DOE G 421.1-2

Approved: 10-24-01
Sunset Review: 10-24-03

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 and Facility Safety Policy

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Nuclear and Facility Safety Policy

FOREWORD

This Department of Energy (DOE) Implementation Guide is approved for use by the DOE Office of Nuclear and Facility Safety Policy and is available for 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—

Richard Stark
EH-53/270/GTN
U.S. Department of Energy
Washington, D.C. 20585
Phone (301) 903-4407
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 (DSAs) defined in that subpart. The guidance describes the analytical methods, documentation requirements, and safety commitments that go into the development of a comprehensive safety basis and DSA.

In an effort to further improve the implementation of Subpart B of 10 CFR 830, DOE is in the process of updating three standards to support the 830 rule:

- DOE-STD-1104-96, *Review and Approval of Nonreactor Nuclear Facility Safety Analysis Reports*;

- DOE-STD-3009-94, Change Notice No. 1, *Preparation Guide for U.S. DOE Non-Reactor Nuclear Facility Safety Analysis Reports*; and

- DOE-STD-3011-94, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans*.

The successors to these documents should be consulted and used as soon as they become available.

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.

This page intentionally left blank.

CONTENTS

This page intentionally left blank.

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. 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 documented safety analysis (DSA) development process and the safe harbor provisions of the Appendix to 10 CFR 830 Subpart B.

Specifically, paragraphs 830.201, 830.202, 830.204, 830.206, and 830.207, require that a contractor responsible for a DOE Hazard Category 1, 2 or 3 nuclear facility must—

- establish and maintain a safety basis for the facility;
- perform work in accordance with the safety basis and, in particular, with the hazard controls that ensure adequate protection of workers, the public, and the environment; and
- pending issuance of a safety evaluation report in which DOE approves a safety basis for an existing DOE nuclear facility, the contractor responsible for the facility must continue to perform work in accordance with the safety basis for the facility in effect on October 10, 2000, or as approved by DOE at a later date, and maintain the existing safety basis consistent with the rule requirements.

In establishing the safety basis for a Hazard Category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must—

- define the scope of the work to be performed;
- identify and analyze the hazards associated with the work;
- categorize the facility consistent with DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, Change Notice No. 1, September 1997, or successor document;
- prepare a (DSA) for the facility; and
- establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment.

The DSA for a DOE Hazard Category 1, 2 or 3 nuclear facility (including National Nuclear Security Administration (NNSA) Hazard Category 1, 2, or 3 nuclear facilities) 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.

The preparation of DSAs must conform to one of the methodologies set forth in Table 2 of Appendix A of10 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. The use of alternative methods or significant deviations from the safe harbor methods, if

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

proposed, must be approved by the responsible DOE organization as defined in DOE M 411.1-1B, *Safety Management Functions, Responsibilities, and Authorities Manual* (FRAM), including where applicable NNSA, and the concurrence (or comment if an NNSA facility is involved) of the DOE Office of Environment, Safety and Health (EH). Generally, in order to approve an alternative method, the DOE responsible organizations would need to find that the alternative methodology was sufficiently rigorous to provide an equivalent level of safety in the alternative DSA and resulting controls.

Subpart B of 10 CFR 830, Safety Basis Requirements, requires that, as long as a facility is a Category 1, 2 or 3 nuclear facility, 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.

These transition activities can include a period designated in the Appendix to Subpart B as "transition surveillance and maintenance," followed by deactivation, then possibly another period of transition surveillance and maintenance, and then decontamination and decommissioning. While surveillance and maintenance is done during all these periods, the term "transition surveillance and maintenance" is used to designate those periods of time when surveillance and maintenance is the predominant activity at the facility; that is, times other than when deactivation or decontamination and decommissioning is taking place. The rule requires that a safety basis, appropriate to the activities taking place, exists for each of the phases of the life cycle, including each of the transition activities until the facility is no longer a Category 1, 2 or 3 nuclear facility.

2. APPLICATION (830.1–.3)

The information contained in this Guide is intended for use by all Department elements, including the NNSA, and all contractors for a DOE-owned or DOE-leased Hazard Category 1, 2, or 3 nuclear facility or nuclear operation. 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 because their activities normally do not use, store, or form radioactive materials. However, target

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.

areas associated with the accelerators and areas associated with the radioactive materials produced by the accelerators are not considered to be part of the accelerator and continue to be subject to the provisions of 10 CFR 830 to the extent that they use, store, or form radioactive materials. Thus, target areas that contain or form radioactive inventories within the DOE-STD-1027 limits are subject to 10 CFR 830.

This Guide does not prescribe the format for a DSA. Each of the safe harbor methods in Table 1 provides a suggested format that is appropriate to the specific application.

3. IMPLEMENTATION (830.207 AND RULE APPENDIX)

If a contractor believes that the safety basis for an existing Hazard Category 1, 2, or 3 DOE nuclear facility already meets the requirements of the rule and reflects the current work and hazards associated with the facility or activity, the contractor responsible for the facility must, by April 9, 2001, affirm to DOE that the existing safety basis satisfies the requirements of 10 CFR 830, document the adequacy of the existing safety basis and request DOE to issue a safety evaluation report that approves the existing safety basis. The rule requires this reevaluation and affirmation of the safety basis even if a safety evaluation report (SER) has been previously written. If DOE does not issue a safety evaluation report by October 10, 2001, the contractor must submit a new safety basis by April 10, 2003. If a contractor believes that the currently approved safety basis does not meet the requirements of the rule, the contractor must work to the currently approved safety basis and develop a DSA that satisfies the rule by April 10, 2003. If the contractor believes that the current safety basis does not reflect current operations (e.g., the current safety basis reflects previous operations that have been changed), the contractor must notify DOE of the need for upgrading the safety basis and must identify any interim safety measures that may be needed. By April 10, 2003, contractors must submit DSAs for facilities that do not have an approved DOE SER from the October 2001 exercise or for the facilities for which the contractors had indicated the safety basis did not meet the requirements of the rule in April 2001.

It is desired that both the contractor and DOE take positive action in establishing safety bases under the rule. The contractor should maintain cognizance of the status of DOE reviews and work with DOE to resolve the status of the safety basis submitted in a timely fashion. If the safety basis was originally developed using one of the safe harbors of the rule and the contractor affirms that the safety basis complies with the rule requirements, the safety evaluation report for the safety basis was issued approving the safety basis and the safety basis and the safety evaluation report are current and comply with the rule, then the DOE effort to verify compliance with rule provisions should be small.

The USQ process is a key element in keeping the safety basis current with DOE approvals as required. The Nuclear Safety Management rule (10 CFR 830) requires a contractor responsible for an existing Hazard Category 1, 2, or 3 DOE nuclear facility to submit for DOE approval a procedure for its USQ process by April 10, 2001 (See 10 CFR 830.203 and DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question (USQ) Requirements*).

It is recognized that there may be nuclear facilities which have not yet upgraded to meet the rule requirements and may not be able to do so within the 2 1/2-year period after the rule is published, even though DOE 5480.23, *Nuclear Safety Analysis Reports*, with essentially the same requirements, was effective in 1992. The effect of 10 CFR 830 is to require compliance. Contractors should evaluate all their safety basis documents to determine which ones comply with the rule and which ones must be upgraded. Those which will require beyond April 10, 2003, to upgrade should be the subject of a temporary (or for good cause, permanent) exemption from the rule under the provisions of 10 CFR 820.61.

Pending issuance of a safety evaluation report in which DOE approves a safety basis for an existing Hazard Category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must continue to perform work[3] in accordance with the safety basis for the facility in effect on October 10, 2000, or as approved by DOE at a later date and maintain the existing safety basis consistent with the rule requirements.

A contractor may not begin operation of a new Hazard Category 1, 2 or 3 DOE nuclear facility or a major modification of an existing Hazard Category 1, 2 or 3 DOE nuclear facility until completion, defined by the issuance of a safety evaluation report in which DOE approves the safety basis for the facility or modification.

4. IMPLEMENTATION GUIDANCE (830.202, .204 and .205)

4.1 Documented Safety Analysis (830.202, .204 and Rule Appendix A)

Development of a DSA or preliminary documented safety analysis (PDSA) is the process whereby facility hazards are identified, controls to prevent and mitigate potential accidents involving those hazards are proposed, and commitments are made for design, construction, operation, and disposition so as to assure adequate safety at DOE nuclear facilities. DOE, in its review and approval role, may require modification or addition to these commitments by the responsible contractor. Throughout the life of the facility, from design and construction to mission-oriented operations, through deactivation, long-term surveillance and maintenance, to decontamination and decommissioning, there must be a safety basis in place that is appropriate to the activities (operations) occurring during each of those phases.

During design and construction, the governing safety basis document is the PDSA. It is updated as the design matures and is approved prior to procurement and construction activities. Until approval, the PDSA and its updates serve to keep DOE informed as to how DOE nuclear safety design criteria are being addressed in the design. Project design reviews provide the vehicle by which safety-related changes are reviewed and DOE can provide guidance to the contractor. Prior to operations, the PDSA evolves to a final DSA that reflects the facility as actually constructed.

During mission-oriented operations and for each phase thereafter until, through deactivation or decontamination and decommissioning, the facility falls below the Category 3 threshold for nuclear facilities, the DSA must be kept current, considering any changes to the facility or its operations. The USQ process is key to this requirement. The USQ process must be integrated with the configuration management process that must be a part of the safety management

---

[3] As described in the Preamble to the Interim Final Rule: The definition of "work" as applied to this rule is very broad and encompassing. It includes any defined task or activity that may affect a safety basis for a facility. It could include such diverse activities as operations, research and development, environmental restoration and remediation, maintenance and repair, design and construction, software development and use, inspection, data collection, administration, and analysis.

program commitments of a DSA. The USQ process is the tool by which it is determined when DOE must approve any changes to the facility or its operations.

A DSA must demonstrate the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment. DOE expects a contractor to use a graded approach to develop a DSA and describe how the graded approach was applied. The level of detail, analysis, and documentation will reflect the complexity and hazard associated with a particular facility or activity. Thus, the DSA for a simple, low-hazard facility may be relatively short and qualitative in nature, while the DSA for a complex, high-hazard facility may be quite elaborate and more quantitative. DOE will work with its contractors to ensure a DSA is appropriate for the facility or activity for which it is being developed. Table 1 identifies acceptable methodologies for preparing a DSA.

DSAs are prepared in order to be the primary reference on facility safety. Contractor management uses the DSAs for new nuclear facilities, to have an authoritative documented record of DSA derived and programmatic safety commitments made to DOE governing safety and health aspects of project management, engineering, design, procurement and construction of the facility or the development of the nuclear operation. DOE O 420.1, *Facility Safety*, contains requirements for the design of new nuclear facilities and mandates the use of safety analyses to guide safety aspects of design. In addition, 10 CFR 835, Subpart K, "Occupational Radiation Protection," gives regulatory requirements for design and control. These analyses should be summarized in the DSA to support the rationale for safety aspects of design.

4.1.1 Preliminary Documented Safety Analysis (PDSA) (830.206)

To obtain early agreement between DOE and its contractors regarding what safety systems and design features are needed in new nuclear facilities, a contractor responsible for a new DOE nuclear facility or a major modification to an existing DOE nuclear facility that is Hazard Category 1, 2, or 3 must submit a PDSA to DOE for approval. DOE approves the PDSA prior to procuring materials or components, or beginning construction.

PDSAs for new facilities serve as the principal safety basis for the DOE decision to authorize design, procurement, construction, and pre-operational testing. The safety analysis should be initiated and technical interchanges conducted with DOE at the earliest practical point in conceptual or preliminary design, so that required functional attributes of safety SSCs can be specified in the detailed design. These early interchanges are intended to support development of a consensus on the safety issues between the various design and safety organizations involved in the project. The PDSA will identify preliminary commitments to the facility's ultimate design and operation.

DOE does not expect a PDSA to be needed for activities that do not involve significant construction—such as environmental restoration activities, decontamination and decommissioning activities, specific nuclear explosive operations, transition surveillance and maintenance activities—or for activities that are not major modifications. For activities that are

not major modifications, the USQ process should be used to determine if DOE approval is needed. If so, a safety analysis that supports the request for approval should be developed. If the request is approved, then the safety analysis should be included in the DSA when the modification is completed.

The PDSA required by 10 CFR 830.206 may need updating to sustain the reliability of the information therein, until such time as it is superseded by a Final DSA. The contractor should update the PDSA as necessary to keep it applicable to the evolving design so that the Department can continue to rely on the information in the PDSA.

A PDSA should contain a description of the preliminary design of the facility with respect to safety SSCs and safety design features, identify research or other data collection necessary to finalize the design, and document the preliminary approaches to startup and operations management. The PDSA should show how the nuclear safety design criteria are proposed to be satisfied. In addition, a PDSA should contain descriptions and commitments to DOE with respect to contractor management and oversight of the construction project. Most such programmatic commitments would be found in the associated program control documentation rather than the PDSA. These involve management and organization, management controls and coordination, quality assurance, compliance determination, internal inspection, and safety review functions for the procurement, construction, and startup phases of the project. These safety commitments and goals will become a basis for DOE safety performance evaluation during the construction phase of the project.

Table 2 provides a summary of the PDSA development process for capital acquisition projects in relation to project milestones (See DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*). Such projects would include new facilities and major (capital) additions to existing facilities. The rule requires a PDSA to be prepared for major modifications and defines a “major modification” to include substantial changes to the safety basis of a facility.

For the design and construction of a new facility or activity, it is imperative that safety be addressed early so that it can be “designed-in” instead of “added-on.” To achieve this integration of safety into design, there needs to be continuous interaction between safety analysts and the designers throughout the design process, as described in DOE O 420.1 and the related Implementation Guides. (See DOE G 420.1-1, DOE G 420.1-2, DOE G 440.1-5, and the criticality design standards ANSI/ANS 8.1, 8.2, 8.3, 8.5, 8.6, 8.7, 8.9, 8.10, 8.12, 8.15, 8.17, 8.19 and 8.21.) All of these hazards (nuclear, explosive, natural phenomena, fire, criticality, etc.) should be addressed as early as possible in the design of new nuclear facilities and major modifications so that passive and active design concepts can be economically incorporated into the design. DOE encourages the use of design and safety features rather than procedural and administrative controls to address worker and public safety. (See Section 5.2.1)

4.1.1.1 PDSA Development During Conceptual Design, CD-1

The initial safety analysis should be developed during conceptual design and be submitted for review with the conceptual design report (CDR). The safety analysis should consist of a process hazards analysis (PrHA) that identifies the types and magnitudes of hazards that are anticipated in the facility. From this, the appropriate nuclear safety design criteria should be identified, and at least a top-level description should be given of how these criteria will be met in the design. The rule requires that contractors either use the nuclear safety design criteria in DOE O 420.1 or propose alternative criteria for DOE approval.[4] In addition, 10 CFR 835, Subpart K, "Occupational Radiation Protection," gives regulatory requirements for design and control. Contractors should also consult the guidance for DOE O 420.1.

4.1.1.2 PDSA Development During Preliminary Design, CD-2

In the preliminary design phase, the draft PDSA should be submitted to support review of the preliminary design package. It should include analysis of design basis accidents, and any safety class SSCs should be identified along with their safety functions and functional requirements. The PrHA should be updated to be consistent with the preliminary design modifications, including all of the identified hazards. A first cut should also be made of potential safety significant SSCs and their functional requirements. The draft PDSA should show how nuclear safety design criteria are met as well as how applicable laws and regulations will be met. The draft PDSA should be submitted with the preliminary design package.

The PDSA should anticipate ways the facility can be constructed, maintained, operated, and shut down safely in compliance with applicable laws and regulations. "Operated" and "maintained," as used here, refer to operation and maintenance in the broadest sense that embraces the full range of operations, testing, surveillance, maintenance, minor modifications, etc. "Shut down" refers to the capability to maneuver the facility into a safe, stable state during routine shutdowns in the event of incidents and accidents and during long-term decommissioning. It also follows that PDSAs should identify those laws and regulations that apply to the safe design or operation of the facility. DOE will initiate preparation of the SER on the PDSA.

4.1.1.3 PDSA Development During Final Design, CD-3

In the final design phase, the PDSA should be modified as necessary to reflect the evolving design. Hazard and accident analyses should be mature in that all of the identified hazards and the potential accidents should be addressed. The supporting analyses should be sufficiently rigorous to justify the selection of safety SSCs and controls. The accepted hierarchy of controls

---

[4] If DOE O 420.1 design criteria are not expected to be satisfied, alternative design criteria that provide an equivalent level of safety should be prepared for DOE's approval in accordance with the DOE FRAM (See the "safe harbor" discussion in the Introduction, above.) very early in the design phase.

Table 2. PDSA Development Process for New Nuclear Facilities or Major Capital Modifications of Existing Nuclear Facilities.

	Pre-Conceptual Planning	Conceptual Design	Preliminary Design	Final Design	Construction[5]	Operations
	Critical Decision-0	**CD-1**	**CD-2**	**CD-3**	**CD-4**	
Major Project Planning Activities	Develop conceptual design and justification of mission need	Acquisition plan, conceptual design report, system design description, cost and schedule	Establish performance baseline budget (PBB), refine design	Prepare design packages: update PBB, project execution plan (PEP), Prepare construction and procurement packages	Construct to PEP with PDSA change control	
Major Safety Analysis Activities	Identify hazards, design criteria, and site selection criteria	Facility hazard categorization, process hazards analysis (PrHA), complete initial safety analysis and identify permits	Complete[6] PDSA[7] Develop NEPA, environmental assessment and environmental impact statement documentation	Update PDSA and prepare and NEPA and environmental documents	Operational readiness review planning and change control, prepare DSA	
Major DOE[8] Approval and Review Activities	Review mission need, authorize funding for conceptual design	Review conceptual design report and hazard categorization, authorize funding for design	Review contractor's project management system, PEP and PBB. Review the PDSA and initiate safety evaluation report. Authorize final design activities (including external independent review)	Review and update PBB and PEP, and PDSA authorizing construction activities. Issue safety evaluation report on PDSA.	Oversight, prepare SER DSA and conduct operational readiness review	

[5] Limited procurement and construction activities may be approved by DOE before the PDSA is approved.

[6] Including accident analysis for all known hazards and identification of safety class systems and requirements.

[7] A PDSA is not required except for new construction or major modifications of nuclear facilities but the "preliminary design phase" would still be required for "capital asset acquisitions" that are not major modifications to nuclear facilities.

[8] The level of DOE review and approval authority changes with the cost of the project but for "capital asset acquisition" the project phases remain essentially unchanged except for environmental restoration and facility disposition projects which do not ordinarily require the four critical decision phases.

includes passive engineering features, active engineering features, administrative controls, and personal protective equipment. Safety SSCs should be identified and their performance requirements clearly described. A proposed list of controls and safety management programs should be developed to address operational safety considerations. The PDSA should be reviewed and approved by DOE with an SER. These approvals should occur prior to undertaking procurement of materials or components, construction, and preoperational testing of a new nuclear facility.

4.1.1.4 Procurement and Construction During PDSA Development

Section 830.206 allows limited procurement and construction activities before the 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 the following:

(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 must 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.

4.1.1.5 DOE Review and Approval of the PDSA

The DOE safety review is part of a continuous interaction between DOE and the responsible contractor during the design evolution of a nuclear facility. The timing of completion of the SER with respect to the critical decision milestones is subject to negotiation and should consider the complexity of the facility and the urgency of the facility's mission. DOE will complete the SER when the design is sufficiently mature for DOE to authorize procurement, construction, and final design activities.

DOE will review and comment on the PDSA. It is expected that typically one round of questions and responses will be required to obtain approval. DOE reviewers and the approver of the PDSA should recognize that the level of detail that exists at the PDSA stage is not the same that is available during the final DSA review. DOE PDSA reviewers should be mindful that the PDSA is based on evolving designs; is based on the available knowledge of equipment to be procured after the PDSA is approved; and may identify the need for additional research and final data collection.

Therefore it is recommended that the DOE PDSA reviewer prepare the PDSA SER based on one of the following PDSA findings/evaluations:

- the proposed design item/system/activity is completely reviewed and found acceptable (subject to any DOE-imposed changes);

- the proposed design item/system/activity is based on preliminary information and is accepted based on commitments to fully meet specific safety criteria in the final DSA (such as separation, redundancy, maintainability access, etc.); and

- the design item/system/activity is based on evolving research and/or information gathering and/or is accepted based on the preliminary information and the requirement to complete specific research before the DSA is finalized, to provide the final data in the DSA.

While it is most desirable for the DOE PDSA reviewers to make the first finding, DOE reviewers need to acknowledge the possibility and the acceptability of the other two PDSA SER findings. After the SER has been completed the PDSA will be treated as a controlled document and must

be updated as necessary to maintain the accuracy of the safety basis information through amendments or supplements to the PDSA.

4.1.2 Final Documented Safety Analysis (Final DSA) (830.204 and .207)

During construction, the final DSA is developed. It is based on the facility as built and as it will be operated and finalizes the description of needed safety management programs. After the construction has been completed and the DSA has been updated to reflect the as-built design and development of the TSR bases, DOE reviews the revised DSA and updates the SER authorizing operations subject to any necessary conditions, including the need for an operational readiness review (See DOE O 425.1B). Approved final DSA, TSRs and other hazard control documents contain the principal safety basis for a DOE decision to authorize facility operation. Once facility operation is authorized, the final DSA and hazard controls will be the principal safety bases for sustaining authorization and safety oversight.

A final DSA documents the safety basis and provides detailed information for a determination that the facility can be operated, maintained, shut down, and decommissioned safely and in compliance with applicable laws and regulations. This has much the same meaning as does the similar language for PDSAs, except that for final DSAs, the descriptions of operations are complete, detailed, and based on final information.

4.1.3 Annual DSA Updates (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 must 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[9] 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 must 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

---

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

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.

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. Any agreements predating the rule that delay the annual update requirements must be made into an exemption to the rule, if desired to continue. The exemption process is described in 10 CFR 820, Part E.

4.2 Safety Basis For Special Activities (830.202 and Rule Appendix)

As defined in 10 CFR 830.3, the safety basis is the DSA and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely in a manner that adequately protects workers, the public, and the environment.

The development of the DSA and hazard controls for several types of special activities identified in the Appendix to Subpart B is described in the following subsections.

4.2.1 Safety Basis for Select Environmental Restoration Activities (Table 2 of the Rule Appendix)

For the purpose of this Guide, "select environmental restoration activity" means an activity that involves either (1) restoration work not done within a permanent structure or (2) 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 "select 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 (See Table 2 of the Appendix to Subpart B).

For select environmental restoration activities a health and safety plan (HASP) can be used as alternative documentation to satisfy both Price-Anderson Amendments Act nuclear safety requirements and the OSHA worker safety requirements. DOE-STD-1120-98 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 sitewide programs and describe how they would be applied for these activities.

DOE-STD-1120-98, *Integration of Environment, Safety and Health into Facility Disposition Activities*, or its successor document, 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. 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 and he needs to identify environmental requirements.

4.2.2 Safety Basis for Nuclear Explosive Operations (Table 2 of the Rule Appendix)

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-3009-94, Change Notice No. 1 or successor document 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-DP-STD-3016-99 or successor document 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 must possess certain attributes. First, the generic operation must 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 must 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) must 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 must be compared with the facility DSA to ensure they are consistent and appropriate, and not in conflict. This hazard analysis must be thorough, and requires evaluation of the complete spectrum of hazards and accidents. The effort

is largely qualitative, and at times semiquantitative; 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 is acceptable, but these should not be used as absolute cutoff criteria for dismissing physically credible low-probability accidents, without any evaluation of preventive and mitigative features. This distinction is made to prevent "pencil sharpening" at the expense of objective evaluation of hazards, particularly in the presence of large data and phenomenological uncertainties.

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 must 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 should take precedence.

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-3009-94, Change Notice No. 1 or successor document to determine that nuclear explosive facilities must 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 must 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).

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 explicitly referred to in DOE O 452.1A as 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.

4.2.3 Safety Basis for Transportation Operations (Table 2 of the Rule Appendix)

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 must also satisfy DOE O 452.1A and DOE O 452.2A. Onsite transportation or transfer of all nuclear material is covered by 10 CFR 830 as provided under safe harbor provisions of the rule.

Both offsite transportation in the national security interest, including nuclear explosives, and onsite transportation of nuclear explosives should comply with the safety requirements of DOE O 461.1, DOE M 461.1-1, and other DOE-approved subordinate documents. Onsite transportation of nuclear explosives must also comply with the safety requirements of DOE O 452.2A. 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 460.1A and the onsite portion of DOE O 461.1.

Transportation TSRs are addressed in DOE G 423.1-1, *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 Facility Authorization and DOE's Approval of DSA (830.207)

DOE employs DSAs, TSRs, and SERs as the principal safety documentation in its decision to authorize construction and operation of nuclear facilities, including NNSA nuclear facilities. For new facilities, approval of the PDSA is required before construction is begun. A contractor may not begin operation of a new Hazard Category 1, 2 or 3 DOE nuclear facility or a major modification[10] of an existing Hazard Category 1, 2 or 3 DOE nuclear facility before DOE issues an SER approving the safety basis for the facility or modification. (See Section 3, Implementation.)

DOE-STD-1104-96, *Review and Approval of Nonreactor Nuclear Facility Safety Analysis Reports*, or successor document, 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, must 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 must 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.

5. ACCEPTABLE METHODS (830.204 AND RULE APPENDIX)

The DSA should 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] "Major modification" means a modification to a DOE nuclear facility that is completed on or after April 9, 2001, that substantially changes the existing safety basis for the facility.

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 are expected to reflect the new guidance.

The DOE Standards specified in the appendix to the rule have gone through a DOE-wide concurrence process, with peer technical review and comment resolution, including review by the Defense Nuclear Facilities Safety Board. DOE is confident these standards provide good methods for developing a DSA. If a contractor uses a "safe harbor" methodology, that methodology should result in a contractor satisfying the regulatory requirements for a DSA. However, the contractor is responsible for meeting the requirements of the rule, even if it uses a safe harbor standard to prepare its DSA.

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

- technical description of the alternative method or deviation (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.

The DOE Office of Environment, Safety and Health will work with the line organization to provide an additional level of peer review. The detail and rigor of this process will be determined on a case-by-case basis. It will be a function of the extent of the departure of the methodology or deviation from the safe harbor methods and the effect of using the new methodology on the resulting safety basis. If approved, DOE could assign the alternative methodology or deviation the status of a safe harbor.

The safety basis requirements (10 CFR 830.201, 830.202, 830.204, 830.206 and 830.207) are described below.

5.1 Development of Hazard Categorization for Legacy Nuclear Facilities Without Inventory Information (Table 2 of the Rule Appendix)

Many facilities within the DOE complex have been shut down, still containing radioactive materials, and have remained dormant for many years. Often, records were not kept or were lost on the types and location of radioactive materials remaining in these dormant facilities. In addition, radioactive materials from other facilities may have been moved into these dormant facilities. This section discusses and provides guidance on how the material inventories can be estimated and the preliminary hazard categorization calculated.

The preferred method of characterizing facility or activity hazards is to assess the extent, type, and location of radioactive materials. A preliminary hazard categorization is performed based on a review of facility-related information. This can be accomplished by collecting and reviewing available facility operating records and existing hazard baseline documentation. Interviewing past and present employees supplements information on past operations especially where mishaps or incidents have occurred. Reviewing Occurrence Reporting and Processing System (ORPS) reports or lessons-learned reports may identify hazards that were previously unknown.

During the development of facility surveillance and maintenance plans consistent with DOE O 430.1A, *Life Cycle Asset Management,* an assessment of the detailed facility condition is performed. This should be accomplished by a multidisciplinary team that includes the project manager, engineering representatives, ES&H personnel, and workers. This assessment commonly includes, but is not limited to, various intrusive activities such as facility walkdowns, sampling and analysis to accurately identify radionuclide inventories, and an assessment of safety-class and safety-significant SSCs. If sufficient information to support accurate hazard categorization is not gathered during the initial formulation of surveillance and maintenance plans, additional assessments are conducted to complete the facility hazard classification and, if appropriate, supplement the existing surveillance and maintenance plan.

Further guidance on hazard identification and characterization for facilities in surveillance and maintenance, deactivation or decommissioning can be found in DOE-STD-1120-98, *Integration of Environment, Safety, and Health into Facility Disposition Activities,* or successor documents. Section 3.1.3 directly addresses methods of identifying and characterizing hazards where they are unknown.

For environmental remediation and facilities going into the decommissioning life cycle, prior to conducting this assessment, the identification and analysis of hazards and development of controls pertaining to any intrusive characterization activities should be documented in a HASP consistent with 29 CFR 1910.120.

As an alternative to the first approach, if no facility-specific information is available, Hazard Category 2 can be assigned to a nuclear facility as a default preliminary categorization and then a final categorization must be performed by characterizing the facility in compliance with DOE-STD-1027-92 and 10 CFR 830.

5.2 Topics for DSA (830.204 and Rule Appendix)

The DSA must—

- describe the facility and the work to be performed;
- identify the hazards associated with the facility;
- evaluate all accident conditions that are presented by natural and/or manmade hazards;
- derive the hazard controls, including TSRs, to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls 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; and
- define necessary criticality safety programs.

DOE has developed DOE-STD-3009-94, Change Notice No. 1, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facilities Documented Safety Analysis*. This preparation Guide provides both a standardized format and suggested content for nonreactor nuclear facilities with an emphasis on existing Hazard Category 2 facilities. DOE-STD-3009-94 has also been used successfully to prepare DSAs for critical assemblies.

There is an ANS standard that provides guidance for small research reactors (ANS 15.21) and NUREG-1537 provides guidance for nonpower reactors. Most DOE large reactors use Reg. Guide 1.70. However, none of these reactor formats was intended for DOE reactors and each has left out several topics that should be included. For DOE reactors, in addition to the topics discussed in Reg. Guide 1.70, hazard analysis and categorization of the facility and applicable facility design codes and standards should be added. DOE-STD-3009-94, Change Notice No. 1 or successor document 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 Reg. Guide 1.70) rather than that identified in 10 CFR 830.

DOE 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.

The following sections provide general guidance on the content that should be provided in the DSA for DOE nuclear facilities, including NNSA nuclear facilities.

5.2.1 Content of Category 1 or 2 Hazard Nuclear Facility DSA (830.204 and Rule Appendix)

DOE-STD-3009-94, Change Notice No. 1 provides a suggested format and content for Hazard Category 1 and 2 nuclear facility DSAs.

With regard to safety management programs that may be sitewide 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 sitewide program documentation for the details. A radiation protection program for a tritium facility would incorporate different features of the sitewide program than would a plutonium facility, for example. The DSA should explain how the appropriate features of the sitewide program are implemented at the specific facility. A list of safety management rules, directives and standards is included in Appendix A for the user's convenience.

5.2.1.1 Criticality Safety Analyses for Hazard Category 1 or 2 Nuclear Facilities

Inadvertent criticality hazards must be considered in the general treatment of hazard analyses during the development of a DSA. Paragraph 830.204 requires, in the preparation of a DSA, description of the design and work to be done, a systematic identification of hazards, evaluation of 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, derivation of hazard controls, definition of safety management programs necessary for safety, including a criticality safety program. It is important to recognize that all these elements, as may relate to criticality hazards, must be treated in the DSA, not just deferred to a criticality safety program. Evaluation of normal, abnormal, and accident conditions means development of scenarios that could result in an unintended criticality and development of the appropriate hazard controls (prevention and mitigation). Only a few evaluations of criticality scenarios for a facility need to be carried to dose consequence calculations and documented in the DSA to evaluate the need for safety class SSCs. Criticality safety evaluations (CSEs) are developed for all process areas involving criticality hazards under the Criticality Safety Program. The CSEs support the DSA and should be summarized in the hazard analysis section of the DSA, including hazard controls in sufficient detail to provide assurance that all criticality hazards have been addressed. Consideration of the need for analysis of accidents which may be beyond the design basis of the facility can be done in a summary fashion in the DSA. The intent is to ensure that no accident scenarios with significant risk implications have been dismissed that need DOE management attention in authorizing facility operations.

A useful format for CSEs is outlined in DOE-STD-3007-93, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Non-Reactor Nuclear Facilities,* or successor document. A CSE must be documented clearly and with appropriate detail to allow independent review and evaluation of the results. Guidance for review of CSEs is provided in DOE-STD-1134-99, *Review Guide for Criticality Safety Evaluations*, or successor document.

All safety-related controls (criticality related or otherwise) are identified and characterized during the course of the hazards and accident analyses performed in support of the DSA. A subset of all controls will get safety class or safety significant designation, and some of these may be related to control of criticality accidents. Controls that are identified and discussed in CSEs may or may not end up as safety class or safety significant depending on the basis for these designations derived from the hazards analysis and accident analysis in the DSA. Depending on the situation, criticality derived TSRs would usually be limiting conditions of operation, design features, or administrative controls (approved written procedures). Procedures are not generally described in detail in a DSA. TSR-level controls should be identified on a case-by-case basis and should be graded according to the guidance in DOE-STD-3009-94, Change Notice No. 1 or successor document with regard to the classification of controls.

The USQ process applies to the documented and approved safety basis. The Nuclear Safety Management rule (10 CFR 830) requires all proposed new or changed processes in a facility, including those involving criticality safety are required to undergo a USQ review by the Nuclear Safety Management rule. When the USQ determination is positive, indicating the need for DOE review and approval of the change, the safety analyses and controls associated with the approved action become part of the safety basis for the facility. Any changes necessary to the DSA and TSR documents as a result of the change should be incorporated at the next annual update. This does not mean that all CSE analyses should be incorporated into the DSA nor does it mean that DOE approves all CSEs. The results of the USQ determination define the need for DOE approvals of the supporting CSEs and explicit updates of the DSA and TSR.

5.2.2 Content of the DSA for a Category 3 Hazard Nuclear Facility (830.204 and Rule Appendix)

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 Chapters 2, 3, 4, and 5 of DOE-STD-3009-94, Change Notice No. 1 or successor document 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 (consisting primarily of inventory limits and safety management programs) and their bases.

For sitewide 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 sitewide program documentation for the details.

5.2.3 Use of a HASP as Hazard Baseline Documentation for Decommissioning Activities (830.204 and Rule Appendix)

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-1120-98, *Integration of Environment, Safety, and Health into Facility Disposition Activities*, or successor document; 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, work 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.

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. 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.

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 sitewide 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.

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.

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 detailed guidance on the structure and content of a HASP can be found in DOE EM-STD-5503-94, *DOE Limited Standard, EM Health and Safety Plan Guidelines* or successor document.

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-1120-98, *Integration of Environment, Safety and Health into Facility Disposition Activities*, May 1998, or its successor document, 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, 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.

Appendix I of DOE-STD-1120-98 recommends examples of hazard baseline documents for each disposition phase. 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 (see Section 5.2.4), 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, DOE must re-approve it before decommissioning operations may continue. As described in DOE-STD-1120-98 or successor documents, 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.

5.2.4 Basis for Interim Operations for Deactivation, Surveillance and Maintenance, and Limited Operational Life Facilities (830.204 and Rule Appendix)

Traditionally, DSAs have been used as the long-term safety basis document for nuclear facilities usually under steady-sate conditions. There are primarily two cases where the rule allows a basis for interim operations (BIOs) to be used as the appropriate safety basis documentation: (1) for short-lived activities and (2) during transition phases, including transition surveillance and maintenance, deactivation, and decontamination and decommissioning. 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 430.1A, *Life Cycle Asset Management*, and its corresponding Guides also provide guidance on using a BIO.

Deactivation refers to the process of placing a facility in a stable[11] 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.

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

---

[11] 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.

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).

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 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.

DOE-STD-3011, *Guidance for the Preparation of DOE 5480.22 (TSR) and DOE 5480.23(SAR) Implementation*, or successor document provides the format and content for developing a BIO. Section 3.3.4 and Appendix G to DOE-STD-1120-98, or successor documents, provides implementation insight and interpretation letters clarifying the development and use of the BIO as a DSA.

Hazards are being removed during facility disposition activities. A BIO per DOE-STD-3011 and DOE-STD-1120-98, or successor documents, 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 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.

5.3 Hierarchy and Selection of Safety Items (Hazard Controls)

The DSA requirements of 10 CFR 830 permit several safe harbor methods for preparing a DSA. However, the concepts of DOE-STD-3009, Change Notice No. 1 or successor document for the classification of hazard controls generally apply to all of the safe harbors. This section provides a discussion of these concepts and references to relevant sections of the Standard for more details.

5.3.1 Hierarchy

This section addresses items that perform a safety function in DOE facilities. These include safety class SSCs, safety significant SSCs, and other SSCs that perform a safety function, sometimes known as items "important to safety" and also, at some sites, "defense-in-depth items" that are not safety significant. The section describes what is meant by these terms and how they relate to each other.

The safety class SSC classification was instituted to deal with SSCs that have special importance with regard to protection of the public, modeled after engineered safety features of power reactors that are required to meet siting criteria.

The safety significant SSC classification was instituted to provide additional public protection by providing multiple means of dealing with accidents (defense in depth) and to provide protection for onsite personnel who may not be protected by distance factors, as the public is, because of large DOE sites.

The terminology "safety SSC" is used to refer to both safety class and safety significant SSCs. The significance of either of these categories is in the expectation that safety SSCs will be designed, qualified, procured, installed, and maintained so that they will perform their safety function when called upon to do so during normal, abnormal, and accident conditions. DOE O 420.1 and the associated Guide DOE G 420.1-1 provide guidance in these respects for new facilities and major modifications of existing facilities. In the case of existing facilities and safety items that satisfy the criteria for designation as a safety SSC, they will not necessarily have been designed to the standards applicable to a new facility or modification. Additional defense-in-depth measures or compensatory measures such as enhanced surveillance and maintenance may be necessary to support the criterion of assurance that they can perform their safety function when called upon.

Not all SSCs that perform a safety function should be classified as safety class or safety significant, because if everything is safety class or safety significant, then really nothing is special, because then no SSC would receive any different treatment that might be expected of very important safety SSCs. Some sites have called these lesser SSCs "defense-in-depth SSCs" or " SSCs important to safety." Although defense in depth is a criterion for safety significant designation, these sites have also used this terminology for a lesser level of SSCs. These SSCs of lesser importance are not dealt with in DOE O 420.1 or its Implementation Guide, DOE G 420.1-1, relative to design criteria or performance expectations. For the purpose of this Guide, these items are called "other SSCs important to safety."

5.3.2 Selection Process

Safety Class SSCs

DOE-STD-3009, Change Notice No. 1, January 2000, Appendix A discusses the evaluation guideline (EG) to be used in classifying a safety system as safety class, and the methodology of performing calculations necessary to apply the EG. This appendix is applicable to existing

facilities. DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety*, also addresses the use of the EG, but does so in the context of design of new nuclear facilities.

The EG in STD-3009-94, Change Notice No. 1 or successor document, and DOE G 420.1-1 is 25 rem as a result of an unmitigated accident and is frequency independent. Cautions are made in both documents that this should not be regarded as a "bright line" criterion and that doses challenging 25 rem (DOE-STD-3009) or in the rem range (DOE G 420.1-1) would indicate the need to consider classifying preventative or mitigative SSCs as safety class. Caution is also made that there is no hard cut-off in frequency, such as 10 (-6) for "credible" accidents in application of the EG.

It is recognized that some DOE sites have instituted their own versions of evaluation guidelines for safety class SSCs, and that these EGs are frequency dependent, and are sometimes numerically less than 25 rem (so-called step function criteria). Further, often they are used as dose acceptance criteria instead of as a safety SSC classification technique. These site-specific EGs are not endorsed by 10 CFR 830 or this Guide because (1) they encourage dose and frequency calculations in place of good safety practice and judgment, (2) DOE does not have accident dose limits, and (3) they don't deal with the profound uncertainties in dose calculations and frequency estimates. In the case of the calculations, reviews and approvals become focused on the calculations and models used, and dose and frequency estimates are seldom known to within one or two orders of magnitude with any certainty, thus making any calculational result a blur on the step function criteria. In the case of accident dose limits, it is impractical in all cases to impose them on existing operations at DOE sites for all potential accidents. The imposition of such limits in these situations is inappropriate because it invites attempts to lower doses through innovative modeling techniques or selective adjustment of analysis parameters, instead of addressing the safety issues. Use of these local criteria as acceptance criteria is regarded as outside the safe harbor method described in DOE-STD-3009-94, Change Notice No. 1 or successor document.

Safety Significant SSCs

DOE-STD-3009-94, Change Notice No. 1, invokes safety significant SSCs for either defense in depth or for worker safety. No dose criteria are assigned as EGs in these cases. The classification of SSCs as safety significant should be based on qualitative assessments. In the case of defense in depth, SSCs designated as safety significant are selected to prevent or mitigate accidents of lesser consequence or to provide extra layers of protection beyond that provided by safety class SSCs. The specifics of safety significant designation intent are addressed in the definitions section of DOE-STD-3009-94, Change Notice No. 1 or successor document, in the Introduction, and in Sections 3.3.2.3.2, Defense in Depth, and 3.3.2.3.3, Worker Safety.

In the context of defense in depth, the intent is threefold. First, associated with the classical defense-in-depth philosophy, SSCs identified as safety significant are intended to build in layers of defense against the release of hazardous materials (not just radioactive materials) so that no one layer, no matter how good, is completely relied upon. Second, in recognition that several

DOE sites are quite large and that the site boundary distance from any given facility may also be large, application of the EG for safety class SSCs, alone, may not provide an adequate level of protection for persons outside of the facility but within the site boundary, safety significant SSC designation can provide such protection. Finally, because the EG for safety class SSCs is not intended to imply an acceptable level of public dose, safety significant SSCs for defense in depth provide for achieving public dose levels from accidents to significantly below 25 rem, especially when unmitigated dose calculations would not trigger a safety class SSC.

In the context of worker protection, the qualitative criteria of DOE-STD-3009-94, Change Notice No. 1 (acute worker fatality or serious injury, see definition section), are intended to apply to in-facility workers, especially those immediately involved in an accident. While some sort of assessment of the level of accident consequences is necessary to apply the criteria, it is not appropriate to perform dose calculations and apply any numerical dose criterion for decision making. If these assessments involve calculations, they should be, at most, "back of the envelope" type calculations to give a sense of the order of magnitude of the doses. In the case of worker doses, especially immediately involved workers, the assumptions that could be made in the course of any more definitive calculations could easily affect the results by orders of magnitude. Thus, such calculations, if used to apply a numerical criterion, would divert attention from good safety decisions to arguments about the calculations and assumptions during the review.

As in the case with safety class SSCs, it is recognized that individual sites have instituted onsite frequency dependent dose acceptance criteria (so-called step functions) to apply to collocated workers and have even limited consideration of workers with regard to safety significant SSC designation to the collocated worker while excluding in-facility workers. 10 CFR 830 and this Guide do not endorse these practices, for most of the same reasons as described previously relating to safety class SSCs as well as those discussed in the previous paragraph. Use of these local criteria as acceptance criteria is regarded as outside the safe harbor methods described in DOE-STD-3009-94, Change Notice No. 1.

Other SSCs Important to Safety

These are items that perform a safety function, but do not rise to the level of importance of safety class or safety significant SSCs. They are, basically, everything else that might provide some level of protection. Some sites differentiate these items from industrial level equipment for the purpose of ensuring some additional level of care in procurement and maintenance. However, there are no DOE standards or Guides explicitly covering the design and procurement of these items.

In some situations, contractors have attempted to minimize the number of safety significant SSCs in a facility, perhaps beyond what would be prudent. For example, confinement ventilation systems and fire protection systems are often not accorded the status of even safety significant even when they may be dealing with the greatest facility hazards. This may be because of a perceived burden that goes along with design, procurement, and operations and maintenance of

safety class and safety significant SSCs. This practice should be avoided, because of the lack of any DOE standards for SSCs that are not designated either safety class or safety significant.

Use of Hazard Ranking Mechanisms in Selecting and Classifying Controls

A purpose of hazard and accident analyses of a DSA is to ensure all hazards are considered and a complete set of hazard controls are identified and appropriately classified. Section 3.3.2.3.5 of DOE-STD-3009-94, Change Notice No. 1 discusses the role of accident binning in facilitating this process. The proper use of the binning tool is to accumulate all related accident scenarios that have the same potential prevention or mitigation hazard controls, and to select the bounding one of these scenarios to be used to evaluate the proper classification of the hazard controls. For example, there is an entire spectrum of fires that may be possible in one part of a facility, and those fires may be controlled by a sprinkler system. The designation of the sprinkler system as safety class or safety significant should be based on the bounding fire of all fires that the sprinkler system would be applied to. Fires in another part of the facility for which the sprinkler is not effective would need to be considered in another bin for the purpose of classifying the control system applicable to them. Similarly, accidents of another character, say pipe or vessel bursts, cannot be binned with fires, because the hazard controls for those accidents would be different from those for fires. Further, the bounding accident of a type may be bounding for consequences outside the facility, but not necessarily bounding for in-facility worker consequences. Thus, the binning tool should only be considered an aide to organize the process of selecting and classifying hazard controls.

5.4 Relationship of Integrated Safety Management to Facility Safety Basis

An integrated safety management system (ISMS) is a total management system that mandates the incorporation of safety and environmental considerations into the process of defining, planning, and executing work. When work is planned, it must include the elements necessary to provide for adequate safety of the public, workers, and the environment. These safety elements must be budgeted and implemented.

The five core functions of an ISMS are (1) define the scope of work, (2) analyze hazards, (3) identify controls, (4) perform work in accordance with the controls, and (5) establish feedback and improvement. These functions are applicable on three levels that may be involved with any work: task level, facility level, and site level. A completely ISMS compliant safety strategy deals with all aspects of safety, including industrial safety, industrial hygiene, fire safety, electrical safety, chemical safety, and nuclear safety at each level. To be completely ISMS compliant, a facility that contains many different types of hazards must deal with all of them in a systematic and integrated way. A hazardous facility's safety basis is its specific safety strategy. A contractor's commitment to facility operations in accordance with its documented safety basis is one of DOE's assurances that work can and will be conducted safely.

The ISMS core functions that are key for developing a safety basis are analyzing all hazards and identifying controls. When describing an ISMS, contractors must define how these functions

will be accomplished. Within DOE, this is done through regulations and DOE Orders which deal with these functions, and the flow down of these requirements through implementing standards and procedures that provide more detail on how the requirements will be implemented at the working level. This flowdown starts with Lists A and B of contracts (required by the Department of Energy Acquisition Regulation), which are listings of regulations and laws (List A) and DOE Orders and Standards (List B). List A and List B are contract terms and conditions that establish the requirements that contractors will comply with in performing their work.

The safety basis requirements of Subpart B of 10 CFR 830 are focused on the facility-level functions of analyzing hazards and identifying controls. The rule does not discriminate between the types of hazards that should be considered (although only those with a nuclear nexus could be subject to Price Anderson enforcement actions should the rule be violated). A facility safety basis treats task-level hazards through ISMS provisions for analyzing hazards and identifying controls for that level of work, and the safety basis invokes the safety management programs that implement those processes through the administrative controls of the TSR. Similarly, the safety basis incorporates site-level functions for analyzing hazards and identifying controls through invoking sitewide programs such as the emergency management program, also through the TSR administrative controls. In this way, a facility safety basis developed under 10 CFR 830 conforms to the principles and functions of ISMS.

Operational safety is generally maintained through the use of standard operating procedures for normal and off-normal (and sometimes emergency) conditions. Operational safety is directed toward protection of workers and minimization of off-normal (anticipated upset) conditions, and toward ensuring that operations remain within specified (design) parameters. It is concerned with the maintenance of controls to limit worker exposure to all of the hazards identified and controls to stabilize minor upsets and off-normal conditions. Management of normal operations and off-normal conditions involves considerations for design such that integrated hazards analyses are completed for deviations from design intents.

The safety of nonroutine work, or short-term tasks, is generally maintained through the use of a work authorization system, rather than through standard operating procedures. The safety of nonroutine work is also directed primarily toward protection of workers, usually maintenance workers. It is addressed using such methods as job task analysis or job hazards analysis. When short-term, nonroutine work is undertaken, job hazards analyses or job task analyses are performed to identify hazards and appropriate controls to protect workers performing that work. These integrated analyses typically consider what can go wrong, how to prevent it, and what measures are needed for worker protection, for example, the discriminate use of personal protective equipment.

DOE O 440.1A addresses safety management, primarily oriented to worker safety, for normal operations and off-normal conditions (including short-term, nonroutine work) primarily in paragraphs 4i and 4j and Attachment 2, paragraphs 9 and 12 of the Order and in its Guides, DOE G 440.1-1, sections 4.3 and 4.4 and in DOE G 440.1-3, *Occupational Exposure Assessment.*

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 834, Radiation Protection of the Public and the Environment (Draft).

7. 10 CFR 835, Radiation Protection for Occupational Workers.

8. 10 CFR 850, Chronic Beryllium Disease Prevention Program.

9. 10 CFR 1021, (DOE) National Environmental Policy Act Implementing Procedures.

10. 29 CFR 1910, Occupational Safety and Health Standards.

11. 29 CFR 1926, Occupational Safety and Health Regulations for Construction.

12. 40 CFR, Environmental Protection Agency.

DOE Orders and Manuals

1. DOE O 210.1, *Performance Indicators and Analysis of Operations Information*, dated 9-27-95.

2. DOE O 225.1A, *Accident Investigations*, dated 11-26-97.

3. DOE 231.1, *Environment Safety and Health Reporting Requirements*, dated 9-30-95.

4. DOE O 232.1A, *Occurrence Reporting and Processing of Operations Information*, dated 7-21-97.

5. DOE O 360.1A, *Federal Employee Training*, dated 9-21-99.

6. DOE M 411.1-1B, *Safety Management Functions, Responsibilities, and Authorities Manual* (FRAM), dated 5-22-01.

7. DOE O 413.1, *Management Control Program*, dated 12-6-95.

8. DOE O 413.3, *Program and Project Management for The Acquisition of Capital Assets*, dated 10-13-00.

9. DOE O 414.1A, *Quality Assurance*, dated 9-29-99.

10. DOE 420.1, *Facility Safety*, dated 10-13-95.

11. DOE O 420.2A, *Safety of Accelerator Facilities*, dated 1-8-01.

12. DOE O 425.1B, *Startup and Restart of Nuclear Facilities*, dated 12-21-00.

13. DOE O 430.1A, *Life Cycle Asset Management*, dated 10-14-98.

14. DOE O 435.1, *Radioactive Waste Management*, dated 7-9-99.

15. DOE 440.1A, *Worker Protection Management for DOE Federal and Contractor Employees*, dated 3-27-98.

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

17. DOE O 451.1B, *National Environmental Policy Act Compliance Program*, dated 10-26-00.

18. DOE O 452.2A, *Safety of Nuclear Explosives Operations*, dated 1-17-97.

19. DOE O 460.1A, *Packaging and Transportation Safety*, dated 10-2-96.

20. DOE O 461.1, *Packaging and Transfer or Transportation of Materials of National Security Interest*, dated 9-29-00.

21. DOE M 461.1-1, *Packaging and Transfer of Materials of National Security Interest Manual*, dated 9-29-00.

22. DOE 4330.4B, *Maintenance Management Program*, dated 2-10-94.

23. DOE 5400.1, *General Environmental Protection Program*, dated 11-9-88.

24. DOE 5480.19, *Conduct of Operations Requirements for DOE Facilities*, dated 7-9-90.

25. DOE 5480.20A, *Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities*, dated 11-15-94.

26. DOE 5480.23, *Nuclear Safety Analysis Reports*, dated 4-10-92.

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

28. DOE 5530.3, *Radiological Assistance Program*, dated 1-14-92.

29. DOE 5610.13, *Joint Department of Energy/Department of Defense Nuclear Weapon Safety, Security, and Control Activities*, dated 10-10-90.

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. 1, January 2000, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, dated July 1994.

3. ANS STD 15.21, *Standard Format and Content for Safety Analyses Reports for Small Research Reactors*, dated 12-14-99.

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

5. DOE-STD-1104-96, *Review and Approval of Nonreactor Nuclear Facility Safety Analysis Reports*, dated February 1996.

6. DOE-STD-1120-98, *Integration of Environment, Safety, and Health Into Facility Disposition Activities*, dated May 1998.

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

8. DOE-STD-3007-93, Change Notice No. 1, September 1998, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Non-Reactor Nuclear Facilities*, dated November 1993.

9. 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-3011-94, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans,* dated November 1994.

11. DOE-STD-3015-2001**,** *Nuclear Explosive Safety Study Process,* dated February 2001.

12. DOE-EM-STD-5503-94, *EM Health and Safety Plan Guidelines,* dated December 1994.

13. DOE-DP-STD-3016-99, *Limited Standard: Hazard Analysis Reports for Nuclear Explosive Operations*, dated February 1999.

14. 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.

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

16. DOE G 423.1-1, *Implementation Guide for use in Developing Technical Safety Requirements*, dated 10-24-01.

17. DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question (USQ) Requirements*, dated 10-24-01.

18. DOE G 440.1-5, *Implementation Guide for Fire Safety Program*, dated 9-30-95.

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

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

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

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