Department of Energy
Washington, DC 20585

April 18, 2018

MEMORANDUM FOR DISTRIBUTION

FROM: WILLIAM A. ECKROADE W. A. Eckroade
ACTING DIRECTOR
OFFICE OF ENTERPRISE ASSESSMENTS

SUBJECT: *Office of Enterprise Assessments Lessons Learned from Assessments of Safety into Design of New U.S. Department of Energy Nuclear Facilities – April 2018*

The U.S. Department of Energy (DOE) independent Office of Enterprise Assessments (EA) conducted a series of assessments at DOE high-hazard (Hazard Category 2) nuclear facility design and construction projects between 2012 and 2017. These projects were under the direction of the DOE Office of Environmental Management and the National Nuclear Security Administration. The objective of these assessments was to examine the integration of safety into the design, as well as the development of the safety design basis for the new nuclear facilities, thereby protecting the worker, the public, and the environment, and to disseminate effective management practices and lessons learned throughout the DOE Complex. The new nuclear facilities projects were selected based on the priorities outlined in DOE Order 227.1A, *Independent Oversight Program*.

Findings and observations related to the integration of safety into the design and development of safety design basis from those reports were extracted and condensed to create a summary of contractor and DOE field element performance. This lessons learned report focuses on issues that affect multiple sites and/or facilities and identifies both best practices and areas of weakness as well as recommendations, with the goal of promoting organizational learning and increased performance.

Further details on individual site/facility reports are available at the following link: **https://energy.gov/ea/services/assessments/environment-safety-and-health-assessments/review-reports**

If you have any questions, comments, or feedback, please contact me at (202) 287-5403. Alternatively, your staff may contact Thomas Staker, Director, Office of Environment, Safety and Health Assessments, at (301) 903-5392.

Attachment: *Office of Enterprise Assessments Lessons Learned from Assessments of Safety into Design of New U.S. Department of Energy Nuclear Facilities – April 2018*

cc: Dan R. Brouillette, DS
Lisa E. Gordon-Hagerty, US
Mark W. Menezes, US
Paul M. Dabbar, US

Office of Enterprise Assessments Lessons Learned from Assessments of Safety into Design of New U.S. Department of Energy Nuclear Facilities – April 2018

Joseph Olencz, AU-1.1
Patricia R. Worthington, AU-10
Garrett A. Smith, Jr., AU-31
Todd A. Shrader, CB
Bryan C. Bower, CC
Dae Y. Chung, EM-3
Joceline M. Nahigian, EM-2.1
James A. Hutton, EM-3.1
Gordon C. Langlie, Jr., EM-3.114
John A. Mullis, EM-90
Douglas E. Hintze, EM-LA
Steven E. Winberg, FE-1
Mark J. Matarrese, FE-7
W. Ike White, NA-1
Stephanie P. Duran, NA-1.1
Steven C. Erhart, NA-1.1
Robert M. George NA-233
James J. McConnell, NA-50
Patrick T. Cahalane, NA-50
Daniel Sigg, NA-51
Gregory P. Hatchett, NA-51
Jeffry L. Roberson, NA-51
Geoffrey L. Beausoleil, NA-NPO-1
Mark L. Holecek, NA-KC
W. Steve Goodrum, NA-LA
Peter D. Rodrik, NA-LL
Jeffrey P. Harrell, NA-SN
Steven J. Lawrence, NA-NV
N. Nicole Nelson-Jean, NA-SV
Edward G. McGinnis, NE-1
Raymond V. Furstenau, NE-1
D. Craig Welling, NE-1
Tracey L. Bishop, NE-3
Dennis M. Miotla, NE-20
Richard B. Provencher, NE-ID
Robert D. Boston, NE-ID
Brian T. Vance, ORP
Robert E. Edwards III, PPPO
Doug S. Shoop, RL
J. Steve Binkley, SC-2
Joseph A. McBrearty, SC-3
Cynthia K. Baebler, SC-AMSO

Office of Enterprise Assessments Lessons Learned from Assessments of Safety into Design of New U.S. Department of Energy Nuclear Facilities – April 2018

Joanna M. Livengood, SC-ASO
Frank J. Crescenzo, SC-BHSO
John D. Greenwood, SC-CH
Michael J. Weis, SC-FSO
Kenneth R. Tarcza, SC-OR
Johnny O. Moore, SC-OSO
Roger E. Snyder, SC-PNSO
Peter O. Johnson, SC-PSO
Paul M. Golan, SC-SSO
Joseph Arango III, SC-TJSO

Office of Enterprise Assessments
Lessons Learned from Assessments of Integration of Safety into Design of New U.S. Department of Energy Nuclear Facilities

April 2018

Office of Nuclear Safety and Environmental Assessments
Office of Environment, Safety and Health Assessments
Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

Acronyms

CFR	Code of Federal Regulations
CRAD	Criteria and Review Approach Document
CSDR	Conceptual Safety Design Report
DNFSB	Defense Nuclear Facilities Safety Board
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
EA	DOE Office of Enterprise Assessments
ECRTS	Engineered Container Retrieval and Transfer System
FSS	Fire Suppression System
HSS	DOE Office of Health, Safety and Security (predecessor of EA)
LAWPS	Low Activity Waste Pretreatment System
MAR	Material-at-risk
NNSA	National Nuclear Security Administration
PDSA	Preliminary Documented Safety Analysis
PSDR	Preliminary Safety Design Report
PSVR	Preliminary Safety Validation Report
SAC	Specific Administrative Control
SDS	Safety Design Strategy
SER	Safety Evaluation Report
SSC	Structure, System, and Component
STP	Sludge Treatment Project
SWPF	Salt Waste Processing Facility
TSR	Technical Safety Requirement
UPF	Uranium Processing Facility
WTP	Waste Treatment and Immobilization Plant

Office of Enterprise Assessments
Lessons Learned from Assessments of Integration of Safety into Design of New U.S. Department of Energy Nuclear Facilities

EXECUTIVE SUMMARY

The U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments, within the independent Office of Enterprise Assessments (EA), conducted assessments at DOE high-hazard (Hazard Category 2) nuclear facility design and construction projects between 2012 and 2017. These projects were under the direction of the DOE Office of Environmental Management and the National Nuclear Security Administration. The objective of these assessments was to examine the integration of safety into the design, as well as the development of the safety design basis for the new nuclear facilities. A disciplined safety-in-design approach ensures that the required level of safety is integrated early into facility design, so that undue project delays and cost increases can be prevented. The safety design basis leads to the facility's final safety basis, which comprises the documented safety analysis and technical safety requirements. An adequate safety basis provides reasonable assurance that the facility can be constructed and operated in a manner that adequately protects workers, the public, and the environment.

This lessons learned report focuses on safety design basis development issues that potentially affect multiple nuclear facility projects at different DOE sites, and identifies strengths and weaknesses, best practices, and recommendations, with the goal of promoting organizational learning. The lessons learned are based on analyzing and grouping significant observations from EA assessments in the following three fundamental aspects of safety-in-design integration and safety design basis development: (1) hazard and accident analyses; (2) hazard control selection; and (3) safety functional and performance requirements.

Overall, EA found that safety design basis development efforts at most new nuclear facility projects adequately integrated safety into design through following the structured processes defined in DOE directives. Stronger programs existed at facilities that adhered more closely to the principal DOE standard, DOE-STD-1189, *Integration of Safety into the Design Process*. Close coordination and interaction between the DOE field element and the project's nuclear safety and design teams from project inception also contributed to successful projects. Further, the integration of design engineering and nuclear safety basis activities within a single contractor organization was a best practice that contributed significantly to high quality and consistency in the safety design basis and engineering documents. EA also identified other best practices. One project performed thorough engineering design analyses to provide a sound technical basis for its safety systems. At another project, the nuclear criticality safety evaluations and the selection of controls to prevent criticality accidents were completed in an exemplary manner.

EA also observed weaknesses in each of the three broad technical areas of safety design basis development mentioned above. The assessments found several instances of insufficient hazard and accident analyses, including some weaknesses in implementing hazard analysis methodology for analyzing relatively complex processes. EA also found incomplete or inadequate identification of candidate hazard controls, incorrect safety functional classification of selected controls, and misapplication of the design criteria for safety structures, systems, and components.

While the issues identified by internal and external organizations, including those by EA, were being adequately resolved at the facilities, the lessons learned provide a basis for several recommendations. Notably, a number of these recommendations identify the need for close communication and coordination throughout the project among the groups responsible for developing the safety basis and safety design:

- The safety design strategy (SDS), a key requirement of DOE-STD-1189, is an important document that provides an early, detailed approach to developing the integrated safety design. This approach should be closely coordinated to achieve a consistent method for implementing the SDS throughout the design process and minimizing design changes later in the design and construction of the facility.

- In building the nuclear facility project organization, organizational designs that facilitate and encourage close coordination and integration of the safety basis analysts with the design and process engineers during all phases of the project enhance the final safety design and should be a key consideration.

- Interactive review of the safety functions, functional requirements, and performance criteria of safety structures, systems, and components by the cognizant design and process engineers throughout the safety analysis and design phases is essential to ensure that safety performance criteria are adequately understood, translated into appropriate design criteria, evaluated in the safety basis, and protected by maintenance and surveillance requirements.

- Timely coordination between developing the fire hazards analysis and the safety design basis documents at various design phases is important to ensuring that key information, such as postulated fire scenarios, hazard controls, and the facility interfacing systems, is consistent in both sets of documents.

Office of Enterprise Assessments
Lessons Learned from Assessments of Integration of Safety into Design of New U.S. Department of Energy Nuclear Facilities

1.0 INTRODUCTION

The U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments, within the independent Office of Enterprise Assessments (EA), conducted targeted assessments at DOE high-hazard (Hazard Category 2) nuclear facility design and construction projects between 2012 and 2017. These assessments examined the integration of safety into the design, as well as the development of the safety design basis for the new nuclear facilities. The nuclear facility projects were under the direction of the DOE Office of Environmental Management and the National Nuclear Security Administration (NNSA). The objective of each assessment was to evaluate the development of an adequate safety design basis, in accordance with DOE's nuclear safety requirements, prior to construction and operation of the nuclear facility.

The safety design basis for new nuclear facilities includes the conceptual safety design report (CSDR), preliminary safety design report (PSDR), and preliminary documented safety analysis (PDSA), which are prepared at successive design phases. These documents are steps towards the facility's final safety basis, which comprises the documented safety analysis (DSA) and technical safety requirements (TSRs). DOE's review and approval of the safety design basis documents for nuclear facilities provides reasonable assurance that the safety design basis is sufficient for proceeding to the next phase of design or construction. An adequate safety basis provides reasonable assurance that the facility can be constructed and operated in a manner that adequately protects workers, the public, and the environment. A major purpose of EA's assessments of safety design basis development *during* the design and construction of a high-hazard nuclear facility was to provide oversight of DOE's efforts to ensure that the required level of safety is integrated early into facility design, so that undue project delays and cost increases could be prevented.

This lessons learned report is based on a collective analysis of EA's assessments of safety design basis development. It focuses on issues that potentially affect multiple new nuclear facility projects at different DOE sites, and identifies both areas of strengths and weaknesses (Section 2) and best practices (Section 3), with the goal of promoting organizational learning. This report also provides recommendations (Section 4) for consideration by DOE field elements and contractors managing new nuclear facility projects.

1.1 Background

EA manages the Department's independent oversight program. This program is designed to enhance DOE safety and security programs by providing the Secretary and Deputy Secretary of Energy, Under Secretaries of Energy, other DOE managers, senior contractor managers, Congress, and other stakeholders with an independent evaluation of the adequacy of DOE policy and requirements implementation; the effectiveness of DOE and contractor line management performance and risk management in safety and security; and other critical functions, as directed by the Secretary. The DOE independent oversight program is described in and governed by DOE Order 227.1A, *Independent Oversight Program*. EA implements the program through a comprehensive set of internal protocols and assessment guides.

DOE Order 227.1A states that:

> *"Independent Oversight appraisals must be prioritized on areas of greatest potential risks and implemented in a manner that supports DOE line management in accomplishing its line management oversight and achieving DOE mission objectives safely and securely. Higher priority and greater emphasis is placed on conducting Independent Oversight appraisals of high consequence activities, such as* ***nuclear project design, construction and commissioning; high hazard nuclear operations****;…"* [Emphasis added.]

EA enhanced its oversight of high-hazard nuclear facilities under design and construction after Congress, in the Appropriations Act of fiscal year (FY) 2012 and of each subsequent year, made the continued annual funding for such facilities contingent upon EA's oversight. This provision in the Appropriation Act for FY 2017 (PL. 244-187, Section 303) states:

> *"None of the funds made available in this title shall be used for the construction of facilities classified as high-hazard nuclear facilities under 10 CFR Part 830 unless* ***independent oversight is conducted by the Office of Enterprise Assessments*** *to ensure the project is in compliance with nuclear safety requirements."* [Emphasis added.]

EA accomplishes this portion of its mission by conducting technical assessments designed to provide assurance that contractor organizations are appropriately implementing DOE nuclear safety requirements and national consensus standards. EA developed Protocol-EA-31-02, *Office of Environment, Safety and Health Assessments Protocol for High-Hazard Nuclear Facility Project Oversight*, which establishes the requirements and responsibilities for managing and conducting EA's independent oversight of high-hazard nuclear facility projects. The term "high-hazard" used in the legislation and elsewhere does not have a formal definition in DOE standards; however, the term generally is understood to refer to DOE Hazard Category 1 and 2 nuclear facilities (defined in DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*), which have the potential for significant onsite consequences of accidents. To the extent feasible, EA conducts its appraisals concurrent with line management oversight assessments to maximize the effectiveness of its oversight activities and minimize the impact on project organizations.

1.2 Scope and Methodology

This report reflects an analysis of the collected results of EA's assessments and other oversight reviews of safety design basis development at seven new high-hazard (Hazard Category 2) nuclear facility projects at four DOE sites. The sites and facilities assessed, along with the responsible contractors, local DOE offices, and DOE Headquarters program offices, are listed in Table 1. The table also indicates the types of safety design basis documents reviewed for each facility. The oversight reports published by EA and its predecessor organizations from December 2012 through December 2017 are listed in Appendix B.

Table 1
Nuclear Facilities, Contractors, DOE Program Offices, and DOE Field Offices in the Assessment

Assessment Site	Nuclear Facility Project and Safety Design Basis Document Type *	Contractor	DOE Headquarters Program Office	DOE Field Element
Hanford Site	Tank Farms Low Activity Waste Pretreatment System (LAWPS) PSDR/preliminary safety validation report (PSVR)	Washington River Protection Solutions, LLC	Office of Environmental Management	Office of River Protection
Hanford Site	Waste Treatment and Immobilization Plant (WTP) - High Level Waste Facility hazard analysis report (HAR), PDSA/safety evaluation report (SER)	Bechtel National, Inc.	Office of Environmental Management	Office of River Protection
Hanford Site	WTP - Low Activity Waste Facility HAR, PDSA/SER	Bechtel National, Inc.	Office of Environmental Management	Office of River Protection
Hanford Site	Sludge Treatment Project - Engineered Container Retrieval and Transfer System (STP-ECRTS) PDSA	CH2M Hill Plateau Remediation Company	Office of Environmental Management	Richland Operations Office
Los Alamos National Laboratory	Transuranic Waste Facility PDSA/SER, DSA/TSR	Los Alamos National Security, LLC	NNSA	NNSA Los Alamos Field Office
Savannah River Site	Salt Waste Processing Facility (SWPF) PDSA, DSA/TSR	Parsons Corporation	Office of Environmental Management	SWPF Project Office of the Savannah River Operations Office
Y-12 National Security Complex	Uranium Processing Facility (UPF) PSDR/PSVR, PDSA/SER	Bechtel National, Inc.	NNSA	NNSA Production Office

* Refer to the list of acronyms for the name of the type of safety design basis document.

The individual EA assessment reports were "snapshots" of the status of DOE contractors' efforts, at the time of the assessment, towards developing the safety design basis for their facilities. EA strategically engaged at different phases of development of safety design bases for the selected facilities. At some

facilities, EA reviewed successive revisions of certain safety design basis documents, such as the PSDR and PDSA. EA assessments also included reviews of hazard analysis activities for different processes and safety systems. However, EA's program of assessments was not intended to cover all aspects of safety design basis development at each new nuclear facility project. Also, since the development effort reflected work in progress (draft documents) subject to ongoing internal contractor and DOE reviews, EA selectively reviewed DOE field offices' safety design basis review reports.

The scope of the assessments at each facility was guided by an appropriately tailored EA Criteria and Review Approach Document (CRAD), supplemented as necessary by selected aspects of EA CRADs in related functional areas. Example CRADs are listed below:

- CRAD 31-1, *Hazard Analysis*
- CRAD 31-2, *Preliminary Documented Safety Analysis*
- CRAD 31-07, *New Nuclear Facility Documented Safety Analysis and Technical Safety Requirements*
- CRAD 31-29, *Review of Nuclear Facility Preliminary Safety Basis Development*
- CRAD 45-34, *Fire Protection*
- CRAD 64-19, *Engineering Design and Safety Basis*
- CRAD 45-18, *Criticality Safety Controls Implementation*.

EA used the criteria and approaches in these CRADs to determine whether the draft safety design basis documents met DOE requirements for technical adequacy in the areas examined. The assessments generally focused on the following areas of safety-in-design integration and development of the facility's safety design basis: identification and evaluation of hazards; analysis of postulated accidents; derivation of hazard controls, including safety structures, systems, and components (SSCs) and specific administrative controls (SACs); and description and evaluation of the safety functional requirements and performance criteria for safety SSCs and SACs.

The EA assessments of safety design basis development for the new nuclear facilities did not include certain other aspects of integration of safety in design, such as the safety design strategy (SDS), project management aspects (e.g., responsibilities of the integrated project team and the safety design integration team), project risk and opportunities assessment, engineering design process, and configuration management. Results of EA assessments of engineering design process and configuration management, and the lessons learned from those assessments, are documented separately in *Office of Enterprise Assessments Lessons Learned from Assessment of Engineering Process at U.S. Department of Energy Nuclear Facilities*, August 2017.

In the overall assessment discussed in Section 2 below, the collective analysis and summary is based on the generic safety significance of issues identified from individual EA assessments, regardless of the stage of safety design basis development or how the issue was designated and reported. The designation of issues in EA assessments (e.g., findings, potential concerns, deficiencies, or comments for resolution) generally depended on the stage of the project's safety design basis documentation under review. Further, the EA assessment reports provided to the assessed organizations may have resulted in corrective actions or enhancements that are not reflected in this report.

1.3 Requirements and Guidance

The nuclear safety requirements for DOE nuclear facility projects flow down from Title 10, Part 830 of the U.S. Code of Federal Regulations (10 CFR 830), *Nuclear Safety Management*. DOE's regulations for developing the PDSA, DSA, and TSR for new nuclear facilities are provided in 10 CFR 830 Subpart B - *Safety Basis Requirements* and its Appendix A, *General Statement of Safety Basis Policy*. These

regulations specify that a contractor responsible for a DOE nuclear reactor facility may prepare the DSA in accordance with DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, commonly referred to as a "safe harbor." Although this standard was significantly revised in 2014, all new nuclear facility projects addressed in this report followed the 1994 version (and applicable change notices) of the standard.

The integration of safety into the design of new nuclear facilities, starting early and continuing throughout the design process, is required and emphasized in DOE Order 413.3B (2010), *Program and Project Management for the Acquisition of Capital Assets*, and is also specified in DOE Order 420.1C (2012), *Facility Safety*. These orders mandate the use of the safety-in-design principles and concepts described in DOE-STD-1189-2008, *Integration of Safety into the Design Process*, throughout the facility design process. This standard specifies the approach for integrating specific project management, design process, and safety design basis development activities. It also requires developing pertinent safety design basis documents, including the CSDR, PSDR, PDSA, and DSA, as well as corresponding DOE approval reports, namely the conceptual safety validation report, PSVR, and SERs for the PDSA and the DSA, respectively. In particular, the integration of design into safety design basis development requires hazard analysis and associated hazard control selection to be performed and updated iteratively with increasing levels of design detail, starting from the facility level at the conceptual design phase, proceeding through the process or system level at the preliminary design phase, and continuing to the component level at the final design phase.

DOE Order 420.1C (2012) establishes the design and construction requirements for new DOE Hazard Category 1, 2, and 3 nuclear facilities (and for major modifications of such existing facilities). EA assessments took into consideration that for some projects, contractors were contractually obligated to comply with the previous revision, DOE Order 420.1B (2005). Both versions of DOE Order 420.1 provide facility and programmatic safety requirements for nuclear safety design, fire protection, criticality safety, natural phenomena hazards, and system engineering, which are areas of major importance to the safety of nuclear facilities. DOE Order 420.1B/C also establishes specific requirements for the design and construction of safety SSCs by identifying an applicable set of industry codes and standards, as well as other DOE directives and standards. Numerous DOE standards, including those that pertain to the safety basis functional areas stated above, support DOE nuclear safety regulations and orders; these standards include DOE-STD-1066, *Fire Protection*; DOE-STD-3007, *Guidelines for Preparing Criticality Safety Evaluations at DOE Non-Reactor Nuclear Facilities*; DOE-STD-1020, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities*; and DOE-STD-1186, *Specific Administrative Controls*.

The focus of the DOE nuclear safety regulations, requirements, and guidance mentioned above is on developing a sound foundation for the safety design basis of a nuclear facility, which includes thorough and comprehensive hazard and accident analyses coupled with the selection of appropriate hazard controls. These aspects were also the focus of EA's targeted assessments of safety design basis development and of this lessons learned report.

2.0 OVERALL ASSESSMENT

The lessons learned in developing the safety design basis of new nuclear facilities are based on analyzing and grouping significant observations from EA assessments according to the following three fundamental aspects:

- Hazard and accident analyses
- Hazard control selection

- Safety functional and performance requirements

Overall, EA observed that safety design basis development efforts at the facilities assessed were proceeding in accordance with DOE requirements and guidance. Instrumental to the DOE contractors' efforts were standards DOE-STD-3009-94 and DOE-STD-1189-2008. Several nuclear facility projects closely followed the latter (safety-in-design standard) to successfully implement effective processes to integrate project management, design engineering, and safety design basis development. EA found stronger programs at facilities that adhered closely to these and other related standards. All assessed facilities followed well-established hazard and accident analysis techniques. In most cases, these facilities evaluated the hazards comprehensively to identify an appropriate set of hazard controls, and appropriately used the radiological and chemical hazard exposure thresholds in DOE-STD-1189-2008 and DOE-STD-3009-94 to classify safety controls for worker and public protection. The descriptions of the functional and performance requirements for safety controls were mostly consistent with the safety functions defined in hazard evaluations. EA's assessments of draft PSDRs and PDSAs indicated that issues identified in reviews by internal and external organizations, including those identified by EA, were being adequately resolved and incorporated into the safety design bases.

EA's observations also included weaknesses in each of the three broad technical areas. The assessments detailed several instances of insufficient hazard and accident analyses, including some weaknesses in implementing hazard analysis methodology for relatively complex processes. EA also found incomplete or insufficient identification of candidate hazard controls, incorrect safety functional classification of selected controls, and misapplication of the design criteria for safety SSCs.

The three technical areas are discussed in the subsections below. The discussion of each area begins with a broad statement summarizing the applicable high-level criteria paraphrased from the pertinent DOE regulations and directives. These statements are followed by the strengths and weaknesses found in the area.

2.1 Hazard and Accident Analyses

Criteria: *The DSA for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility, provide a systematic identification of both natural and man-made hazards associated with the facility, and evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility. Hazard and accident analyses must be consistent with the DOE safe harbor methodologies, and provide systematic and complete results for the selected hazards/accidents, consistent with the current design stage, to facilitate developing controls and their design and functional requirements. Safety must be integrated into the design early in, and throughout, the design process. (10 CFR 830 Subpart B, DOE Order 420.1B/C, DOE-STD-3009, DOE-STD-1189)*

A hazard analysis is the initial step towards developing the safety design basis for a nuclear facility. It is undertaken to systematically identify and evaluate facility hazards, potential accidents, and hazard controls. DOE-STD-3009-94 describes the safe harbor methodology for this process. At the conceptual design phase of a new nuclear facility, the limited design detail generally allows only a facility-level hazard analysis. As the design matures through preliminary and final design phases, DOE-STD-1189-2008 requires system-level hazard analyses in increasing detail to cover the full scope of facility processes and associated operations. The hazard evaluation is required to address the complete spectrum of hazards and potential accidents. The primary objective of initiating hazard analysis early in the design development, and continuing to refine it through the design phases, is to ensure that all required hazard

controls for the facility, especially those that require significant resources, such as major safety SSCs, are identified as early as possible.

EA assessments of nuclear facility projects found that hazard and accident analyses supporting the safety design basis development followed established methods, were appropriate to the facility's design phase and the complexity of operations, and enabled identifying a robust set of hazard controls. However, EA also identified several instances of insufficient hazard and accident analyses, as well as some weaknesses in the implementation of hazard analysis methodology.

The strengths and weaknesses in the hazard and accident analyses reviewed by EA are discussed below.

2.1.1 Strengths

EA found that, in most cases, the safety design basis documents provided comprehensive evaluations of an appropriate spectrum of potential facility and process upsets comprising representative and unique events, consistent with each nuclear facility's design phase. The hazard analyses at most facilities appropriately evaluated each facility system through a "what-if" analysis or hazard and operability analysis (HAZOP). The analyses generally were thorough, and the use of HAZOP, when selected, provided repeatability and transparency of the process.

The facility and site information in the safety design basis documents was sufficient, consistent with the facility's design maturity, to identify hazards and perform the necessary accident analyses. For example, the process flow diagrams and process and instrumentation drawings were consistent with the facility's preliminary design, and sufficient to support a system-level hazard analysis. The documents properly identified specific locations of hazardous material relative to process equipment. Projections for the maximum anticipated hazardous material-at-risk (MAR) included conservative margins to account for material in components still under design. Further, the documented site characteristics were sufficient to evaluate natural phenomena and external hazards affecting the safety design basis.

Where appropriate to the project, the hazard analysis team prepared an integrating hazard analysis that provided common information to all of the facility's process/system hazard analyses, including natural phenomena and external hazards. The integrating analysis also provided an overview of the facility's hazard analysis process, including a list of potential engineered controls.

The results of hazard analyses were well organized in hazard evaluation tables that grouped the information by event category. The summaries provided the postulated event location and description, type of hazardous material release, summary of causes, likelihood and consequences, and a broad set of hazard controls, both engineered and administrative controls, for later designation as safety class, safety-significant, or defense-in-depth.

The accident analyses adequately described the accident progression. The consequence calculations, such as those for fires, spills, and nuclear criticality, were appropriately conservative in determining potential unmitigated accident consequences to facility and co-located workers, and the public, and in supporting safety functional classification of SSCs.

2.1.2 Weaknesses

The weaknesses identified in this area are delineated as follows:

- Inadequacies in hazard and accident analyses
- Inadequacies in implementation of hazard analysis methodology.

Inadequacies in Hazard and Accident Analyses

EA found several specific instances where potential accident scenarios had not been systematically or fully evaluated, such that the proposed hazard control measures were inadequate or incomplete. The following are examples:

- **Fuel Pool Fire.** An accident analysis of potential fuel pool fire scenarios in a facility was inadequate for several reasons. The analysis assumed a floor surface, drum configurations, and administrative limits for flammable and combustible material, all of which were significantly different from the facility's design and other analyses. In addition, the accident analysis did not consider potential pool fire events during truck unloading operations. Thus, the analysis did not encompass all potential fuel spills and fires at the facility.

- **Glovebox Fire.** At one facility, the hazard analysis did not fully analyze certain glovebox fire scenarios and their unmitigated consequences, which led to the inadequate safety classification of the identified controls. Although sprinklers could not be installed in the gloveboxes due to criticality concerns, fires originating in the glovebox and spreading outside the glovebox were not analyzed. Consequently, the glovebox inerting systems and the supporting instrumentation and controls were not part of the safety-significant hazard control set.

- **Seismic Events.** In a few cases, the postulated seismic events were not adequately analyzed. At one facility, the accident analysis did not analyze the potential for post-seismic fires in certain locations with significant MAR quantities and fire loading. The analysis also did not address whether a crane fall caused by the event might increase the consequences. Further, the earthquake return period and accelerations assumed in the analysis were not in accordance with the design requirements for the facility. At another facility, seismic events with estimated radiological doses to co-located workers greater than 5 Rem were not carried forward from the hazard evaluation into the accident analyses. This omission led to the assignment of the lowest seismic design categories, when the correct consequence levels were within the range (5 - 100 Rem) requiring higher seismic design categories for pertinent SSCs.

- **Internal Flooding.** In considering internal flooding hazards, one hazard analysis addressed the effect of flooding loads on the floors, but did not address the potential effects of high water levels on SSC operation. In addition, the analysis did not identify the non-safety systems that needed further analysis to determine their appropriate flood hazard design category.

Inadequacies in Implementation of Hazard Analysis Methodology

EA's assessments of hazard analyses of a variety of facility processes and systems identified several issues with the implementation of the methodology for defining and characterizing hazard or accident scenarios. Such issues potentially compromised the capability of hazard analyses to systematically evaluate hazards and to identify appropriate candidate hazard controls, resulting in inadequacies illustrated above. These issues are discussed below.

- **Event Definition.** The postulated event was not always defined sufficiently to allow the identification of all the causes and the potential candidate controls for those causes. In some cases, non-mechanistic failures (e.g., unstated equipment failures or implied operator errors) were assumed such that the described sequence of events did not follow from an identified cause. In

other cases, the event description contained unstated conditions or assumptions that hindered the identification of event causes and corresponding candidate controls.

- **Failure Modes.** In some hazard analyses, all credible failure modes were not consistently identified and evaluated. In particular, the analyses did not consider the dependent failure of a system or component (e.g., post-seismic crane fall) or undetectable failures (e.g., potential latent flaws) coupled with the initiating event.

- **Spectrum of Conditions.** A few hazard analyses did not sufficiently explore the various potential conditions of an event to ensure that all candidate controls were identified. For example, a partial failure of a subsystem (rather than full failure) or a partial detachment of a container (rather than full detachment) could merit the consideration of additional controls.

- **Operational Modes.** In one hazard analysis of a complex system, the site did not consistently consider all applicable operational modes, operating configurations, and process parameter deviations that could potentially affect system performance. In some cases, combinations of subsystems in different operational modes presented additional configurations that were not analyzed.

2.2 Hazard Control Selection

Criteria: *The DSA for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility, derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment; demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards; and define the process for maintaining the hazard controls current at all times and controlling their use. Safety analyses must be used to identify safety class and safety-significant SSCs to fulfill the safety functions in order to prevent and/or mitigate design basis accidents, including natural and man-induced hazards and events, and to identify SACs needed to fulfill safety functions. An SAC exists when an administrative control is identified in the DSA as a control needed to prevent or mitigate an accident scenario, and has a safety function that would be safety-significant or safety class if the function were provided by an SSC. (10 CFR 830 Subpart B, DOE Order 420.1B/C, DOE-STD-3009, DOE-STD-1189, DOE-STD-1186)*

DOE requires, as part of hazard evaluation, the identification of all controls that can prevent or mitigate a postulated hazard scenario. It also requires designating hazard controls (SSCs, administrative, and programmatic) as safety class or safety-significant when they are relied upon to prevent or mitigate consequences of accidents. This designation is specifically required when the consequences of accidents meet certain specified qualitative and quantitative criteria that ensure adequate protection of workers, the public, and the environment against potential uncontrolled releases of radioactive or other hazardous materials. All preventive and mitigative controls associated with the given hazard event must be considered for such designation. DOE standards provide a hierarchy of controls that gives preference to passive over active SSCs, engineered features over SACs and other administrative controls, and preventive over mitigative controls. Further, DOE requires that the controls incorporate a defense-in-depth approach with layers of defense against the uncontrolled release.

EA's assessments of the safety design basis documents indicated that the nuclear facilities were making adequate progress towards establishing a proper and complete set of hazard controls, and developing the DSA/TSRs. However, EA identified several instances of inadequacies in the identification of candidate hazard controls, which were often rooted in inadequate hazard evaluation.

The following subsections discuss the areas of strength and weakness. The weaknesses are covered below in two separate subsections for SSC controls and SACs.

2.2.1 Strengths

In most cases, the nuclear facility hazard evaluations identified a complete set of candidate hazard controls to support control set selection. The controls were consistent with the logic in the hazard analyses.

The safety design basis documents provided adequate description of the methods used to compare the unmitigated consequences of postulated accidents against DOE criteria for safety classification of the selected hazard controls needed to protect against uncontrolled radiological and chemically hazardous releases. The documents also addressed SSCs to be classified as defense-in-depth.

The selection and designation of safety-significant SSCs for criticality safety consistently focused on the prevention of criticality events that could result in serious consequences (e.g., fatality or serious injury to the facility worker).

Where passive SSCs were identified to prevent unmitigated radiological or hazardous chemical consequences exceeding the DOE criteria, they were properly designated as safety Design Features and were, in most cases, appropriately addressed in the TSR derivation.

In most cases, the safety design basis documents appropriately defined the SACs and other administrative controls. The SACs were evaluated for their ability to meet the safety functions that were identified in the hazard and accident analyses. The hazard evaluations also identified, where appropriate, the required defense-in-depth administrative controls as key programmatic elements for inclusion in the pertinent safety management programs within the TSR.

2.2.2 Weaknesses - SSC Controls

EA found various inadequacies in the identification of candidate hazard controls. The weaknesses are grouped as follows and discussed below:

- Incomplete identification of hazard controls
- Inadequacies in candidate controls for bounding hazard events
- Bias in hazard control selection.

Incomplete Identification of Hazard Controls. In instances where a postulated sequence of failures was not sufficiently described, EA observed that the hazard evaluation did not identify a complete candidate control set. Examples include:

- **Sequential Failures of Process Units.** In a postulated hazard event progression at one facility, where structural damage to one process unit caused loss of pressure control in the second unit, the hazard evaluation did not identify preventive or mitigative candidate controls to interrupt the event progression (e.g., preventing failure of the first unit or the loss of the second unit).

- **Dropped Load.** In another case, a dropped load hazard event did not include preventive engineered controls for equipment or computer failures (e.g., redundant hook). While the causes for the postulated event included these types of failures, the only proposed control was an administrative control (i.e., the hoisting and rigging program).

- **Loss of Ventilation Flow.** In a hazard event evaluated at a waste processing facility, the loss of cooling resulted in adverse high temperature effects on safety control systems. However, the hazard evaluation did not identify the room cooling system as a candidate control.

Inadequacies in Candidate Controls for Bounding Hazard Events. EA found that some bounding hazard scenarios, also referred to as representative accidents, considered in hazard analyses were not representative of certain underlying events. Representative accidents bound a number of underlying events, which are of lesser risk and share the same event causes and candidate controls. In other cases, the relationship between the bounding accidents and the underlying events was undefined. As a result, the identified set of candidate hazard controls was inadequate or incomplete. The following are examples of this inadequacy:

- **Hazardous Leak.** A bounding accident involving potential worker exposure to a hazardous release, due to an overpressure leak in a processing unit compartment, was considered also to bound other types of release events, such as one caused by high temperature due to cooling system problems and another caused by damage to the unit from a load drop. However, the preventive engineered controls only addressed the overpressure conditions, but did not include prevention of failures from other causes, such as load drop.

- **Ventilation System Blockage.** For a bounding accident that resulted in no flow through high efficiency particulate filters, several interlocks associated with the potential underlying hazard events were not included as candidate controls for the accident.

- **Bounding Vessel Failure.** A bounding accident involving a hazardous release caused by vessel failure was identified to also bound certain hazard events caused by control system failures; however, the relationship of the vessel failure to the control system failures was not defined adequately to identify all the appropriate controls needed to prevent control system failures.

- **Bounding Seismic Event.** One hazard evaluation combined seismic and certain high temperature hazard events under a single bounding seismic event, without defining how the event was representative of a high temperature event caused by a pressure relief valve stuck in the open position.

Bias in Hazard Control Selection. DOE guidance on control selection hierarchy gives preference to prevention over mitigation. EA found that for some postulated hazard events, where preventive controls would be particularly desirable to prevent high consequences, the candidate hazard control set did not provide the necessary balance between preventive and mitigative controls.

For example, in the hazard analysis for one system, which postulated catastrophic boiling liquid expanding vapor explosion events, the identified controls were primarily mitigative without any justification provided for the apparent bias. These events provided little reaction time and insufficient preventive controls, and resulted in potentially high consequences to the co-located worker.

In some cases, EA observed errors in interpreting the safety function of identified controls, such that the controls were mischaracterized (e.g., designated as preventive controls instead of mitigative controls or vice versa). Such deficiencies also adversely affected the balance in control selection. For example, in one hazard evaluation, the ventilation system for a process unit was identified as a mitigative control in a number of events that involved a breach of the process equipment, but the ventilation safety function would instead serve to prevent a release. In another example, an interlock to stop feed to a process during

an event was identified as a mitigative control, whereas the control would actually prevent event progression.

2.2.3 Weaknesses - SACs

EA identified instances where the administrative controls necessary to perform safety functions were either not identified or not designated as SACs. Also, EA found a few cases where a designated SAC was not implemented adequately. These issues are illustrated below.

SACs Not Identified. The following examples illustrate cases where SACs were required, but no controls of any kind were identified:

- **Sealed Sources.** At one nuclear facility, where a building was designed to store calibration sources, the hazard evaluation did not identify SACs to limit the number of sealed sources outside the safety class, fire-rated safes, or to ensure that the sources were safely stored when not in use.

- **Operator Actions to Prevent Explosion.** At another facility, the accident analysis and control selection did not recognize the safety importance of operator actions. These actions included using pre-staged portable equipment to restore purge air to certain process vessels and equipment vapor spaces in order to maintain the flammable vapor concentration below the composite lower flammable limit within four days following a seismic event. In a postulated hazard event involving the loss of power and resulting loss of normal purge air flow, a safety air purge system would supply the required purge air from backup air receivers for four days. However, according to the pertinent safety design analyses, explosions were credible for a period of ten days. Thus, credited operator actions in the form of SACs were required to prevent an explosion after safety purge air was spent.

Administrative Controls Not Designated as SACs. The following are examples of cases where administrative controls were identified, but their safety importance was not recognized and the controls were not designated as SACs:

- **Vault Cover Protection.** At one facility, the installation of a vault cover block to protect facility workers from potential chemical burns, due to a pressurized leak accident, was incorrectly classified as a non-safety, defense-in-depth administrative control, instead of a credited SAC. The unmitigated consequences of this hazard event were estimated to exceed the highest threshold for hazardous exposure to co-located workers. Without a secondary containment, it was not conservative to assume that the process piping and equipment were sufficient to prevent the high consequence event. In addition, establishing a TSR requirement was necessary to verify that cover blocks were installed as a condition for entering the facility's operational mode.

- **Radiological Waste Inventory.** At another facility with the potential for adverse public consequences, the assumptions on waste characteristics and the MAR were protected through an administrative control, instead of a safety class SAC. These assumptions were used to estimate the radiological consequences of postulated accidents. Failure to properly classify a MAR control could lead to exceeding the analyzed accident consequence and invalidating the safety design basis conclusions of adequate protection.

Inadequate SAC. One facility had correctly identified a TSR-level safety class SAC to prevent a radioactive release in the event of a fire. The SAC required a fire watch and included actions to notify the fire department, but did not specifically require the fire watch to extinguish the fire.

2.3 Safety Functional and Performance Requirements

Criteria: *Safety analyses are used to establish the safety functional requirements of the safety class and safety-significant SSCs, and of the SACs needed to fulfill safety functions. The bases for the design, functional, and performance requirements of the selected safety SSCs to prevent or mitigate the postulated accidents are adequately defined and described. A system evaluation supporting the adequacy of safety SSCs and SACs is included in the safety bases. The description of each SAC contains the rationale for designating an SAC and sufficient detail for understanding its safety function and relationship to the safety analysis. Technical safety requirements establish limits, controls, and related actions necessary for the safe operation of a nuclear facility. (10 CFR 830, Subpart B; DOE Order 420.1B/C; DOE-STD-3009; DOE-STD-1189; DOE-STD-1186)*

DOE requires the DSA to describe the safety function, functional requirements, and performance criteria applicable to safety SSCs and SACs to support the safety functions identified in the hazard and accident analyses, and to derive TSRs. A performance criteria evaluation supporting the adequacy of safety SSCs and SACs must be included in the DSA. The evaluation summarizes the technical basis for the relevant design and performance capabilities, which includes demonstrating compliance with applicable DOE design requirements and associated codes and standards, augmented as necessary with calculations, performance tests, or other evidence of reliability.

EA's assessments of safety design basis documents and supporting technical evaluations found that the nuclear facility projects were satisfactorily developing robust design bases for the designated safety SSCs and SACs. However, EA identified certain SSC design and safety classification weaknesses at some facilities. Both strengths and weaknesses are summarized below. The issues concerning the lack of identification and proper classification of SACs were discussed in Section 2.2.3.

2.3.1 Strengths

At all of the facilities reviewed, the safety functions and functional requirements of the safety SSCs documented in the safety design bases were consistent with the hazard and accident analyses. Further, DOE's nuclear safety design criteria were, in most cases, satisfactorily incorporated into the design requirements for safety SSCs, and the supporting engineering design analyses, with a few exceptions, adequately demonstrated how the safety SSCs met the functional and performance requirements.

For most safety systems, the system design descriptions were thorough and provided important design information, including vendor information, to support the ongoing hazard analysis and engineering work.

In most cases, the reviewed TSR derivations accurately translated the safety SSC and SAC functional and performance requirements into an adequate set of formal, implementable operational requirements. The derivation of the TSRs was adequately described in the safety design basis.

2.3.2 Weaknesses

The weaknesses with respect to the safety design basis of selected safety SSCs are grouped as follows for the discussion below:

- Inadequacies in safety classification
- Inadequacies in seismic design categorization
- Inadequacies in design criteria.

Inadequacies in Safety Classification. In some cases, EA found that the safety classification of SSCs, especially support systems or components upon which the designated safety SSCs relied to perform their safety functions, was not appropriate. The following examples illustrate this weakness:

- **Fire Protection.** EA assessments of safety-significant fire suppression systems (FSSs) at two nuclear facilities revealed issues related to freeze protection in the design of water storage tanks and associated systems. Improper safety classification of the freeze protection systems compromised the availability of storage tanks for supplying water to the safety FSS.

- **Backup Electrical Power.** At one facility, the backup electrical power supply to a safety system and to its instrumentation and control interfaces was not classified as safety-significant. In a few other cases, the safety design bases had not identified that backup power was needed for certain safety systems to perform safety functions.

- **Chemical Hazards.** At a facility with dominant chemical hazards, the controls identified for several postulated accidents with high worker consequences (e.g., explosion and loss of containment) were incorrectly classified as non-safety. The safety design basis also did not adequately discuss defense-in-depth and worker safety.

Inadequacies in Seismic Design Categorization. In a few cases, the seismic design category assigned to SSCs that support or interface with safety SSCs was not in accordance with DOE standards. Examples of this issue include:

- **System Interactions.** At one facility, EA identified that the safety function of the FSS could be adversely impacted by potential system interactions with non-safety equipment (commonly known as "two-over-one" interactions). The safety system was designed to the correct seismic design category; however, components of the confinement ventilation system, with potential for adverse system interactions with the safety FSS, were designed to lower seismic design categories.

- **Design Basis Earthquake.** At one facility, the seismic design category assigned to certain process vessels and ventilation system boundary components was inappropriate for supporting a credited safety function that required this equipment to survive a design basis earthquake.

- **Interfacing Systems.** In a few cases, the seismic design category of SSCs was not adequate because safety system boundaries were not defined properly. The safety-significant FSS at one facility was appropriately designed, but the water supply tank it shared with a non-safety water supply system of another facility was designed to a lower seismic design category, and the design did not specify seismic isolation at the interfaces between the differing seismic design boundaries.

Inadequacies in Design Criteria. EA also identified instances where the safety design basis documents were deficient in defining or implementing design criteria for safety SSCs. The following provides some examples:

- **Fire Barriers.** At one facility, the safety fire barriers were designed to protect several safety SSCs (e.g., confinement ventilation equipment, uninterruptible power system, and programmable protection system) to ensure their operability during a fire event. However, the supporting design analysis for the barriers was limited to controlling fire propagation, and did not address protecting the safety SSCs. For example, certain equipment hatches within the fire barriers did not meet the two-hour fire resistance criterion.

- **Shared Fire Water Supply.** If the safety emergency diesel pump failed to supply water to its safety FSS, the design of one nuclear facility required that a safety diesel pump from an adjacent nuclear facility at the site (with the same capacity and flow rate) be redirected to serve in a redundant manner. An emergency hose would supply water to both facilities until the failed pump could be returned to service. However, the design did not account for the constraint that the water storage tank volume was insufficient to supply both facilities.

- **Instrumentation and Control.** At a few facilities, the specified safety design requirements of control systems were incomplete. For example, in one case, the functional requirements for a safety class instrumented system design (to control the functions of several systems, including the confinement ventilation system and emergency power) did not specify important design requirements, such as independence, redundancy, electrical separation, and the ability to withstand single failures.

- **Air Purge of Flammable Gases.** EA identified a few non-conservative assumptions in the analyses supporting design and performance of a facility's safety class air purge system; this system's function is to keep flammable gas concentrations in process vessels below the lower flammability limit. The assumptions concerned the non-conservative initial flammable gas concentration in the vessels, the sources of heat input, and the leakage of purge air. Further, the size of process vessel orifices necessary to allow the required exhaust air flow lacked an adequate technical basis.

- **Seismic Power Cutoff System.** At one facility, a primary function of the safety class seismic power cutoff system was not fully defined and implemented. The operational controls did not require that the cutoff contactor open and isolate power to the facility's waste handling and storage areas. Further, there were no compensatory measures, such as stationing an operator to perform this function when both seismic switches are not in service and bypassed. EA also found that a number of performance criteria for this safety function were missing from the safety design basis.

3.0 BEST PRACTICES

In preparing this lessons learned report, EA identified the following best practices that may be valuable to other DOE sites:

- **Design Engineering and Nuclear Safety Integration.** Two nuclear projects, SWPF and UPF, had organizational structures that clearly facilitated the integration of design engineering and safety activities. A notable strength at SWPF was the strong and effective involvement of the technical staff within an integrated SWPF Engineering and Nuclear Safety organization in developing the hazard and accident analyses, along with designing and procuring facility SSCs. This organization contributed to the high quality and consistency of safety design basis and engineering documents. In the case of UPF, the design engineering and safety design basis development functions, while separate, were well integrated and reported to the same design authority.

- **Criticality Safety.** At UPF, a nuclear facility that will have significant potential for nuclear criticality after it becomes operational, the required criticality safety evaluations and the selection

of controls to prevent potential accidents were in accordance with DOE standards and were completed in an exemplary manner. Each process was thoroughly analyzed for the potential for nuclear criticality accidents. The process evaluation identified the design requirements and presented a robust set of controls for prevention of a nuclear criticality accident caused by operational mishaps and credible abnormal events. The facility developed proper criteria for elevating controls to the safety-significant classification, and the evaluation provided an adequate technical basis for the decisions. Overall, the process was well defined and the nuclear criticality safety controls were properly integrated into the safety design basis.

- **Fire Modeling.** The technical analysis for UPF included a comprehensive analysis of the impacts of potential fires on SSCs of significance to criticality safety, designated as items of interest (IOIs). This analysis involved quantitative fire modeling to determine the Threshold Damage Limit in terms of thermal exposure (temperature at the IOI surface). The analyses identified fire exposure zones (i.e., areas where threshold damage may occur during a fire) to establish minimum safe distances between fire sources and the IOI. In the event an IOI was within a fire exposure zone, the IOI was assigned to one of several control strategies designed to further reduce the risk of exposure to fire. These control strategies included passive measures (e.g., separation distances, spill containment, and protective wraps) and administrative controls, while excluding the use of automatic sprinklers. The multiple-layer, defense-in-depth approach was implemented such that the failure of any single layer would not compromise the IOIs.

- **Design Analyses.** The engineering analyses supporting the design of SWPF safety systems were noteworthy. The architecture of several lengthy, complex analyses was effective in presenting a systematic progression of steps, along with descriptions of the context for each section, and in minimizing the need to cross-reference extensively. The technical analyses were supported by empirical data and, where required, were confirmed with thorough, well-designed empirical testing. Many of the assumptions and bounding conditions were conservatively applied to ensure that an adequate margin of safety was embedded into the overall design strategy. The analyses were properly integrated into the safety design basis.

- **Prototypical Test Facility.** The DOE contractor responsible for SWPF established a testing facility where prototypical concepts are tested to demonstrate the viability of new or untried technologies intended to be incorporated into the facility design. The test facility staff was frequently consulted to validate design and safety analysis assumptions, as well as resolve technical questions arising in the design process.

- **NNSA Technical Bulletins.** The periodic Technical Bulletins issued by NNSA are a valuable resource to the DOE nuclear safety professional staff, both government and contractor, in understanding and implementing DOE nuclear safety requirements. The Technical Bulletin is modeled on a system used by Naval Reactors and is intended to be a vehicle for sharing lessons learned and insights. In addition, the Technical Bulletin is viewed as an authoritative statement on specific technical issues, but not as a directive stating formal policy or requirements. The compilation of Technical Bulletins includes guidance on areas of safety design basis development (e.g., SACs) where EA found weaknesses.

4.0 RECOMMENDATIONS

The recommendations below are based on lessons learned from the collective analysis of EA assessments of safety design basis development summarized in Section 2. While the underlying deficiencies and weaknesses from individual reviews did not apply to every site reviewed, the recommended actions are intended to provide insights for potential improvements at all DOE nuclear sites. Consequently, DOE organizations and site contractors should evaluate the applicability of the following recommended actions to their respective facilities and/or organizations, and consider their use, as appropriate, in accordance with Headquarters and/or site-specific program objectives.

DOE Field Elements

- **Safety-in-Design Process.** Ensure that the safety-in-design process, required by DOE Order 413.3 and implemented through DOE-STD-1189, is initiated and closely followed from the earliest design phase of all nuclear facility projects to which these directives apply. From project inception, establish close coordination and interaction between the nuclear facility project contractor's integrated project team and the safety design integration team. Emphasize the importance of the preparation and maintenance of the SDS as a guide to establishing the hazard controls and developing the safety design basis. Coordinate the contractor's development of the SDS with cognizant DOE project, engineering, and nuclear safety staff, so that the DOE-approved SDS provides an agreed-upon approach to developing the integrated safety design early in (and throughout) the design process, including key safety decisions for major safety SSCs, types of analyses to be conducted, and safety documents to be prepared and used.

- **Review and Oversight.** Ensure that nuclear safety oversight staff review and oversee the contractor's hazard analysis activities, including the identification and selection of hazard controls, early in the design phases in order to develop a robust safety design foundation for the final safety basis.

- **External Reviews.** Engage external reviewers early in the project in order to provide a timely, independent review of the SDS, hazard analyses and controls, and safety SSC design, and to resolve potential problems early in the design process.

DOE Contractors Responsible for Nuclear Facility Projects

The recommendations for DOE nuclear facility project contractors begin with two sets of recommendations emphasizing early safety-in-design integration, followed by three additional sets of recommendations corresponding to the three broad areas of safety design basis development discussed in Section 2, Overall Assessment.

Safety-in-Design Integration

- **Safety-in-Design Process.** Ensure that the SDS provides a detailed approach to developing the integrated safety design early in the process, including key safety decisions for major safety SSCs, types of analyses to be conducted, and safety documents to be prepared and used. This approach should be closely coordinated with the responsible DOE field element organization to achieve a consistent method for implementing the SDS throughout the design process, which will minimize design changes later in the final design and construction of the facility.

- **Safety Basis and Design Engineering Integration.** In building the nuclear facility project organization, consider organizational designs that facilitate and encourage close coordination and integration of the safety basis analysts and design and process engineers during all phases of the project. For example, consider these disciplines reporting to the same organizational authority. Ensure that the safety basis and engineering teams are working together in performing all safety-in-design integration activities and developing the various products called for in DOE-STD-1189.

Integration of Fire Hazards Analyses with Safety Design Basis

- **Coordination in the Analyses and Documentation of Fire Hazards.** Improve coordination between developing fire hazards analyses and the safety design basis documents at various design phases. Ensure that key information, such as postulated fire scenarios, hazard controls, and the facility interfacing systems, is consistent in both sets of documents.

Hazard and Accident Analyses

The following recommendations concern the specific technical aspects of hazard analysis where EA identified generic weaknesses:

- **System Definition.** Ensure that the scope, description, boundaries, and interfaces of each facility system or subsystem are clearly defined and made available to the team preparing, conducting, and documenting the hazard analysis.

- **Potential Failures.** In the case of relatively complex events, delineate the stages of event progression to systematically identify the causes and the candidate controls, both mitigative and preventive, at each stage of an event scenario. Evaluate the entire end-to-end event scenario, taking into account the potential failures.

- **Bounding Accidents.** Document the methodology for selecting bounding accidents and candidate hazard controls. Before candidate controls are selected, explain the criteria or parameters that will be used to evaluate whether the selected bounding accidents are representative of the underlying hazard events. Also, ensure that the bounding accidents are not inappropriately combined with other events, which could compromise identifying candidate controls in accordance with the preferred DOE hierarchy of controls.

- **Applicable Lessons Learned.** Ensure that applicable lessons learned from failures and problems in other similar processes or safety systems are reviewed and taken into consideration in hazard analysis.

Hazard Control Selection

- **Role and Description of Controls.** Ensure that the hazard control set for a postulated hazard event is complete, adequately described, and balanced from the standpoint of preventive and mitigative controls, such that the ability to prevent the event is not overlooked. Verify that the role of each identified candidate control is correctly understood and designated as preventive or mitigative, so that it is appropriately considered in accordance with the preferred DOE hierarchy of controls.

- **SAC Training.** Provide enhanced training to safety analysts on identifying, developing, writing, and implementing SACs in accordance with DOE standards, especially on specifying the SACs

safety functional requirements and performance criteria. Consider appropriately incorporating guidance related to SACs that is contained in various NNSA Technical Bulletins.

Safety SSC Functional and Performance Requirements

- **Coordination with Design and Process Engineers.** Ensure that the safety functions and performance criteria for safety SSCs are interactively reviewed by the cognizant design and process engineers throughout the safety analysis and design processes. Verify that safety performance criteria are adequately understood, translated into appropriate design criteria, evaluated in the safety basis, and protected by maintenance and surveillance requirements.

- **Safety Classification of Support and Interfacing Systems.** Define safety SSC boundaries and interfaces comprehensively to ensure proper classification of all supporting, interfacing, and segregated components of the system. Evaluate the support SSCs required for safety SSCs to perform their safety functions, and assign SSCs the appropriate safety classification and design category, in accordance with DOE requirements.

Appendix A
Supplemental Information

Office of Enterprise Assessments Management

William A. Eckroade, Acting Director, Office of Enterprise Assessments
Thomas R. Staker, Director, Office of Environment, Safety and Health Assessments
William E. Miller, Deputy Director, Office of Environment, Safety and Health Assessments
C.E. (Gene) Carpenter, Jr., Director, Office of Nuclear Safety and Environmental Assessments
Kevin G. Kilp, Director, Office of Worker Safety and Health Assessments
Gerald M. McAteer, Director, Office of Emergency Management Assessments

Quality Review Board

Steven C. Simonson
John S. Boulden III
Thomas R. Staker
William E. Miller
Michael A. Kilpatrick

Office of Enterprise Assessments Report Contributors

Preparers
James O. Low (Lead)
Shivaji S. Seth

Additional Contributors
Kevin E. Bartling
Michael V. Frank
Roy R. Hedtke
Katherine S. Lehew
Mary Miller
David J. Odland
Joseph J. Panchison
Donald C. Prevatte
Jeffrey L. Robinson
Daniel Schwendenman

Appendix B
Source Documents
(Listed by facility, in reverse chronological order)

Hanford Site Tank Farms Low Activity Waste Pretreatment System

- EA Report, *Targeted Assessment of the Hanford Site Tank Farms Low Activity Waste Pretreatment System Preliminary Safety Design Basis – December 2017*

- EA Field Notes, *Hanford Tank Farm Low Activity Waste Pretreatment System Draft Preliminary Safety Design Report Review*, FN-EA-31-WRPS-7-10-2017

- EA Field Notes, *Tank Farm Low Activity Waste Pretreatment System Visit*, FN-EA-31-WRPS-2-13-2017, Rev. 1

Hanford Site Waste Treatment and Immobilization Plant - High Level Waste Facility

- EA Field Notes, *Operational Awareness Visit to the Waste Treatment and Immobilization Plant High Level Waste Facility Draft Preliminary Documented Safety Analysis Reviews*, FN-EA-31-WTP-HLW-10-17-2016 Rev.2

- EA Field Notes, *Operational Awareness Visit to the Waste Treatment and Immobilization Plant High Level Waste Facility*, FN-EA-31-WTP-HLW-7-11-2016

- EA Report, *Targeted Assessment of the Waste Treatment and Immobilization Plant High-Level Waste Facility Radioactive Liquid Waste Disposal System Safety Basis Change Package – May 2016*

- EA Operational Awareness Record, *Review of Waste Treatment and Immobilization Plant High Level Waste Facility Concentrate Receipt/Melter Feed/ Glass Formers Reagent Hazards Analysis Event Tables*, EA-WTP-HLW-2015-02-02

- EA Operational Awareness Record, *Observation of the Waste Treatment and Immobilization Plant High Level Waste Facility Concentrate Receipt/Melter Feed/ Glass Formers Reagent Hazards Analysis Activities and Review of the Radioactive Liquid Disposal Hazards Analysis Event Tables*, EA-WTP-HLW-2014-10-20

- EA Operational Awareness Record, *Observation of Waste Treatment and Immobilization Plant High Level Waste Facility Radioactive Liquid Disposal System Hazards Analysis Activities*, EA-WTP-HLW-2014-08-18(a)

Hanford Site Waste Treatment and Immobilization Plant - Low Activity Waste Facility

- EA Field Notes, *Operational Awareness Visit to the Waste Treatment and Immobilization Plant – Low Activity Waste Facility Safety Basis Development Activities*, FN-EA-31-WTP-LAW-10-17-2016

- EA Field Notes, *Operational Awareness Visit to the Waste Treatment and Immobilization Plant Low-Activity Waste Facility Draft PDSA Development Review*, FN-EA-31-WTP-LAW-4-24-2017

- EA Operational Awareness Record, *Review of the Waste Treatment and Immobilization Plant Low-Activity Waste Facility Preliminary Documented Safety Analysis Addendum*, OAR-EA-WTP-LAW-2017-03-09

- EA Field Notes, *Operational Awareness Visit to the Waste Treatment and Immobilization Plant Low Activity Waste Facility Draft PDSA Review*, FN-EA-31-WTP-LAW-2-13-2017

- EA Field Notes, *Operational Awareness Visit to the Waste and Immobilization Plant - Low Activity Waste Facility Safety Basis Development Activities*, FN-EA-31-WTP-LAW-07-11-2016

- EA Field Notes, *Operational Awareness Visit to the Waste Treatment and Immobilization Plant Low Activity Waste Facility – C5V Functional Classification Activities*, EA-WTP-FN-2016-01-26 (Rev.2)

- EA Operational Awareness Record, *Review of the Waste Treatment and Immobilization Plant Low-Activity Waste Facility Preliminary Documented Safety Analysis Change Package for the Effluent Management Facility*, EA-WTP-LAW-2016-01-25

- EA Report, *Review of the Hanford Site Waste Treatment and Immobilization Plant Low-Activity Waste Facility Hazards Analysis Reports for the Melter and Melter Offgas Systems – September 2015*

- EA Report, *Review of the Hanford Site Waste Treatment and Immobilization Plant Hazards Analysis Report for the Low-Activity Waste Facility Reagent Systems – July 2015*

- EA Operational Awareness Record, *Review of Waste Treatment and Immobilization Plant Low-Activity Waste Facility "Facility-Wide" Draft Hazard Analysis Report*, EA-WTP-LAW-2015-02-02

- EA Operational Awareness Record (December 2014), *Waste Treatment and Immobilization Plant Low Activity Waste Facility Waste Handling Systems Hazard Analysis Activities*, EA-WTP-LAW-2014-08-18(b)

- EA Operational Awareness Record (December 2014), *Observation of Waste Treatment and Immobilization Plant Low Activity Waste Facility Reagent Systems Hazards Analysis Activities*, EA-WTP-LAW-2014-06-02

- EA Independent Activity Report, *Observation of the Waste Treatment and Immobilization Plant Low Activity Waste Facility Hazards Analysis Activities*, IAR-WTP-2014-03-31

- HSS Independent Activity Report, *Observation of the Waste Treatment and Immobilization Plant Low Activity Waste Facility Heating, Ventilation, and Air Conditioning Systems Hazards Analysis Activities*, HIAR-WTP-2014-01-27

- HSS Independent Activity Report, *Observation of Waste Treatment and Immobilization Plant Low Activity Waste Facility Off-gas Systems Hazards Analysis Activities*, HIAR-WTP-2014-01-27

- HSS Independent Activity Report, *Catholic University of America Vitreous State Laboratory Tour and Discussion of Experiments Conducted in Support of Hanford Site Waste Treatment and Immobilization Plant Select Systems Design*, HIAR-VSL-2013-11-18

- HSS Independent Activity Report, *Observation of Waste Treatment and Immobilization Plant Low Activity Waste Melter and Melter Off-gas Process System Hazards Analysis Activities*, HIAR-WTP-2013-10-21

- HSS Independent Activity Report, *Operational Awareness of Waste Treatment and Immobilization Plant Low Activity Waste Melter Process System Hazards Analysis Activity*, HIAR-WTP-2013-07-31

- HSS Independent Activity Report, *Waste Treatment and Immobilization Plant Low Activity Waste Melter Off-gas Process System Hazards Analysis Activity Observation*, HIAR-WTP-2013-05-13

- HSS Independent Activity Report, *Follow-up of Waste Treatment and Immobilization Plant Low Activity Waste Melter Process System Hazards Analysis Activity Review*, HIAR-WTP-2013-03-18

- HSS Independent Oversight Report, *Review of the Hanford Site Waste Treatment and Immobilization Plant Low Activity Waste Melter Process System Hazards Analysis Activity – December 2012*

Hanford Site Sludge Treatment Project - Engineered Containment Retrieval and Transfer System

- EA Report, *Review of the Hanford Site Sludge Treatment Project Engineered Container Retrieval and Transfer System Preliminary Documented Safety Analysis, Revision 00 – April 2015*

Los Alamos National Laboratory Transuranic Waste Facility

- EA Memorandum for Manager, Los Alamos Field Office, *EA Assessments of the Los Alamos National Laboratory Transuranic Waste Facility Documented Safety Analysis and Technical Safety Requirements*, December 23, 2016

- EA Field Notes, *Transuranic Waste Facility 100% DSA-TSR EA-31 Review Briefing*, FN-EA-31-LANL-8-24-2016

- EA Field Notes, *Review of Transuranic Waste Facility 95% Documented Safety Analysis and Technical Safety Requirements*, FN-EA-31-LANL-2016-04-21

- EA Operational Awareness Record, *Review of Transuranic Waste Facility 90% Draft Documented Safety Analysis and Technical Safety Requirements Submittals*, EA-LANL-2015-07-07

- EA Report, *Independent Oversight Review of the Los Alamos National Laboratory Transuranic Waste Facility Safety Basis and Design Development – July 2014*

- HSS Independent Activity Report -Rev. 0, *Office of Enforcement and Oversight's Office of Safety and Emergency Management Evaluations Activity Report for Coordination Meeting with National Nuclear Security Administration Los Alamos Field Office Safety Basis Review Team Leader for Transuranic Waste Facility Preliminary Documented Safety Analysis Report*, HIAR-LANL-2013-04-08

Savannah River Site Salt Waste Processing Facility

- EA Report, *Independent Oversight Review of the Savannah River Site Salt Waste Processing Facility Safety Basis and Design Development – August 2013*

Y-12 National Security Complex Uranium Processing Facility

- EA Report, *Assessment of the Y-12 National Security Complex Uranium Processing Facility Preliminary Documented Safety Analysis – January 2018*

- EA Report, *Targeted Assessment of the Y-12 National Security Complex Uranium Processing Facility Preliminary Safety Design Basis – April 2017*

- EA Report, *Independent Oversight Appraisal of the Uranium Processing Facility Safety Basis Preliminary Safety Design Report Process at the Y-12 National Security Complex – May 2013*