainder of PDSA Chapters and the Executive Summary, as necessary. Consistency must be maintained throughout the updates to PDSA Chapters.

2.6 Resolve Outstanding Comments

Step	Action
2.6.1	Resolve and incorporate all open comments remaining from PDSA Rev. G3 (NNSA LASO, Technical Independent Project Review, DNFSB, Los Alamos National Security SB-DO, and CMRR Quality Assurance review), updating the SS and SC information in steps 2.1 through 2.5 as necessary.

3.0 Attachments

Attachment	Title
1	Table 3-37 in Section 3.5
2	HA Table in Section 3.3.2.3 Defense in Depth

Attachment 1
HA Table in Section 3.3.2.3 Defense in Depth

Note: **Data in columns is not complete. Table provides format and example content only**

Control Description by Safety Function	**Designation** (Performance Category)	**Basis for Designation**	**Safety Function**	**Functional Requirements**	**Support SSC(s) or DF**	**Chap. 4 Section and SDD**
Enclosure Confinement System (GB-Confine) (The enclosure confinement includesGBs, drop boxes, MTS tunnel, and maintenance enclosures)	SS Design Feature (PC-2)	HA scenarios (potential list) 1. Radiological Releases from Spills: Mitigation for HA scenarios, identified in Table 3-9a - spills inside enclosures or mechanical damage to enclosures that could result in a spill from the enclosure. 2. Hazardous Chemical Spills and fires 3. Radiological Releases from Fires 4. Radiological Releases from Explosions 5. Criticality Accidents 6. High Radiation Exposures to Workers 7. Natural Phenomena 8. External Events	Provide a confinement barrier to readily dispersible radioactive material in GBs, drop boxes, or the MTS tunnels and maintenance enclosures during normal operations. Provide mitigation to minimize the loss of confinement in enclosures during abnormal incidents involving the following: • Mechanical damage to the enclosure confinement from external and internal scenarios identified in the	Maintain confinement of dispersible radioactive materials during normal operations by maintaining a negative pressure differential and upon loss of ventilation. Maintain full or partial confinement during abnormal operational accidents identified in the HA, involving, • Mechanical damage to the enclosures The enclosure (structural) confinement system must be functional during and after a PC-2 seismic event, including any equipment within, from breaching the enclosure.	Zone 1 ACVS Seismic II/I Structural	4.4.2 S.1.7.5

		NOTE: if the consequence does not place a demand on the system, it will be listed as NONE for safety function.	HA (table 3-9a). • Fire • Explosions Provide a confinement barrier to readily dispersible radioactive material in GBs, drop boxes, or the MTS tunnels and maintenance enclosures during a PC-2 seismic event. Provide geometry that reduces the likelihood of an inadvertent criticality in an enclosure where fissile material may be present.	Enclosures that contain fissile material are to be designed to prevent inadvertent criticality through appropriate design features. Features designed to prevent inadvertent criticality shall be operable during and after a seismic event.		
Long Term Vault Crane (LTV-MM)	SC SSC (PC-3)	Design Basis Accidents • DBA 3.4.2.13 Seismic Event • DBA 3.4.2.14 Seismic with Fire	Provide structural support to overhead utilities or equipment that can cause insult to radioactive material sources. (Part of two-over-one protection.)	Maintains structural integrity of overhead SSCs (including anchors/supports for the FSS and anchors/supports for the cranes in the storage vaults) to PC-3 seismic criteria.	Facility Structure	4.3.2 S.1.2.1 S.1.20.4

Attachment 2
HA Table in Section 3.3.2.3 Defense in Depth

Table 3-9a HA Radiological Spill Scenarios That Require SS Control Coverage[1]

Note: table is not complete. Only used for example of format/content

HA Scenario #	Description	Structure	Enclosure Confinement	ACVS Z1	ACVS Z2	ACVS Z3	ACVS PF-4 Tunnel	PCVS	LTV Container	STV container	TRU Containers	Large vessel	ARDS	STV Storage Design	LTV Storage Design	Seismic Qual (II/I)	SAC-LTV Cooling	SAC-LTV Heat	SAC-No HE residual in LV
Accidents Outside GBs that Impact Containers																			
TO-001 TO-047	Forklift impacts container, cryogen spill fails containers in PF-4 tunnel						X	X	X	X	X		X						
TO-006 TO-007 TO-013	FL incident, Door Impacts Containers, Personnel drops container > 10 ft.				X	X		X	X	X	X		X						
TO-072	LV falls while moving, falls through to basement or down elevator	X			X	X		X			X	X							
TO-063	FL impacts ductwork/SNM spill							X	X	X	X		X						

[1] Scenarios with P, CW, and W consequences in HA Bins 'A' or 'B' are judged to challenge the evaluation guidelines and require consideration of SS controls.

HA Scenario #	Description	Structure	Enclosure Confinement	ACVS Z1	ACVS Z2	ACVS Z3	ACVS PF-4 Tunnel	PCVS	LTV Container	STV container	TRU Containers	Large vessel	ARDS	STV Storage Design	LTV Storage Design	Seismic Qual (II/I)	SAC-LTV Cooling	SAC-LTV Heat	SAC-No HE residual in LV
Accidents With Spills from Enclosures																			
MTS-001, 013	Trolley malfunction (spill), MTS failure		X	X				X					X						
MTS-003, 007, 009 NFL-014	Forklift strikes trolley, Gas bottle missile, overhead equipt/component drop (causes MTS/GB breaches) Equip failure/fragments, Gas cylinder missile (GB Breaches)	X	X	X	X			X					X						
MTS-005	MTS drop > 10 ft	Remainder of table to be completed																	
MTS-018	Container failure (high pressure)																		
LVA-002	LV falls off skid/pallet with floor failure																		
LVA-006	LV port damage during GB connection																		
LVA-008	Overhead equip falls																		

HA Scenario #	Description	Structure	Enclosure Confinement	ACVS Z1	ACVS Z2	ACVS Z3	ACVS PF-4 Tunnel	PCVS	LTV Container	STV container	TRU Containers	Large vessel	ARDS	STV Storage Design	LTV Storage Design	Seismic Qual (II/I)	SAC-LTV Cooling	SAC-LTV Heat	SAC-No HE residual in LV
	onto LV area																		
NFL-001, 004, 016, 020, 034, 038, 049 LVA-014, LVA-016	Container failure in GB, Operator spills SNM inside/outside GB, GB failure (pressure), Cryogenic spill/SNM impacted,																		
NFL- 018, 057	Container failure in Open Front, Operator spills SNM in Open front, Glove breach in GB (no spill)																		
NFL-022 SVS-006	NDA or Vault shelving falls																		
MM-001	Container fails (pressurized)																		
MM-003, 007, 009, 011, 041, 043, 047, 050	Equip failures impact SNM in MM room, Material spills inside GB or outside, forklift incident, GB failure, loss of power leads to container drop																		

HA Scenario #	Description	Structure	Enclosure Confinement	ACVS Z1	ACVS Z2	ACVS Z3	ACVS PF-4 Tunnel	PCVS	LTV Container	STV container	TRU Containers	Large vessel	ARDS	STV Storage Design	LTV Storage Design	Seismic Qual (II/I)	SAC-LTV Cooling	SAC-LTV Heat	SAC-No HE residual in LV
TO-064	FL impacts duct in basement/SNM spill								X	X	X		X						
TO-015 TO-023	Elevator drops (containers)					X		X	X	X	X								
TO-021	Worker drops container					X		X	X	X									
TO-034	Container failure (LP venting),			X	X			X	X	X	X		X						
TO-049 TO-059	RLUOB tunnel container failure, FL impacts container in tunnel									X	X								
TO-057, 065	Vehicle impacts NF, Vehicle drives over LTV (bldg failure) – building failure	X							X	X				X	X				
Accidents With Spills Outside (Dock Area)																			
TO-068 TO-071	Truck/FL impacts LV in yard, LV falls											X							
TO-011	Door (exterior) impacts containers										X								
TO-055	Firearm Discharge (dock)										X	X							X

HA Scenario #	Description	Structure	Enclosure Confinement	ACVS Z1	ACVS Z2	ACVS Z3	ACVS PF-4 Tunnel	PCVS	LTV Container	STV container	TRU Containers	Large vessel	ARDS	STV Storage Design	LTV Storage Design	Seismic Qual (II/I)	SAC-LTV Cooling	SAC-LTV Heat	SAC-No HE residual in LV
MM-005, 013	Gas Cylinder missile, Forklift																		
MM-023	Container (drum) fail																		
LVS-001, 005, 006, 007, 008	LTV crane incident/spill, Forklift incident, container falls, cranes drops container(s)																		
LVS-002, 003, 012, 019, 022 SVS-002, 004, 010	LTV hand tool container breach, container failure in storage, cryogenic spill																		
LVS-004	Container drops into stairwell																		
LVS-011	Container overpressure																		
LVS-020 SVS 015	Loss of LTV cooling																		
LVS-023 SVS-005	Gas cylinder missile																		
SVS-001,	STV container drops, container																		

HA Scenario #	Description	Structure	Enclosure Confinement	ACVS Z1	ACVS Z2	ACVS Z3	ACVS PF-4 Tunnel	PCVS	LTV Container	STV container	TRU Containers	Large vessel	ARDS	STV Storage Design	LTV Storage Design	Seismic Qual (II/I)	SAC-LTV Cooling	SAC-LTV Heat	SAC-No HE residual in LV
009, 014, 017	failures, Pneumatic hand tools/compressed air																		
SVS-003	Container failure																		
LVS-021 SVS-016 LVA-012 NFL-036, 040 MM-039 SRW-032	Service line failure (Contamination)																		
LVS-027 SVS-021 MM-052 NFL-055 MTS-028 LVA-022	Firearm																		
SRW-018	Waste drums container failure																		