DOE G 421.1-2

Approved: xx-xx-2011

IMPLEMENTATION GUIDE FOR USE IN DEVELOPING DOCUMENTED SAFETY ANALYSES TO MEET SUBPART B OF 10 CFR 830

[This Guide describes suggested nonmandatory approaches for meeting requirements. Guides are not requirements documents and are not construed as requirements in any audit or appraisal for compliance with the parent Rule, 10 CFR 830.]

U.S. DEPARTMENT OF ENERGY
Office of Nuclear Safety

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Nuclear Safety

FOREWORD

This Department of Energy (DOE) Implementation Guide is approved use by all DOE elements, including the National Nuclear Security Administration (NNSA) and its contractors. Suggestions for corrections or improvements to this Guide should be addressed to:

Michael Hillman
U.S. Department of Energy
Washington, D.C. 20585
Phone (301) 903-3568
Facsimile (301) 903-6172

This Guide was developed in support of Title 10 Code of Federal Regulations (CFR) Part 830, Subpart B, "Safety Basis Requirements", and provides guidance in meeting the provisions for documented safety analyses defined in that subpart.

This document may be used by all contractors for DOE Hazard Category 1, 2, or 3 nuclear facilities, including contractors for NNSA Hazard Category 1, 2, or 3 nuclear facilities. Throughout this document, wherever it references a contractor or a DOE contractor, the statement applies to a contractor for NNSA as well.

This Guide does not establish or invoke any new requirements.

CONTENTS

1. INTRODUCTION

Title 10 Code of Federal Regulations (CFR) Part 830, Subpart B, "Safety Basis Requirements," requires the contractor responsible for a Department of Energy (DOE) nuclear facility to analyze the facility, the work to be performed, and the associated hazards and to identify the conditions, safe boundaries, and hazard controls necessary to protect workers, the public, and the environment from adverse consequences. Refer to 10 CFR 830.202 and 10 CFR 830.204 for a verbatim description of the requirements applicable to the development of a Documented Safety Analysis (DSA). These analyses and hazard controls constitute the safety basis upon which the contractor and DOE rely to conclude that the facility can be operated safely. Performing work consistent with the safety basis provides reasonable assurance of adequate protection of workers, the public, and the environment. This Guide elaborates on the DSA development process and the safe harbor provisions of Appendix A to 10 CFR 830 Subpart B.

2. APPLICABILITY

The information contained in this Guide is intended for use by all Department elements, including the National Nuclear Security Administration (NNSA), and all contractors for a DOE-owned or DOE-leased Hazard Category 1, 2, or 3 nuclear facility or nuclear operation. As described in 10 CFR 830.2, DOE nuclear activities that are regulated through a license by the Nuclear Regulatory Commission (NRC) or a state under an Agreement with the NRC, including activities certified by the NRC under section 1701 of the Atomic Energy Act (Act); activities conducted under the authority of the Director, Naval Nuclear Propulsion, pursuant to Executive Order 12344, as set forth in Public Law 106–65; transportation activities which are regulated by the Department of Transportation; and activities conducted under the Nuclear Waste Policy Act of 1982, as amended, and any facility identified under section 202(5) of the Energy Reorganization Act of 1974, as amended; and activities related to the launch approval and actual launch of nuclear energy systems into space are exempt from the DSA rule and therefore do not need to follow this guidance. Accelerators and their operations are excluded from the safety basis requirements of the rule.

3. OVERVIEW OF THE GUIDE

Section 4 contains generally applicable implementation guidance for the requirements of 10 CFR 830 for DSAs (section 4.1). Section 4.2 contains specific implementation guidance for each of the rule's safe harbor methodologies for developing a DSA. Sections 4.3 and 4.4 address annual updates of DSAs and DOE's approval of DSAs. Appendix A addresses new DOE nuclear facilities designed under the provisions of DOE Standard (STD)-1189, *Integration of Safety into the Design Process*, and the transition from a Preliminary DSA (PDSA) to an operational DSA, as well as approvals for procurement and construction activities in advance of approval of a PDSA. Appendix B contains the references for this Guide.

4. IMPLEMENTATION GUIDANCE

4.1 Documented Safety Analysis

The DSA for a DOE Hazard Category 1, 2 or 3 nuclear facility (including NNSA Hazard Category 1, 2, or 3 nuclear facilities), in accordance with 10 CFR 830.204 must, as appropriate for the complexities and hazards associated with the facility or activity:

- describe the facility, activities, and operations (including the design of safety structures, systems, and components (safety SSCs), and the work to be performed);
- provide a systematic identification of both natural and manmade hazards associated with the facility;
- evaluate normal, abnormal, and accident conditions, including consideration of natural and manmade 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;
- 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 them current at all times and controlling their use;
- define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection; and
- with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a criticality safety program that—
    - ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions,
    - identifies applicable nuclear criticality safety standards,[1] and
    - describes how the program meets applicable nuclear criticality safety standards.

In accordance with 10 CFR 830.204, a DSA must provide a systematic identification of both natural and man-made hazards to demonstrate that all relevant accidents have been considered, appropriate preventative and mitigative measures have been included, and that the consequences of these accidents are acceptably low for the protection of workers, the public, and the environment. The facility documentation (equipment specifications, procedures, safety programs, etc.) should be in sufficient detail to support the safety analyses.

10 CFR 830.204(b)(3) requires that a contractor consider the need for analysis of accidents which may be beyond the design basis of the facility in developing the DSA. Beyond design

[1] DOE O 420.1 provides criticality safety requirements that need to be incorporated into the identification process.

basis accidents (BDSA) are events that are not expected to occur at a facility, but are nevertheless considered in the DSA. Accidents beyond the design basis accidents which should be considered include:

- More severe natural phenomena events than those prescribed for in DOE natural phenomena hazards standards.
- More severe external events (e.g., airplane crashes) than those prescribed for in DOE accident analysis standards.
- Failure of a hazard control(s) that maintain important safety functions, such as energy removal (e.g., from fires or decay heat) or confinement.
- Extended Station Blackout (loss of all AC and DC power for days) both as an initiating event and, as a consequence following a DBA analyzed in the DSA.

The analysis should be focused on options for any additional preventive or mitigative controls or actions, or options for improving the robustness of safety systems that may be needed in response to the occurrence of BDBAs. This analysis is intended to provide insights into the safety margins that the nuclear facility design has for responding to the bounding conditions that are represented for DBAs.

In some cases, an evaluation of accident management strategies, resources necessary for implementing such strategies, as well as potential impacts of the events on collocated facilities, site-wide infrastructure and availability of the emergency management resources may also be warranted. The analysis also provides insights into practical measures that could be instituted before or after an event to monitor and mitigate conditions following a BDBA. Realistic (e.g., best estimate) BDBA analysis need not include the conservatisms normally applied when performing DBA analyses.

The DSA should document the scope and method of how BDBAs were analyzed, results of a realistic analysis of impact of failure of hazard controls, and results of analysis of any additional opportunities to mitigate BDBAs. These analyses can serve as bases for cost-benefit considerations for improvements, either for the facility or associated with enhanced emergency management capabilities. It may be appropriate to include some BDBA considerations into the emergency plans of the DOE and non-DOE organizations that could potentially be called upon to respond to a BDBA.

The coordination with emergency management to plan for responses appropriate for the occurrences of BDBAs could also lead to plans for design changes with appropriate considerations of costs and benefits. An example of this possibility is the provision of standardized connections external to the facility for pumped water supply for cooling or fire suppression and/or electrical supply by emergency diesels brought in through emergency response capabilities.

Table 1 identifies acceptable methods for preparing a DSA. The primary objectives of the DSA process are to provide the bases for approval of new facilities and operations as well as continued safe operations of existing facilities and major modifications thereto and eventual

decommissioning, define and control the safety bases and commitments and provide the analytical rationale for operations as delineated in 10 CFR 830.205, "Technical Safety Requirements." The "safe harbor" provisions in Table 1 include "successor documents." As these safe harbor documents are improved, new DSAs and updates to existing DSAs should reflect the new guidance.

Alternative methods or significant deviations from the safe harbor methods, if proposed, in accordance with 10 CFR 830.204, must have the approval of the responsible DOE organization, including where applicable NNSA, and the concurrence (or comment if an NNSA facility is involved) of the DOE Office of Health, Safety and Security (HSS) Requests for such approvals should be submitted to the appropriate line organization with a copy to the HSS. The request should include the following elements:

- technical description of the alternative method or deviation (may be in form of a topical report);
- justification for the request;
- intended application(s);
- record and results of internal peer reviews of the alternative method or deviation; and
- evidence that use of the alternative methodology or deviation would result in an equivalent or otherwise adequate level of safety for the public, the workers, and the environment compared to the applicable safe harbor method.

Table 1. Safe Harbor Methods for DSAs.

The contractor responsible for:	may prepare its documented safety analyses by:
(1) a DOE reactor	using the method in U.S. Nuclear Regulatory Commission Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants*, or successor document.
(2) a DOE nonreactor nuclear facility	using the method in DOE-STD-3009-94, Change Notice No. 1, January 2000, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, dated July 1994, or successor document.
(3) a DOE nuclear facility with a limited operational life[2]	using the method in either: (1) DOE-STD-3009-94, Change Notice No. 1, dated January 2000, or successor document, or (2) DOE-STD-3011-94, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans*, dated November 1994, or successor document.
(4) the deactivation or the transition surveillance and maintenance of a DOE nuclear facility	using the method in either: (1) DOE-STD-3009, Change Notice No. 1, dated January 2000, or successor document, or (2) DOE-STD-3011-94 or successor document.
(5) the decommissioning of a DOE nuclear facility	(1) using the method in DOE-STD-1120-98, *Integration of Environment, Safety, and Health into Facility Disposition Activities*, dated May 1998, or successor document; (2) using the provisions in 29 CFR 1910.120 (or 29 CFR 1926.65 for construction activities) for developing safety and health programs, work plans, health and safety plans (HASPs), and emergency response plans to address public safety, as well as worker safety; and (3) deriving hazard controls based on the safety and health programs, the work plans, the HASPs, and the emergency response plans.
(6) a DOE environmental restoration activity that involves either work not done within a permanent structure or the decommissioning of a facility with only low-level residual fixed radioactivity.	(1) using the method in DOE-STD-1120-98 or successor document, and (2) using the provisions in 29 CFR 1910.120 (or 29 CFR 1926.65 for construction activities) for developing a safety and health program and a site-specific HASP (including elements for emergency response plans, conduct of operations, training and qualifications, and maintenance management).

[2] A limited life facility is one which has an approved deactivation plan (removal of hazards) calling for cessation of operations within a stated period (5 years). This plan should include required funding action and plan change control to ensure relevancy.

Table 1. Safe Harbor Methods for DSAs (continued).

The contractor responsible for:	may prepare its documented safety analyses by:
(7) a DOE nuclear explosive facility and the nuclear explosive operations conducted therein	developing its DSA in two pieces: (1) a safety analysis report for the nuclear facility that considers the generic nuclear explosive operations and is prepared in accordance with DOE-STD-3009, Change Notice No. 1, dated January 2000, or successor document, and (2) a hazard analysis report for the specific nuclear explosive operations prepared in accordance with DOE-STD-3016-99, *Hazards Analysis Reports for Nuclear Explosive Operations*, dated February 1999, or successor document.
(8) a DOE Hazard Category 3 nonreactor nuclear facility	using the methods in Chapters 2, 3, 4, and 5 of DOE-STD-3009, Change Notice No. 1, dated January 2000, or successor document to address in a simplified fashion: (1) the basic description of the facility/activity and its operations, including safety SSCs; (2) a qualitative hazards analysis; and (3) the hazard controls (consisting primarily of inventory limits and safety management programs) and their bases.
(9) transportation activities	(1) preparing a safety analysis report for packaging in accordance with DOE O 460.1A, *Packaging and Transportation Safety*, or successor document and (2) preparing a transportation safety document in accordance with DOE G 460.1-1, *Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety*, dated 6-5-97, or successor document.
(10) transportation and onsite transfer of nuclear explosives, nuclear components, Naval nuclear fuel elements, Category I and Category II special nuclear materials, special assemblies, and other materials of national security	(1) preparing a safety analysis report for packaging in accordance with DOE O 461.1, *Packaging and Transportation of Materials of National Security Interest*, dated 9-29-00, or successor document and (2) preparing a transportation safety document in accordance with DOE M 461.1-1, *Packaging and Transfer of Materials of National Security Interest Manual*, dated 9-29-00, or successor document. This Manual canceled by DOE O 461.2

4.2 Safe Harbor Methodologies

In accordance with 10 CFR 830.204, the preparation of DSAs must conform to one of the methodologies set forth in Table 2 of Appendix A of 10 CFR 830 (included here as Table 1 for the user's convenience) or an alternate methodology approved by DOE. These methodologies are called "safe harbors" in 10 CFR 830.

Each of the safe harbors has a methodology specific to the application to satisfy the requirements for the development of a DSA as described in 10 CFR 830.204 for the hazards identification, safety analysis, and derivation of hazard controls. DOE-STD-3009 is a safe harbor for any of the specialized areas covered by the other safe harbors (with the exception of Hazard Category 1 nuclear reactors) and can be used in lieu of any of them. An expectation associated with any of the safe harbors is that the safety classification guidance for safety SSCs and specific administrative controls (SACs) of DOE-STD-3009 will be used in developing the DSA.

As long as a facility is a Category 1, 2 or 3 nuclear facility, in accordance with Subpart B of 10 CFR 830, Safety Basis Requirements, it must have a safety basis, including a DSA, hazard controls [usually technical safety requirements (TSRs)], and an unreviewed safety question (USQ) process. In its life cycle, a nuclear facility generally has a mission-oriented or production phase, after which it is shut down and either devoted to another mission or is declared excess and enters into a disposition process. Transition activities occur between operations and ultimate disposition.

4.2.1 DOE Reactors (Safe Harbor 1)

Most DOE large reactors use Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants*. There is an ANS standard that provides guidance for small research reactors (ANSI/ANS-15.21, *Format and Content for Safety Analysis Reports for Research Reactors*). NUREG-1537 (*Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors*) also provides guidance for nonpower reactors. However, none of these reactor formats was written for DOE reactors and each has left out several topics that should be included. For DOE reactors, in addition to the topics discussed in Regulatory Guide 1.70, hazard analysis and categorization of the facility and applicable facility design codes and standards should be added. DOE-STD-3009 provides specific guidance for the content and organization DOE expects for these additional topics. DSAs for reactors often use different safety classification terminology (e.g., conforming to NRC Regulatory Guide 1.70) rather than that identified in 10 CFR 830.

DOE O 5480.30, *Nuclear Reactor Safety Design Criteria*, contains a requirement that all DOE reactor designs be evaluated and compared with the design criteria of the Order and the results included in the DSA. That Order should also be consulted for reactor DSA content guidance.

4.2.2 Hazard Category 2 and 3 Nonreactor Nuclear Facilities (Safe Harbor 2 and 8)

DOE has developed DOE-STD-3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facilities Documented Safety Analysis*. This Standard provides both a standardized format and suggested content for nonreactor nuclear facilities with an emphasis on existing Hazard Category 2 and 3 facilities. DOE-STD-3009 has also been used successfully to prepare DSAs for critical assemblies. However, it may also prove useful, in the case of critical assemblies, to consult ANSI/ANS-15.21 to assure completeness regarding criticality hazards.

The DSA requirements for a Hazard Category 3 nuclear facility are not as extensive as those for higher hazard facilities. A contractor with a DOE nonreactor, Hazard Category 3 nuclear facility can apply the methods defined in DOE-STD-3009 to address the following topics, as applicable, in the DSA and the TSRs (See Table 1):

- facility description and operation, including safety SSCs;
- process hazards analysis; and
- the hazard controls and their bases.

For site wide safety management programs (for example, radiation protection), the DSA should explain the features of those programs that are important to the facility safety basis and can refer to the site wide program documentation for the details.

4.2.3 DOE Facilities with Limited Operational Life and Deactivation or Transition Surveillance and Maintenance (Safe Harbors 3 and 4)

DOE-STD-3011, *Guidance for the Preparation of Basis for Interim Operations (BIO) Documents* provides the format and content for developing a BIO. DOE-STD-1120, *Integration of Environment, Safety, and Health into Facility Disposition Activities*, provides implementation insight and guidance clarifying the development and use of the BIO as a DSA.

Traditionally, DSAs have been used as the long-term safety basis document for nuclear facilities usually under steady-state conditions. There are primarily two cases where the rule allows a BIO to be used as the appropriate safety basis documentation: (1) for a DOE nuclear facility with a limited operational life and (2) during transition phases, including transition surveillance and maintenance and deactivation. A BIO is applicable to a nuclear facility in transition as the facility moves through the appropriate life cycle states, providing accurate safety documentation for rapidly changing activities. A BIO can also be linked to a series of tasks or activities. DOE O 430.1B, *Real Property Asset Management*, and its corresponding Guides also provide guidance on using a BIO.

The following discusses situations when use of a BIO is appropriate

4.2.3.1 Deactivation

Deactivation refers to the process of placing a facility in a stable[3] and known condition including the removal of readily removable hazardous and radioactive materials to ensure adequate protection of the worker, public health and safety, and the environment, thereby limiting the long-term cost of surveillance and maintenance. Deactivation activities include the removal of energy sources, draining and/or de-energizing nonessential systems, removal of stored radioactive and hazardous materials, and related actions. However, the process of deactivation may not include all decontamination necessary for the dismantlement and demolition phase of decommissioning.

4.2.3.2 Transition Surveillance and Maintenance

Surveillance and maintenance activities are performed during all phases of the facility life cycle. "Transition surveillance and maintenance" refers to the surveillance and maintenance activities that occur after the production (or normal life mission) phase of a facility when these activities are the predominant activities at the facility and does not include the surveillance and maintenance conducted during deactivation or decommissioning activities. A BIO should address the safety of the conduct of surveillance and maintenance activities and the maintenance of the facility in a stable and known condition. Surveillance and maintenance activities include providing periodic inspections and maintenance of structures, systems, and equipment necessary for the satisfactory containment of contamination and for protection of workers, the public, and the environment. Maintenance of the facility in a stable and known condition includes actions to prevent the alteration in chemical makeup, physical state, and/or configuration of a hazardous substance or radioactive material. It also includes actions taken with regard to physical SSCs (e.g., roofs, ventilation). The safety of the conduct of surveillance and maintenance activities, other than transition surveillance and maintenance activities, that occur following completion of the program mission, is addressed in the documented safety basis for that respective period (e.g., deactivation BIO).

4.2.3.3 Shutdown with Uncertain Future

When a facility is shut down, that is, its production or normal mission has ended, and its future has not been determined but could include a restart, a changed production mission, or eventual deactivation and decommissioning, the question of how to address the facility safety basis arises. For some limited time, it may be adequate to maintain the facility under the operational safety basis until management decisions are made for the path forward for the facility. However, this can be expensive because of facility staffing requirements and maintenance of equipment, etc. and may be excessive for an inactive mode. Additionally, hazards may develop that may be

[3] Stable means that a facility and its contents are in a condition that eliminates or mitigates hazards and ensures adequate protection to workers, the public, and the environment. Achieving and maintaining stability may require actions to prevent alteration in the chemical makeup, physical state, and/or geometry (leading to increased reactivity) of a hazardous substance or radioactive material. Achieving and maintaining stability also involves actions taken with regard to physical structures (e.g., roofs), systems (e.g., ventilation), and components.

peculiar to a long-term shutdown mode, such as chemical changes in storage tanks leading to explosive mixtures, corrosion of materials, etc., that an operational safety basis might not have considered. Therefore, the length of time that a shutdown facility may continue under an operational safety basis cannot be specified for all situations. Certainly, it should not extend longer than the operational safety basis can be complied with. For example, if the operational staff starts to be assigned elsewhere, then staffing requirements cannot be met. It would not be appropriate to just change the staffing requirements from that required by the existing safety basis, because then that safety basis likely could not be adequately complied with. In any case, the period before a transition surveillance and maintenance safety basis is entered into should not be more than about a year, until an annual safety basis update is completed.

Hazards are being removed during facility disposition activities. A BIO per DOE-STD-3011 and DOE-STD-1120 needs to describe the appropriate transition activity and process in place so that a controlled removal of hazards and safety features can be reflected in the documentation. The USQ process (refer to DOE G 424.1-1) can be used as a management tool for determining whether the removal of hazards, safety systems and equipment, and corresponding controls needs to be approved by DOE.

4.2.4 Decommissioning of a DOE Nuclear Facility (Safe Harbor 5)

The contractor responsible for decommissioning of a DOE Hazard Category 1, 2 or 3 nuclear facility may prepare its DSAs using the method in DOE-STD-1120; using the provisions in 29 CFR 1910.120 (except paragraph (P), treatment, storage and disposal requirements), or 29 CFR 1926.65 for construction activities, for developing safety and health programs, comprehensive work plans, Health and Safety Plans (HASPs), and emergency response plans to address public safety, as well as worker safety; and deriving hazard controls based on the safety and health programs, the work plans, the HASPs, and the emergency response plans.

4.2.4.1 Background

The use of a HASP for the decommissioning DSA parallels the OSHA requirements in 29 CFR 1910.120 (except paragraph (P), treatment, storage and disposal requirements) and 29 CFR 1926.65 during decommissioning. The hazards faced during decommissioning operations are primarily related to worker safety, and the OSHA regulations were aimed primarily at protecting the workers. DOE has committed in a memorandum of understanding with the Department of Labor to conduct decommissioning and disposition work according to OSHA requirements (see http://www.hss.doe.gov/HealthSafety/WSHP/rule851/MOU_DOE_OSHA1992.pdf). A detailed comparison of the two sets of requirements for contractors performing decommissioning activities was performed. It was determined that the requirements of the DSA could be met by (1) complying with 29 CFR 1910.120 and 29 CFR 1926.65 for safety and health programs, work plans, HASPs, and emergency response plans, (2) deriving corresponding TSRs and administrative controls, (3) addressing public safety, as well as worker safety in an additional sections of the safety and health programs, work plans, HASPs, and emergency response plans, and (4) submitting the documents required by these alternative requirements to DOE for approval.

4.2.4.2 Safety and Health Programs

The safety and health program provides the mechanism for identifying, evaluating, and controlling health and safety hazards and providing for emergency response. The program documentation includes an organizational structure, a comprehensive work plan, a facility- or activity-specific HASP, the medical surveillance program, the employer's standard operating procedures, the safety and health training, the emergency response plan, and any interfaces between the site wide programs and facility- or activity-specific activities. The program descriptions prescribed in the rule can be included in the safety and health program. In addition to the emergency response plan and training and qualifications, conduct of operations, and maintenance management programs should be provided in the safety and health program documentation.

4.2.4.3 Comprehensive Work Plan

The comprehensive work plan addresses and defines the tasks and objectives of decommissioning or environmental restoration activities, including the logistics and associated resources to execute and achieve the objectives. It identifies specific methods for accomplishing the stated tasks and objectives, including operating procedures. The comprehensive work plan should also document a description of the facility and site. The comprehensive work plan can also be used to document/reference relevant safety management programs, per Section 830.204(b)(5), including the USQ process, and management of change procedures.

4.2.4.4 Health and Safety Plans (HASPs)

The facility- or activity-specific HASP addresses the safety and health hazards of each phase of the decommissioning or environmental restoration operation and includes the specific requirements and procedures and other controls for worker protection.

The safety and health hazard analyses section of the HASP generally addresses the task-level hazards to workers, which is the appropriate level for the select environmental restoration activities. For these activities, the normal HASP that examines radiological issues is the appropriate DSA with the addition of nuclear hazard classification to the HASP hazard analysis section. For decommissioning activities other than those specified in the definition of selected environmental restoration activities, the hazard section of the HASP should address the facility-level nuclear safety analysis, including accident analysis and consequences to the public and workers. The following topics could be addressed in the hazard analysis section of the HASP, or as an appendix to the HASP, potential hazards affecting the public, controls for these hazards, and corresponding TSRs or administrative controls that may be required. HASPs used as nuclear safety basis documents need to be approved by DOE, including the NNSA where applicable, prior to commencing decommissioning operations.

Hazard baseline documentation provides a formal record of the plan for performing the work, all identified hazards, including those that workers may encounter during disposition work activities, and the controls that are established to support safe work execution. The type and extent of hazard baseline documentation should be commensurate with the scope of activities to

be performed, the hazards associated with the activities, and the controls necessary to do the work safely. DOE-STD-1120, *Integration of Environment, Safety and Health into Facility Disposition Activities*, provides criteria, organized primarily around facility types that may be used in grading these considerations. For purposes of determining hazard baseline documentation, facilities should be designated as Hazard Category 1, 2, or 3 nuclear, or radiological (i.e., below Hazard Category 3 nuclear facility definitions provided in DOE-STD-1027-97, Change Notice No. 1, *Hazard Categorization and Accident Analysis Techniques for Compliance with 5480.23)*, or nonnuclear. The types of hazard baseline documents that support safe facility disposition activities typically are a work package, a HASP (for the specific case of decommissioning), a documented hazard analysis, a basis for interim operation, or a DSA.

HASPs are meant to be responsive to changed conditions such as hazards, hazard controls, and activities performed. When a HASP is revised and updated, in accordance with 10 CFR 830.202, DOE must re-approve it before decommissioning operations may continue. As described in DOE-STD-1120, the USQ process can be used to determine whether DOE is required to approve the deletion of safety systems and corresponding controls as the hazards are removed.

4.2.5 Environmental Restoration Activities (Safe Harbor 6)

DOE-STD-1120 provides guidance for developing the DSA for decommissioning a facility that involves only low-level residual fixed radioactivity. Although this Standard was not originally intended for nonfacility environmental restoration activities (e.g., remediation of a burial ground or other activities that require earth moving), the guidance provided in this Standard should be useful for planning and conducting environmental restoration activities that involves either work not done within a permanent structure or the decommissioning of a facility with only low-level residual fixed radioactivity. Appendix A of the Standard is particularly helpful in identifying environmental requirements independently of whether the work is performed within a permanent structure or outside a permanent structure. Similarly, a contractor decommissioning a facility that involves only low-level residual fixed radioactivity should develop a HASP that identifies environmental requirements.

Decommissioning a facility that involves only low-level residual fixed radioactivity which remains following reasonable efforts to remove radioactive systems, components, and stored materials and that does not prudently require the use of active safety systems or components designed to prevent or mitigate the accidental release of hazardous radioactive materials. The safety basis for environmental restoration activities parallels the Occupational Safety and Health Administration (OSHA) requirements in 29 CFR 1910.120 (except paragraph (P), treatment, storage, and disposal requirements) and 29 CFR 1926.65. The hazards faced during environmental restoration operations also are primarily worker safety related and the OSHA regulations were aimed primarily at protecting the workers. Therefore, use of the OSHA requirements was made an acceptable alternative for meeting the nuclear safety rules.

A HASP can be used as alternative documentation to satisfy both 10 CFR 830 nuclear safety basis requirements and the OSHA worker safety requirements. DOE-STD-1120 provides guidance on the format and content for developing a HASP. The HASP is meant to be revised as

necessary to reflect changes in hazards, hazard controls, and activities performed. In addition to developing the HASP, the rule requires the contractor to provide a description of the emergency response, conduct of operations, training and qualification, and maintenance management programs. Generally, these descriptions would simply identify the applicable/necessary portions of the site wide programs and describe how they would be applied for these activities.

4.2.6 Nuclear Explosive Facilities and Operations (Safe Harbor 7)

The safety basis for nuclear explosive operations (NEOs) in nuclear explosive facilities is constructed in two parts. The first is oriented towards the facility and the safety systems and controls associated with the facility, per se. The second is oriented towards the operations on a specific NEO and the controls directly associated with those operations. The reason for this partition of the safety basis is that nuclear explosive operations are typically short-term (months), and many different operations may be carried out in the same facility (sequentially). With this scheme, the same facility safety basis can be used with multiple nuclear explosive operations. For this reason, the DSA/TSR component of the NEO authorization documents is broken into two parts. The first part of the documentation is a generic DSA/TSR portion based on DOE-STD-3009 in format and content or equivalent that assumes a specially constructed generic NEO as the basis for its hazard and accident analysis.

The second part of the documentation is a hazard analysis report (HAR) based on DOE-NA-STD-3016 in format and content, which uses a specific NEO as the basis for its hazard and accident analysis. The HAR contains a detailed hazard analysis of the specific NEO, the facilities (as appropriate and as a complement to the facility DSA), and potential deviations from the expected operational parameters that can result in accidents affecting the worker, the public, or the environment. The HAR is an integrating document for all safety basis issues related to a specific NEO. The TSRs derived from the HAR for the specific NEO are considered an integral part of the safety basis and are referred to as the operation-specific TSRs. The USQ process would use both of these parts of the overall NEO authorization documents for its evaluations, just as the DSA/TSR construct is used for the typical nuclear facility safety basis.

The specially constructed NEO as the basis for the generic operation of the DSA/TSR should possess certain attributes. First, the generic operation should be comprehensive in nature, in the sense that it would need to embody all similar and specific operations envisioned for the subject facilities. Thus, while certain operations would use the same facility systems, such as cranes, filtration, ventilation, and fire protection, others might have requirements for operation-specific SSCs, such as a dissolution station. In other words, the concept of the generic operation is one that establishes the mission- and safety-related design requirements for the facilities. Second, the generic operation should be bounding in terms of the requirements that it will impose on the safety-related controls. Thus, material at risk (e.g., radionuclides) and other hazardous materials (e.g., explosives, combustibles), and their relationship to accident phenomenology (e.g., release from door cracks versus from blown-off ceiling) should be established in such manner that the resulting engineered or administrative controls would be capable of meeting their functional requirements for each specific NEO. These requirements on the generic operational characteristics are necessary to ensure that facility safety design remains valid for the intended operations. Minimal future modifications would be needed for continued facility safety

assurance. Thus, the DSA for generic operations would need to have this kind of information to the degree of completeness that would be required to design the facility from scratch, considering all of the planned operations that the facility would need to accommodate in the future.

The HAR generates a detailed hazard analysis of the specific NEO, including all relevant accident scenarios and associated controls. Each HAR should be compared with the facility DSA to ensure they are consistent and appropriate, and not in conflict. This hazard analysis should be thorough, and requires evaluation of the complete spectrum of hazards and accidents. The effort is largely qualitative, and at times semi quantitative; it forms the basis for the entire safety analysis effort. Detailed probabilistic calculations are neither expected nor required. Accident scenarios should be considered based on the physical possibility of the phenomena. The use of lower-binning threshold frequencies should not be used as cutoff criteria for dismissing physically credible low-probability accidents. Generic TSRs are derived from generic DSAs. They encompass all of the controls derived from the hazard analysis, either explicitly (e.g., limiting conditions of operation) or implicitly (e.g., mention of various safety management programs in the administrative controls section). TSR related requirements on controls are in effect at all times since they apply to all (generic) operations at the facility.

The control requirements derived from the HAR-related TSRs remain in effect only for the duration of the specific operation. They should be checked to ensure they are consistent with the facility-based (permanent) TSRs to ensure there is no conflict. In the event facility-based TSRs conflict with HAR-related TSRs, HAR-related TSRs, the conflict needs to be resolved.

The DSA construct, and to the same extent, its TSR and the HAR and operation-specific TSR for nuclear explosive facilities and operations, are inherently different from their typical nuclear facility counterparts in several respects. It is important to accommodate the key differences when developing the authorization documents for a NEO. As examples consider the concept of hazard categorization for nuclear facilities and both the concept and the process for designation of safety SSCs.

In the area of safety system designation, it is instructive to revisit both the concept and the process. The safety class designation process for SSCs proceeds from first the determination of need for such designation at a given facility (including all of its associated processes), to the actual selection process among the individual safety systems. The determination of "need for safety class designation" at a nuclear explosive facility is a moot point, vis-a-vis the concept of potential offsite consequences. In other words, there is no need for performing an explicit unmitigated release consequence analysis in accordance with Appendix A of DOE-STD-3009 to determine that nuclear explosive facilities needs to have safety class SSCs for accident prevention or mitigation. This means that any accident scenario that can cause an explosive dispersal of plutonium, or its source-term equivalent, should be prevented or mitigated by a safety class SSC (if feasible). This is because of the nature of NEOs that are conducted in a variety of facilities (within the same site) and locations, including onsite and offsite transportation, and the desire to remove a layer of uncertainty (i.e., dose consequence calculation) from the analytical process.

In addition to SERs for NEO-related authorization documents, DOE performs an extra technical review of NEOs to focus on the unique hazards of these activities. These extra technical reviews are called nuclear explosive safety (NES) master- and program-specific studies. The NES studies can generate additional NES rules over those already generated in the HAR that should be reincorporated into the HAR. This process ensures that the HAR remains the integrating operation-specific authorization document.

The NES master studies provide a generic NES review of information documented in the DSAs.

If a conflict occurs between controls proposed for a lower-order consequence such as personnel contamination and those proposed for a higher-order consequence such as from nuclear detonation, and the conflict cannot be resolved, the higher-order consequence should dictate which control remains in the authorization basis and an exemption should be sought from any rule requirements (such as those of 10 CFR 835) if deletion of the control affects the ability to meet the rule.

Program-specific NES studies provide a more specific review of information documented in a HAR. The NES studies are an important part of safety assurance for NEOs. These program studies provide an expert-based evaluation of nuclear explosive operations processes, tooling, equipment, facilities, and management systems of with special emphasis on high-consequence scenarios unique to specific NEOs. The HAR is the integrating document for all safety basis issues related to a specific program. The NES study generates a report that is an element of the NEO authorization documents.

Facility and NEO readiness reviews are important tests of whether the provisions of the NEO authorization documents (including all safety management program elements) are properly in place. They emanate from the safety basis and are an integral part of the overall safety assurance process.

4.2.7 Transportation Activities (Safe Harbors 9 and 10)

Offsite transportation regulated by the Department of Transportation is not covered by 10 CFR 830. Offsite transportation of national security interest material, including nuclear explosives, is covered under the provisions of 10 CFR 830. Offsite transportation of nuclear explosives is governed by DOE O 452.2D. Onsite transportation or transfer of all nuclear material is covered by 10 CFR 830 as provided under safe harbor provisions of the rule.

Onsite transportation of nuclear explosives should comply with the safety requirements of DOE O 461.1B and other DOE-approved subordinate documents. Onsite transportation of nuclear explosives is also governed by the safety requirements of DOE O 452.2D. Onsite transportation or transfer of other than nuclear explosives, all other nuclear material, including other national security interest material, should comply with the safety basis requirements of DOE O 460.1C and DOE O 461.2.

Transportation TSRs are addressed in DOE G 423.1-1a, *Implementation Guide for Use in Developing Technical Safety Requirements*. For types of transportation operations that remain unchanged for long periods, it is generally good practice to incorporate the controls

into the TSRs for the transportation and storage facilities or the overall site TSRs. Likewise, for facilities that are designed for continuous use in transporting and storing nuclear materials, it is expected that the facility-specific controls would be incorporated into the facility's TSRs rather than the site's generic transportation documents.

4.3 Annual DSA Updates

In accordance with 10 CFR 830.202, contractors must ensure that information in a DSA is current and applicable. The safety basis rule applies to all facilities that satisfy the criteria for Category 3 or higher hazard nuclear facilities except those specifically excluded in section 830.2. Therefore, when a facility changes status, say from a production or mission-oriented status to inactive, transition surveillance and maintenance, deactivation activities, or decommissioning, the DSA and TSR associated with the facility or activity needs to be updated to describe the activities, consider the hazards associated with the new status, and the controls associated with these hazards. Any facility or activity DSA that does not reflect its current status is out of compliance with the safety basis rule. The annual[4] update required by the rule applies to all DSAs, including those not yet rule compliant. DOE remains accountable for safety during the period those DSAs are being upgraded.

The Unreviewed Safety Question rule (10 CFR 830.203) has a primary role in preserving the DOE safety basis for each nuclear facility. The concept of the unreviewed safety question allows contractors to make physical and procedural changes and to conduct tests and experiments without prior DOE approval, as long as these changes do not affect the safety basis of the facility.

When a facility does not change status, but does have changes that affect the safety basis, the DSA and TSR should be updated to reflect those changes. Usually the changes will be the subject of a USQ determination. If there are no changes, notifying DOE of that fact is sufficient for the update. The rule is silent on a cutoff date for changes to the facility to be included in a DSA update. This can be determined on an ad hoc basis but should be compatible with the annual report on USQ determinations (See 10 CFR 830.203). The USQ determinations and associated safety analyses as well as supporting safety analyses for any DOE-approved changes to a facility are considered part of the safety basis until incorporated in an annual update.

The contractor responsible for a facility can provide annual DSA updates by—

- certifying that the existing DSA remains fully applicable;
- providing supplements or amendments to make the DSA current, subject to DOE approval; or
- submitting, for DOE approval, a DSA, which is proposed to supersede the current DSA.

Generally, depending upon the complexity of the facility, it may be impractical to incorporate the most recent USQ determinations and facility changes into the DSA annual update. However, at least those implemented six months or more before the submittal of the annual update should be included.

[4] Annual is intended to mean approximately 12 months with flexibility to coordinate with other commitments.

Consistent with the integrated safety management requirements for feedback specified in the Department of Energy Acquisition Regulation (DEAR) clause (48 CFR 970.5223-1), DOE expects that updates of DSA for facilities in operation for 1 year or more will address the results of the experience feedback program for that facility. Additionally, relevant experience from other facilities both within DOE and from the commercial nuclear industry should be considered. All such relevant information bearing upon the safety of the facility should be examined as part of the update. DOE also expects that relevant research results at nuclear facilities will be evaluated relative to the safety of each DOE nuclear operation as part of the updating of that facility's DSA.

4.4 Facility Authorization and DOE's Approval of DSA

DOE employs DSAs, TSRs, and Safety Evaluation Reports (SERs) as the principal safety documentation in its decision to authorize operation of nuclear facilities, including NNSA nuclear facilities. DOE-STD-1104, *Review and Approval of Nonreactor Nuclear Facility Safety Basis and Safety Design Basis Documents,* provides guidance on the preparation of SERs. One of the guiding principles is, "The Safety Evaluation Report (SER) is primarily a management document that provides the approval authority, the basis for the extent and detail of the DSA review, and the basis for any conditions of DSA approval."

DOE line managers, including NNSA line managers supported by safety professionals, need to satisfy themselves that all the hazards associated with a nuclear facility have been identified and appropriate controls have been put in place to prevent accidents and mitigate consequences of accidents associated with those hazards. Generally, it is most effective for DOE reviewers to be engaged and interact with the contractor during the DSA development process so that the reviewers know the safety issues and how they were resolved. Judgments need to be made regarding what constitutes appropriate controls. These judgments should consider the level of the hazard and potential consequences, the practicality and effectiveness of possible control options, the importance of the mission of the facility, and other relevant factors, if any. These are all elements of the graded approach.

Appendix A

New Facility Considerations

A.1 Design Activities

DOE-STD-1189**,** *Integration of Safety into the Design Process*, governs the development of a safety design basis from conceptual design through final design, including the development of a PDSA during final design.

Section 830.206 of 10 CFR 830 allows limited procurement and construction activities before a PDSA is approved if DOE determines that the activities are not detrimental to public health and safety or the environment and are in the best interests of DOE. The following guidance describes the contractor actions needed to request such approval and the DOE actions needed to review and approve such requests.

A. CONTRACTOR ACTIONS

For each limited procurement and construction request the contractor describes the activity requested, the reason for the request, the benefit to DOE for such a request, the effect of delay in conducting such activities, and the risks associated with performing the requested activity before the PDSA is approved.

B. DOE ACTIONS

DOE reviews each request and evaluates:

(1) whether the conduct of the proposed activity will cause a significant adverse impact on the environment, mission, or safety (the nature and extent of such impact should be considered);
(2) whether redress of any adverse impact from the conduct of the proposed activity can reasonably be effected should such redress be necessary;
(3) whether conduct of proposed activities would foreclose subsequent adoption of reasonable or likely alternatives or options; and
(4) the effect of delay in conducting such activities on DOE interests and missions.

Authorization of limited activities does not supersede DOE review of the PDSA. Therefore, the DOE reviewer and approver should balance the benefits of granting authorization for each proposed activity against the possibility that the PDSA may not find the procured or constructed item to be an approved part of the project.

Contractors should prepare a report that addresses the actions in Section A, above, and submit the report to DOE for review and approval. DOE should prepare a report that documents their evaluation and should address the actions in Section B, above, in the DOE safety evaluation report.

DOE expects nuclear facility construction projects to integrate the planning of operational safety and operations management along with safety design as the project progresses from conceptual design through detailed design, procurement, fabrication, construction, and startup testing.

A.2 Preparation of an Operational DSA

The PDSA for a new facility prepared under the guidance of DOE-STD-1189 is of the same format as a DOE-STD-3009 DSA for existing facilities. However, the process of establishing an operational safety basis for a new facility is different from that for an existing facility because the safety in design process of DOE-STD-1189 results in a well documented safety design basis. Appendix B of DOE-STD-3009 contains guidance for transitioning a PDSA to an operational DSA for new facilities. The intent of the Appendix is to bring the safety design basis information developed during the design process into the operational DSA.

Appendix B

References

Federal Rules

1. Title 10 Code of Federal Regulations (CFR) 708, DOE Contractor Employee Protection Program.
2. 10 CFR 820, Procedural Rules for DOE Nuclear Activities.
3. 10 CFR 830, Nuclear Safety Management.
4. 10 CFR 830 Subpart A, Quality Assurance Requirements.
5. 10 CFR 830, Subpart B, Safety Basis Requirements.
6. 10 CFR 835, Radiation Protection for Occupational Workers.
7. 10 CFR 850, Chronic Beryllium Disease Prevention Program.
8. 10 CFR 1021, (DOE) National Environmental Policy Act Implementing Procedures.
9. 29 CFR 1910, Occupational Safety and Health Standards.
10. 29 CFR 1926, Occupational Safety and Health Regulations for Construction.
11. 40 CFR, Environmental Protection Agency

DOE Orders and Manuals

1. DOE O 153.1, *Departmental Radiological Emergency Response Assets*, dated 6-27-07.
2. DOE O 210.2A, *DOE Corporate Operating Experience Program*, dated 4-8-2011.
3. DOE O 225.1B-A, *Accident Investigations*, dated 3-4-2011.
4. DOE 231.1A Chg 1, *Environment Safety and Health Reporting Requirements*, dated 6-3-04.
5. DOE M 231-1, *Occurrence Reporting and Processing of Operations Information*, dated 8-19-03.
6. DOE O 360.1B, *Federal Employee Training*, dated 10-11-01.
7. DOE O 413.1B, *Internal Control Program*, dated 10-28-08.

8. DOE O 413.3B, *Program and Project Management for The Acquisition of Capital Assets*, dated 11-29-10.

9. DOE O 414.1D, *Quality Assurance*, dated 4-25-2011.

10. DOE 420.1B, *Facility Safety*, dated 12-22-05.

11. DOE O 420.2B, *Safety of Accelerator Facilities*, dated 7-23-04.

12. DOE O 422.1, *Conduct of Operations*, dated 6-29-10.

13. DOE O 425.1D, *Verification of Readiness to Startup or Restart of Nuclear Facilities*, dated 4-16-10.

14. DOE O 426.2, *Personnel Selection, Training, Qualification, and Certification Requirements for DOE Nuclear Facilities*, dated 4-21-10.

15. DOE O 430.1B Chg 1, *Real Property Asset Management*, dated 9-24-03.

16. DOE O 433.1B, *Maintenance Management Program for DOE Nuclear Facilities*, dated 4-21-10.

17. DOE O 435.1 Chg 1, *Radioactive Waste Management*, dated 7-9-99.

18. DOE O 440.1B, *Worker Protection Program for DOE (Including the National Nuclear Security Administration) Federal Employees*, dated 5-17-07.

19. DOE O 442.1A, *Department of Energy Employee Concerns Program*, dated 6-6-01.

20. DOE O 451.1B Chg 2, *National Environmental Policy Act Compliance Program*, dated 6-25-10.

21. DOE O 452.2D, *Nuclear Explosive Safety*, dated 4-14-09.

22. DOE O 452.6A, *Nuclear Weapon Surety Interface with the Department of Defense*, dated 4-14-09.

23. DOE O 460.1C, *Packaging and Transportation Safety*, dated 5-14-10.

24. DOE O 461.1B, *Packaging and Transfer or Transportation of Materials of National Security Interest*, dated 12-20-10.

25. DOE O 461.2, *Onsite Packaging and Transfer of Materials of National Security Interest*, dated 12-20-10.

26. DOE O 5480.30, *Nuclear Reactor Safety Design Criteria*, dated 1-19-93.

Standards, Handbooks, and Guides

1. DOE-STD-1027-92, Change Notice No. 1, September 1997, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, dated December 1992.

2. DOE-STD-3009-94, Change Notice No. 3, March 2006, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, dated July 1994.

3. ANS STD 15.21 R2006, *Standard Format and Content for Safety Analyses Reports for Small Research Reactors*, dated 1996.

4. NRC Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition) Revision 3*, dated November 1978.

5. DOE-STD-1104-2009, *Review and Approval of Nonreactor Nuclear Facility Safety Basis and Safety Design Basis Documents*, dated May 2009.

6. DOE-STD-1120-2005, *Integration of Environment, Safety, and Health Into Facility Disposition Activities*, dated April 2005.

7. DOE-STD-1134-99, *Review Guide for Criticality Safety Evaluations*, dated September 1999.

8. DOE-STD-1189-2008, *Integration of Safety into the Design Process*, dated March 2008.

9. DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Non-Reactor Nuclear Facilities*, dated February 2007.

10. DOE-HDBK-3010-94, *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities,* Vols. I and II, dated December 1994.

10. DOE-STD-3011-2002, *Guidance for Preparation of Basis for Interim Operation (BIO) Documents,* dated December 2002.

11. DOE-NA-STD-3016-2006, *Limited Standard: Hazard Analysis Reports for Nuclear Explosive Operations*, dated May 2006.

12. DOE-STD-5506-2007, *Preparation of Safety Basis Documents for Transuranic (TRU) Waste Facilities*, dated April 2007.

13. DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for Use with DOE O 420.1, Facility Safety*, dated 3-28-00.

14. DOE G 420.1-2, *Guide for the Mitigation of Natural Phenomena Hazards for Nuclear Facilities and Nonnuclear Facilities*, dated 3-28-00.

15. DOE G 423.1-1A, *Implementation Guide for use in Developing Technical Safety Requirements*, dated 11-03-10.

16. DOE G 424.1-1B, *Implementation Guide for Use in Addressing Unreviewed Safety Question (USQ) Requirements*, dated 4-08-10.

17. DOE G 460.1-1, *Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety*, dated 6-05-97.

18. NUREG-1537, *Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors*, dated February 1996

19. DOE-HDBK-1132-99, *Design Considerations*, dated April 1999.

20. DOE-NE-STD-1004-92, *Root Cause Analysis Guidance Document*, dated February 1992.