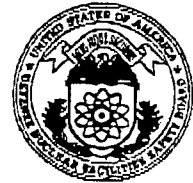


John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
Joseph J. DiNunno
John E. Mansfield
Jessie Hill Roberson

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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



November 7, 2000

The Honorable Bill Richardson
Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Richardson:

On October 10, 2000, the Department of Energy (DOE) published in the Federal Register an interim final rule on Nuclear Safety Management, 10 Code of Federal Regulations (CFR) Part 830. The rulemaking notice invited comments to be submitted by November 9, 2000.

The Defense Nuclear Facilities Safety Board (Board) believes that judicious implementation of this rule can strengthen and enhance an effective safety management program for DOE defense nuclear facilities. This objective can be accomplished if DOE (1) places emphasis on better utilization and upkeep of the many vital safety systems and programs that currently exist to ensure safety rather than a major program of authorization bases reconstruction and (2) uses the enforcement provisions of the Price-Anderson Act and its fee-award contract provisions in a balanced way to obtain the safety performances it expects its contractors to deliver.


Relative to the upgrading of authorization bases, the Board has been among those that have urged DOE to focus upon the specifics of hazardous operations that make up its current missions. During the past five years, the gradual implementation of integrated safety management and the concomitant adoption of authorization agreements have sharpened and clarified the safety envelope for hazardous activities at defense nuclear facilities. The pending program for assessment of vital safety systems in response to Board Recommendation 2000-2, *Configuration Management—Vital Safety Systems*, will help to further define these envelopes. While some authorization bases upgrades may still be needed, particularly those focused upon activity level hazards, the Board believes that resources should be focused upon existing vulnerabilities, such as aged fire protection and ventilation systems. Consistent with achieving safety improvements while minimizing paper requirements that do not substantially improve the safety bases, the Board is providing the enclosed technical report, DNFSB/TECH-28, *Safety Basis Expectations for Existing Department of Energy Defense Nuclear Facilities and Activities*, for DOE and contractor consideration in developing action plans responsive to the new rule.

Relative to the all-encompassing 10 CFR Part 830.120, *Quality Assurance Requirements*, provision of the rule, the Board notes that the criteria established as requirements are not

identical to those that have been long-standing in the nuclear industry. The rationale for the differences and the expectations from the contractors in response are not apparent. The provisions of 10 CFR Part 830.120 are essentially those adopted in 1995 by DOE as part of a Secretarial initiative to go towards a Total Quality Management (TQM) concept for DOE as a whole. While 10 CFR Part 830.120 does not explicitly mandate TQM, the current Guide, G 414.1-2, *Quality Assurance Management System Guide for use with 10 CFR 830.120 and DOE O 414.1*, that provides implementation guidance on the rule does embody much of the TQM philosophy and principles. Since the provisions of the quality assurance (QA) rule provide in large measure the basis upon which enforcement actions involving nuclear safety will take place, the Board believes the achievement of quality products relative to nuclear safety should more clearly be the focus of quality efforts. Unless DOE guidance makes this clear, including the acceptance of industry nuclear quality assurance standards as a way of achieving rule compliance, the rule as drafted could cause needless reworking of contractor's existing QA programs.

Further detailed comments for your consideration are provided in the enclosures.

Sincerely,



John T. Conway
Chairman

cc: The Honorable T. J. Glauthier
Mr. Mark B. Whitaker, Jr.

Enclosures

DETAILED COMMENTS

A. Definition Problems

- 1) **Section 830.201:** “A contractor must perform work in accordance with the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility and, in particular, with the hazard controls that ensure adequate protection of workers, the public, and the environment.”

Comment: This section does not add to the rule's substantive requirements, and because “work” is not defined in the rule, it could lead to unjustified applications of the rule on the one hand, or too-narrow interpretations on the other.

Proposed Change: Delete Section 830.201 and preamble discussion thereof.

- 2) **Definition of “Safety-Class SSCs”:** “Safety class structures, systems, and components means the structures, systems, or components, including portions of process systems, whose preventive or mitigative function is necessary to limit radioactive hazardous material exposure to the public, as identified by the *documented safety analysis* .”

Preamble, page 20: “Safety class structures, systems, and components means structures, systems, or components, including portions of process systems, whose preventive or mitigative function is necessary to limit radioactive hazardous material exposure to the public, as identified by the *safety analysis*.”

Definition of “Safety-Significant SSCs”: “Safety significant structures, systems, and components means the structures, systems, and components which are not designated as safety class structures, systems, and components, but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from *safety analyses*.”

Preamble, pages 21-22: “Safety significant structures, systems, and components means systems, structures, and components which are not designated as safety class systems, structures, and components, but whose preventive or mitigative function is a major contributor to defense in depth (i.e., prevention of uncontrolled material release) and/or worker safety as determined from *hazard analyses*.”

Comment: Inconsistent terminology is used in the proposed rule to describe safety analyses, hazard analyses and documented safety analysis. This inconsistency should be removed for clarity.

Proposed Change: Use “documented safety analysis” consistently.

Section 830.3, definition of “Preliminary Documented Safety Analysis”: “Preliminary documented safety analysis means documentation prepared in connection with the design and construction of a new DOE nuclear facility or a major modification to a DOE nuclear facility that provides a reasonable basis for the preliminary conclusion that the nuclear facility can be operated safely through the consideration of factors such as (1) The nuclear safety design criteria to be satisfied, (2) A safety analysis that derives aspects of design that are necessary to satisfy the nuclear safety design criteria, and (3) An initial listing of the safety management programs that must be developed to address operational safety considerations.”

Comments: (1) The PDSA should identify safety systems in addition to safety programs, and (2) the PDSA should discuss how Integrated Safety Management principles will be used for design.

Proposed Change: “~~and~~ (3) an initial listing of the safety management programs and safety systems that must be developed to address operational safety considerations, and (4) discussion of how integrated safety management principles will be integrated with the facility design.”

- 3) **Appendix Table 3, Item (8):** “nuclear facility with a limited operational life means a nuclear facility for which there is a short remaining operational period before ending the facility’s mission and initiating deactivation and decommissioning and for which there are no intended additional missions other than cleanup.”

Comment: “limited operational life” and “short remaining operational period” are not defined.

Proposed Change: Provide guidance on what these terms mean, for example, “if it would take the same or greater amount of time to prepare a DSA than the expected life of the facility or activity.”

B. Other Comments

1. **Section 830.205(c):** “A contractor for an environmental restoration activity may follow the provisions of 29 CFR 1910.120 or 1926.65 to develop the appropriate hazard controls [rather than the provisions for technical safety requirements in paragraph (a) of this section], provided the activity involves either: (1) Work not done within a permanent structure, or (2) The decommissioning of a facility with only low-level residual fixed radioactivity.”

Comment: DOE-STD-1120-98, *Integration of Environment, Safety, and Health into Facility Disposition Activities*, provides amplifying information regarding the approach to develop and content of a safety basis for facilities that are being dispositioned. Although “environmental restoration activities” are not currently within the scope of the Standard, the Standard provides a DOE memorandum that discusses restoration and disposition activities. Inclusion of DOE-STD-1120-98, or successor document, may be beneficial to implementation because of the amplifying information that is provided. (For example, refer to the Standard, sections 3.1.4 and 3.3.4)

Proposed Change: “A contractor for an environmental restoration activity may follow the method in DOE-STD-1120-98, May 1998, *Integration of Environment, Safety, and Health into Facility Disposition Activities* or successor document; and the provisions of 29 CFR 1910.120 or 1926.65 to develop the appropriate hazard controls . . .”

2. **Appendix Table 2:** “using the method in DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, July 1994 or successor document.”

Comment: DOE has issued a change notice to DOE-STD-3009-94 dated January 2000. This version contains the latest SAR guidance.

Proposed Change: All references to DOE-STD-3009-94 should read “DOE-STD-3009-94, Change Notice No. 1, January 2000, or successor document.”

3. **Section 203(e)(3):** “If the contractor discovers or is made aware of a potential inadequacy of the documented safety analysis: (1) Take action, as appropriate, to place or maintain the facility in a safe condition until an evaluation of the safety of the situation is completed; (2) Notify DOE of the situation; (3) Perform a USQ determination and notify DOE promptly of the results; and (4) Submit the evaluation of the safety of the situation to DOE prior to removing any operational restrictions initiated to meet paragraph (e)(1) of this section.”

Comment: This section assumes that USQDs are done in a timely manner. There have been instances where contractors have taken months, even years, to complete the USQD and implement appropriate controls or corrective actions.

Proposed Change: “(3) Within 30 [60] days, perform a USQ determination and notify DOE promptly of the results;”

4. **Section 204(b)(2):** “[The DSA must identify] both natural and man-made hazards associated with the facility.”

Comment: These hazards should be addressed for both facilities and activities therein.

Proposed Change: “[The DSA must identify] both natural and man-made hazards associated with the facility and with activities conducted in the facility.”

5. **Appendix Paragraph G:** “DOE Order 420.1 provides DOE’s expectations with respect to fire and criticality safety.”

Comment: DOE Order 420.1 contains requirements, not expectations.

Proposed Change: Change the word “expectations” to “requirements.”

6. **Section 830.204(b)(6):** “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: (i) Ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions, (ii) Identifies applicable nuclear criticality safety standards, and (iii) Describes how the program meets applicable nuclear criticality safety standards.

Comment: The rule does not incorporate the criticality standards identified in DOE Order 420.1.

Proposed Change: “(ii) Identifies applicable nuclear criticality safety standards including those referenced in DOE Order 420.1, *Facility Safety*.”

7. **Appendix, Sentence Preceding Table 3:** “Table 3 defines the specific nuclear facilities referenced in Table 2 that are not defined in 10 CFR 830.3.”

Comment: Table 3 defines both facilities and activities.

Proposed Change: “. . . defines the specific nuclear facilities or activities”

DNFSB/TECH-28

**SAFETY BASIS EXPECTATIONS
FOR EXISTING DEPARTMENT OF ENERGY
DEFENSE NUCLEAR FACILITIES AND ACTIVITIES**

Defense Nuclear Facilities Safety Board

Technical Report



October 2000

SAFETY BASIS EXPECTATIONS FOR EXISTING DEPARTMENT OF ENERGY DEFENSE NUCLEAR FACILITIES AND ACTIVITIES



This report was prepared for the Defense Nuclear Facilities Safety Board by the following staff members:

Farid Bamdad
James J. McConnell
Wayne L. Andrews

with assistance from:

Ronald W. Barton
Timothy J. Dwyer
Matthew B. Moury

and former staff member:

John MacEvoy

FOREWORD

In the Defense Nuclear Facilities Safety Board's (Board) Recommendation 95-2, *Integrated Safety Management*, the Board sought to have the Department of Energy (DOE) define and institutionalize a process for arriving at facility- and activity-specific control measures for hazardous work, tailored to the hazards involved. In DNFSB/TECH-5, *Fundamentals for Understanding Standards-Based Safety Management of Department of Energy Defense Nuclear Facilities*, the Board defined four major elements of safety management programs for defense nuclear facilities: (1) Standards/Requirements Identification Document, (2) Authorization Basis, (3) Authorization Agreement, and (4) Readiness Certification.

The Board issued DNFSB/TECH-19, *Authorization Agreements for Defense Nuclear Facilities and Activities*, to provide a suggested approach for preparing Authorization Agreements, with emphasis on their key elements derived primarily from the authorization basis documents. Preparation of authorization bases for defense nuclear facilities has been successful at a majority of existing facilities, mainly as a result of the requirements and guidance provided by DOE in its nuclear safety directives, such as DOE Order 5480.23, *Nuclear Safety Analysis Reports*, and supporting standards. There are, however, some instances in which a lack of proper application of existing guidance, or a lack of integration of existing guidance provided in different documents, may have hindered achieving the expected safety enhancements. This area is the subject of DOE's current programs to evaluate and upgrade facilities' authorization bases.

This report reviews some of the current practices and activities involved in the preparation of authorization bases and presents observations of the Board's staff. Specifically, this report provides suggestions for improving identification of Technical Safety Requirements for passive design features and administrative controls; providing adequate safety bases for existing facilities and activities with short remaining life; providing adequate safety bases for existing facilities and activities with long remaining life; and evaluating the adequacy of design, performance, and reliability of safety controls identified in the authorization bases for existing defense nuclear facilities.

The Board believes this report may assist DOE in providing contractors with clear guidance on how to achieve DOE's safety expectations while minimizing paper requirements. This is consistent with the Board's expectations for continuous assessment and upgrading of the safety bases of defense nuclear facilities as stated in a letter from the Board to Deputy Secretary of Energy, T. J. Glauthier, dated March 2, 2000.

John T. Conway
Chairman

EXECUTIVE SUMMARY

Operational safety at defense nuclear facilities has improved significantly since the formation of the Defense Nuclear Facilities Safety Board (Board) in 1989. Large contributions to this improvement have been made through initiatives of the Department of Energy (DOE) and the Board's recommendations. The Board's Recommendation 95-2 (Defense Nuclear Facilities Safety Board, 1995) and DOE's issuance of new and updated safety directives (such as the 5480 Order series) exemplify such activities.

Implementation of Integrated Safety Management (ISM) Systems at defense nuclear facilities, along with the requirements and guidance provided in DOE Order 5480.23, *Nuclear Safety Analysis Reports* (U.S. Department of Energy, 1992), and its supporting standards, provide a process for the preparation of safety analyses. This process involves methodically and systematically identifying hazards associated with the work being performed, analyzing those hazards, identifying the necessary controls, implementing those controls, and improving operational safety through feedback of lessons learned. Implementation of this process has been largely successful at the majority of existing defense nuclear facilities. There are, however, some instances in which a lack of proper application of existing guidance or lack of integration of existing guidance with the elements of ISM may have limited the achievement of successful results.

This report identifies some areas in need of further guidance and proposes additional guidance for evaluation of existing or preparation of new authorization bases. Currently, there are no consistent expectations for performance, functionality, and reliability of the safety controls that are identified in the authorization bases of existing defense nuclear facilities, especially passive design features and administrative controls. This report demonstrates the need for additional DOE guidance concerning safety structures, systems, and components (SSC), and presents a suggested approach for evaluating the design, performance, and reliability of safety related controls. In summary, this report:

- ! Demonstrates that in many cases, Basis for Interim Operation reports prepared using bounding analyses of hazards need to be supplemented with process hazard analyses as recommended by DOE or replaced with an appropriately tailored Safety Analysis to identify the controls necessary for a given activity to be performed safely.
- ! Presents an approach for tailoring the 17-chapter Safety Analysis Reports (currently recommended by DOE standards) using existing ISM provisions for more effective use of resources and integration of safety initiatives.
- ! Identifies important attributes and characteristics of passive design features and administrative controls consistent with the consequences of the accidents they are intended to help prevent or mitigate.
- ! Shows the need for a directive or DOE-recommended process and suggests a methodology and principal elements for evaluation of design, performance, and reliability of existing design features and safety SSCs that are identified in the authorization basis documents.

TABLE OF CONTENTS

Section	Page
1 INTRODUCTION	1-1
1.1 Background	1-2
1.2 Purpose of This Report	1-3
2 AUTHORIZATION BASES	2-1
2.1 Use of Basis for Interim Operation as Safety Basis	2-1
2.2 Features and Components of Authorization Bases	2-2
3 TAILORED AUTHORIZATION BASIS	3-1
3.1 Existing Facilities with Short Remaining Life	3-1
3.2 Existing Facilities with Long Remaining Life	3-4
3.3 New Activities within Existing Facilities	3-8
4 QUALIFICATION OF CONTROLS	4-1
4.1 Identification of Controls	4-1
4.2 Feedback and Improvement	4-4
APPENDIX A. TECHNICAL SAFETY REQUIREMENTS	A-1
APPENDIX B. DESIGN AND PERFORMANCE ADEQUACY REVIEW	B-1
REFERENCES	R-1
GLOSSARY OF ACRONYMS	GL-1

1. INTRODUCTION

In Order 5480.23, *Nuclear Safety Analysis Reports* (U.S. Department of Energy, 1992), the Department of Energy (DOE) requires that contractors responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities complete safety analyses demonstrating the adequacy of the facilities' safety bases. This expectation, which is simple to articulate, has proven difficult to realize. DOE and its contractors have had even more difficulty in agreeing upon the required format and content of the reports that document safety analyses.

To improve the analysis and communication of the bases for safe operations at defense nuclear facilities, Order 5480.23 (U.S. Department of Energy, 1992) sets forth expectations for a document called a Safety Analysis Report (SAR). These expectations include expanding the documentation of safety bases beyond the traditional focus on hardware designed to protect the public to include all elements of the safety system (e.g., procedures, training, and management) and to encompass protection for workers and the environment. DOE realized that such a shift would require time to implement, even though it would be desirable to start accruing the benefits as soon as possible. To facilitate implementation of its new expectations for safety analysis and documentation, DOE allowed its contractors to develop phased implementation plans and to tailor their responses as appropriate. To expedite the benefits of the new approach, DOE required its contractors to develop Bases for Interim Operations (BIO) that would document the safety of operations during the period prior to completion of the final upgraded safety analyses and reports. DOE communicated its expectations for these temporary documents in DOE-STD-3011-94, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plan* (U.S. Department of Energy, 1994):

It is emphasized that because of the interim nature and expected level of effort of the BIO, maximum use of appropriate existing programs and safety documentation is encouraged, and discussions on the covered topics should be brief and by reference where possible.

This approach was deemed reasonable given DOE's original intent that the BIOs would be relied upon only for a short period. However, most of the BIOs prepared to date have significant potential shortfalls when used as de facto final safety analyses or safety bases.

There are some safety analyses prepared in accordance with DOE's recommended format and content for existing facilities that could be improved by applying a process for design and performance adequacy reviews of safety controls. This is a process by which safety controls are systematically evaluated to ensure that credit given in the safety analyses is technically justified. However, guidance is lacking on a recommended process for identification, performance readiness, cost-benefit analysis, and review and approval of safety controls (safety-class or safety-significant) that would enhance the safety and protection of the public and workers.

1.1 BACKGROUND

DOE issued Order 5480.23 (U.S. Department of Energy, 1992) and its guiding standard, DOE-STD-3009-94 (U.S. Department of Energy, 1994), in 1992 and 1994, respectively, to bring the safety bases of defense nuclear facilities to an acceptable level consistent with then current commercial nuclear practices. The requirements and recommendations in these DOE directives are prescriptive and detailed, and taken primarily from the requirements for safety bases of commercial nuclear reactors.

In 1995, the Defense Nuclear Facilities Safety Board (Board) issued Recommendation 95-2, *Integrated Safety Management*, and two technical reports, DNFSB/TECH-5, *Fundamentals for Understanding Standards-Based Safety Management of Department of Energy Defense Nuclear Facilities* (DiNunno, Defense Nuclear Facilities Safety Board, 1995), and DNFSB/TECH-6, *Safety Management and Conduct of Operations at the Department of Energy's Defense Nuclear Facilities* (Kouts and DiNunno, Defense Nuclear Facilities Safety Board, 1995). These documents were intended to introduce the concept of Integrated Safety Management (ISM) and to ensure enhanced safety of operations at defense nuclear facilities through its implementation. In response to Recommendation 95-2, significant changes were made to the way contractors implemented safety measures. They were required to prepare authorization basis documents that identified the hazards of the work, analyzed those hazards, and identified the necessary controls. Contractors were also expected to sign Authorization Agreements with DOE that identified their safety commitments regarding the implementation of specific controls and adherence to the associated terms and conditions.

In 1998, the Board issued DNFSB/TECH-19, *Authorization Agreements for Defense Nuclear Facilities and Activities* (Bamdad, Defense Nuclear Facilities Safety Board, 1998), presenting some guidance and a suggested approach for the preparation of Authorization Agreements. Guidance provided in DOE Order 5480.23 (U.S. Department of Energy, 1992) and DOE-STD-3009-94 (U.S. Department of Energy, 1994) was comprehensive enough to be adequate for the preparation of authorization basis documents that serve as a foundation for these Authorization Agreements. With the exception of a few facilities, however, this guidance has not been implemented satisfactorily, for several reasons:

- ! Contractors perceive that the guidance is too prescriptive, and although it allows for tailoring based on three defined criteria, it provides inadequate information on how the tailoring should be accomplished.
- ! The guidance needs revision to be consistent with the ISM methodology being implemented at defense nuclear facilities.
- ! The guidance does not provide for contingencies, for expectations regarding potential upgrades, or for qualification of the existing controls to meet some consistent level of reliability for defense nuclear facilities with similar hazards. Instead, the guidance is used to establish the safety of existing facilities based on the existing design and operational boundaries of the facilities.

DOE and its contractors have executed Authorization Agreements for the majority of hazard category 2 defense nuclear facilities. The foundation for these Authorization Agreements is the authorization bases in place at the time. The hazard analyses supporting some of these authorization bases, while adequate in the short run, do not satisfy the expectations for an appropriately tailored safety basis suitable for a complex operation with a long remaining operational lifetime. Some of these authorization basis documents do not describe the current operations in the facility, are based on inadequate bounding scenarios, use the evaluation guideline (25 rem) as a criterion for identifying Technical Safety Requirements (TSR), or do not address worker safety. Although these authorization bases are acceptable for an interim period, appropriate tailoring of DOE's requirements would lead to a more robust analysis in many cases.

1.2 PURPOSE OF THIS REPORT

The purpose of this report is to identify a minimum set of expectations for preparation of safety bases of existing defense nuclear facilities and activities that would demonstrate the adequacy of their safe operations. This report is not intended to generate additional requirements for preparation of authorization basis documents, or produce more volumes of documents. On the contrary, this report emphasizes reducing administrative burden and duplication of the information provided in these documents.

There is significant confusion regarding expectations for the safety analysis and SAR for some DOE facilities. However, this is not necessarily the case for the design phase of a new facility. The physical facility has not yet been built, so numerous options for control schemes are available for consideration. The question with regard to preparation of the safety bases for new defense nuclear facilities is related to DOE's expectations for the amount of safety information to be provided in a Preliminary SAR or Final SAR. DOE Order 5480.23 (U.S. Department of Energy, 1992), its attachment, DOE Order 420.1, *Facility Safety* (U.S. Department of Energy, 1995), and its implementation guides provide some guidance on preparation of Preliminary SARs and Final SARs for new facilities and major modifications to existing facilities.

Major problems arise most commonly when DOE seeks to improve the safety basis for an existing facility, in particular when establishing an "interim" safety basis that is more appropriate for a facility with short remaining life and may not be suitable to serve as the final or long-term safety basis for a facility with long remaining life. Problems also occur when justifying the safety basis of a facility within the bounds of an existing design that may not be adequate to provide the assurance needed for long-term operation. Therefore, two categories of facilities and operations (and associated analyses and reports) require some additional guidance: (1) existing facilities with a relatively long remaining life and (2) existing facilities with a short remaining life.

This report reviews some of the DOE practices and activities in response to the implementation of ISM, examines how these activities may be tied to the safety bases and tailoring of the authorization bases for the facilities, and proposes an approach and the principal elements to be addressed in authorization bases to make them consistent with the intent of ISM and DOE's expectations. The proposed approach encompasses existing facilities with both limited and long-term programmatic missions. The report also documents some of the existing problems in identifying TSR level controls that may have been caused by DOE's lack of an accepted process or guidance.

2. AUTHORIZATION BASES

2.1 USE OF BASIS FOR INTERIM OPERATION AS SAFETY BASIS

One of the fundamental purposes of this report is to discuss the need to augment BIO reports with *process* hazard analyses. Before addressing that point however, it is important to distinguish between BIOs that are intended to be in effect for an interim period and those that can be designated as final safety basis documents. The latter case occurs most often for facilities that have short remaining operational missions; in such cases, the BIOs need to be supplemented by process hazard analyses. The term “interim” for these BIOs should be replaced by “short-term,” and the period involved is based on the operational plans for the facility itself.

In contrast, those BIOs that were written as compensatory measures to satisfy minimal expectations until more appropriate analyses and documentation were available (e.g., a new SAR) can truly be identified as “interim.” The period that this class of BIOs is expected to cover should be defined by the time required to develop and approve the upgraded final safety basis. This type of BIO is typically generated for existing facilities that have substantial hazards and substantial remaining operational lifetimes. Prolonged reliance on this class of BIOs (de facto final safety analyses), due to delays in developing a suitable replacement, can potentially expose the public, and more likely workers, to unanalyzed hazards.

Some BIOs and the analyses that support them are appropriately tailored to satisfy DOE’s expectations for a final safety basis (particularly for facilities facing deactivation or decommissioning that are near the end of their programmatic life). On the other hand, some older safety analyses (prepared mainly in the 1980s) that have been submitted and approved as BIOs would not provide adequate technical rationale to serve, even temporarily, as the authorization basis for a hazardous nuclear activity with a long remaining mission life.

The hazard analyses supporting the BIOs for nuclear facilities are generally based on a review of the bounding scenarios identified for event categories. The analyses do not reflect an attempt to prevent or mitigate accidents with lesser consequences than those of the bounding accident scenarios unless the preventive or mitigative controls are the same. In addition, BIOs generally do not attempt to establish defense-in-depth controls. For example, events are categorized as fires, spills, or explosions, and the bounding scenarios are assessed qualitatively for the identification of facility-level, and in a few cases activity-level, controls for protection of the public. Given their intended short-term function, these BIOs generally are not based on detailed *process* hazard analyses that enable the identification of activity-level controls needed for worker protection. Many BIOs do not include the analysis of consequences to workers and collocated workers or the development of associated controls. This limitation of BIOs, combined with delays in developing SARs or expanded safety bases that include such analyses and resultant controls, suggests that the hazards to workers may not be adequately assessed.

Appendix A to DOE-STD-3011-94 (U.S. Department of Energy, 1994) provides summary guidance for the development of BIOs given its intended function to specify expectations for short-lived documents. This has led to wide variability in the rigor and completeness of the BIOs for facilities across the complex and even within a particular site. There is a need for additional DOE guidance to define what constitutes an adequate authorization basis for facilities throughout the complex that continue to rely on a BIO as the cornerstone of their safety basis. Some existing BIOs are inadequate regardless of whether they are to serve as interim or final authorization basis documents (Letter, Conway to Glauthier, 1999).

2.2 FEATURES AND COMPONENTS OF AUTHORIZATION BASES

The authorization basis for a facility is defined in DOE Order 5480.21, *Unreviewed Safety Questions* (U.S. Department of Energy, 1991), as “those aspects of the facility design basis and operational requirements relied upon by DOE to authorize operation.” The Board considers the authorization basis to be “the composite of information a contractor must provide in response to all ES&H (environment, safety and health) requirements applicable to a facility” (DiNunno, Defense Nuclear Facilities Safety Board, 1995). This information is used by DOE as the basis for signing an Authorization Agreement. The information provided in the authorization basis should, at a minimum, include identification of the hazards of the work, analysis of those hazards, and identification of required controls.

The authorization basis of a facility or activity may comprise several documents: SAR or Basis for Operation (BFO), activity-based hazard analysis, site generic safety analysis, TSRs or Operational Safety Requirements, fire hazard analysis (FHA), Safety Evaluation Report, environmental assessment or impact statement, and (potentially) Emergency Hazard Assessment (EHA). In the following paragraphs a brief description of each of these documents and its relationship with the authorization basis of the facility or activity is provided.

Safety Analysis Report and Basis for Operation. These reports document the safety basis of a facility or operation and demonstrate its adequacy for safe operation, construction, and/or decommissioning (maintenance and shutdown are considered to be modes of operation). These documents systematically identify the hazards of the work; analyze those hazards; and identify the controls needed to eliminate, prevent, or mitigate the hazards to protect the public and workers. Although the content of these documents may vary throughout the complex, they are referred to interchangeably in this report as they both contain the same type of material.

Activity-Based Hazard Analysis. This analysis is focused on the hazards posed by a specific activity. A systematic hazard analysis of the activity is performed to complement other safety analyses that may have been done for the facility where the activity will occur. In this context, the activity-based hazard analysis does not constitute the authorization basis by itself because it may not address external events and natural phenomena hazards, interaction with other activities, or hazards associated with the facility itself.

Site Generic Safety Analysis. The Management and Operating contractor may determine that it is more cost-effective to document the common sections of SARs for several facilities located at the same site in a generic document. This analysis may contain such information as site characterization, natural phenomena hazards, and commitments to site safety programs that would otherwise be included in individual SARs or BFOs. The controls identified in this analysis should complement those identified in more specific hazard analyses; therefore, this document should be referenced in the Authorization Agreement for each specific facility or activity.

Technical (or Operational) Safety Requirements. The information provided in these documents consists primarily of (1) requirements for passive and active engineered design features of structures, systems, and components (SSCs) and their support systems; (2) associated safety, design, or operational limits; and (3) administrative controls and work practices identified for protection of the public, the workers, and the environment. A significant number of TSR documents are prepared using DOE guidance

on format and content without a good understanding of the hierarchy of controls and their specific characteristics or interrelationships. Specifically, the existing defense nuclear facilities rely heavily on their passive design features (such as fire barriers, tanks, pipes, and vessels) for preventing harmful consequences in the event of an accident. These design features may have specific attributes that are taken credit for and should be preserved to control the hazards. For example, the thickness and continuity of fire walls should be preserved to prevent fires from spreading rapidly, or the thickness and leak-tightness of tanks should be maintained to confine radioactive materials. These attributes and their routine surveillance programs should be called out in the TSRs to ensure compliance and avoid deterioration. Many of the existing TSR documents lack such information and the corresponding requirements.

***Suggestion:** The important attributes of the passive design features that are taken credit for in the accident analyses should be identified in the TSRs for routine examination and ensuring that the assumed parameters are controlled throughout the life of the facility. Appendix A of this report describes the expected contents of a TSR document in more detail, including specific characteristics of the elements of such a document.*

Fire Hazard Analysis. DOE Order 420.1 (U.S. Department of Energy, 1995) requires that properly graded FHAs be developed for all nuclear facilities and facilities that represent unique or significant safety risks. It also requires that the conclusions of the fire hazard analysis be incorporated into the SAR accident analysis, and integrated into design basis and beyond design basis accident conditions. Some FHAs for defense nuclear facilities are not completed with enough rigor or detail to allow effective incorporation into SARs. The results of the FHAs, to the extent that they address the fire hazards of the facilities, should be considered as part of the facilities' authorization basis, and the associated controls should be considered for incorporation into the TSR document.

Safety Evaluation Report. The documents identified above are prepared by the contractor and submitted to DOE as the safety bases for the operations or activities whose authorization is requested. The results of DOE's review of these documents, any independent analyses or justification, any additional controls or restrictions on the operations, or further information needed for approval of the operations or activities are documented in a Safety Evaluation Report. This document is part of the authorization basis of the activity.

Environmental Assessment or Impact Statement. These documents are prepared in response to the requirements of the National Environmental Policy Act of 1969. They contain hazard analyses and estimates of the potential health effects of alternatives designed to meet the recommendations of the Council for Environmental Quality. They may also result in a Mitigation Action Plan that sets forth commitments for mitigating the adverse environmental impacts associated with the alternatives. These mitigative measures may be controls that are needed for protection of workers, the public, or the environment. They should, therefore, be considered part of the authorization basis of the preferred alternative when a Record of Decision is made and construction or operation of the alternative is authorized.

Emergency Hazard Assessment. This document is prepared in response to the requirements of DOE Order 151.1, *Comprehensive Emergency Management System* (U.S. Department of Energy, 1995). The contractor is required to perform a systematic hazard analysis of all nuclear and non-nuclear facilities on site. The results of this effort are documented in the EHA to support the definition of emergency planning zones and to aid in the classification of potential events. The EHA may be more comprehensive in identifying all the site hazards than any specific facility safety analysis. It may also make assumptions with regard to the amount of inventory, the reliability of controls, and the response time for mitigating events that may be needed for site safety or considered for incorporation into the Authorization Agreement. The EHA, therefore, should be reviewed for its potential to serve as part of the authorization basis, or the pertinent controls and assumptions of the EHA should be extracted for incorporation into the Authorization Agreement.

The broader definition of authorization basis by the Board, the composite of information provided in response to all ES&H requirements, introduces some other documents to the set identified by DOE. These documents may contain controls for operational hazards of a facility or activity that are identified to support Federal (e.g., Environmental Protection Agency) or State requirements for discharges to the environment, such as permits required for discharge of radioactive materials to water and air. DOE and the Management and Operating contractors for defense nuclear facilities are responsible for acquisition of these permits. In effect, the documents prepared and provided to State or Federal agencies to acquire the permits (authorizations) are also part of the authorization basis of the activity or facility. The controls identified in these documents must also be implemented and maintained to ensure compliance with the commitments made in the permit requests.

3. TAILORED AUTHORIZATION BASIS

The most important aspect of developing an authorization basis is the process of identifying the hazards of the work, analyzing the hazards, and identifying the necessary controls. The nuclear safety information pertinent to this process is usually found in the facility or activity safety basis documents (i.e., SAR/BFO, BIO, and activity-based hazard analysis). For the remainder of the discussion in this report, it is assumed that the BIO or SAR contains the activity-based hazard analysis. An approach is suggested for cases in which this assumption may not be valid.

Paragraph 8.a of DOE Order 5480.23 (U.S. Department of Energy, 1992) describes the graded approach for the level of analysis. The essence of the requirements is that the level of effort necessary for preparation of a SAR should be proportionate to three factors:

- ! The magnitude of the hazards,
- ! The complexity of the facility and systems, and
- ! The stage or stages of the facility life cycle for which DOE approval is sought.

The discussion in the attachment to the Order elaborates on each of these factors and the grading of the SAR to accommodate the requirements. In addition, the attachment provides some high-level guidance on how to determine what the contents of each chapter should be and to what level of detail the information should be provided. This level of guidance would appear to be appropriate and adequate considering the diversity of defense nuclear facilities and their life-cycle expectations. However, judging by the number of updated SARs to date, this approach has not been successful.

The following subsections provide additional guidance based on the experience of the Board's staff in reviewing SARs and BIOs during the past 8 years (since issuance of the Order), including consideration of DOE's successful development of ISM Systems that are currently being implemented at defense nuclear facilities. This discussion is not intended to replace the requirements of the DOE Order or the guidance provided in its attachment, but merely to organize the contents in accordance with the requirements of an ISM System. Guidance is also provided on the contents of SARs and BIOs that reflects current knowledge of the status of authorization basis documents for defense nuclear facilities and areas for improvement.

3.1 EXISTING FACILITIES WITH SHORT REMAINING LIFE



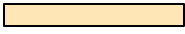
This group of defense nuclear facilities falls into two categories: those that are performing their intended mission-related function for a relatively short period of time and are expected to be shut down within a few years, and those that are generally no longer used for their original programmatic mission and are in the deactivation and decommissioning stage of their life cycle or in a surveillance and maintenance mode at the time their authorization bases are prepared. Most of these facilities are authorized to continue their operations based on a BIO that is either a compilation of the old limited-scope SARs or a preliminary hazard analysis, sometimes complemented by a bounding accident analysis. Little additional insight can be gained from these documents beyond what was available about a decade ago concerning the bounding risk of the operations.

These authorization basis documents may identify some controls that would limit the consequences of a set of bounding scenarios, such as large fires, major spills, bounding explosions, and criticality accidents. DOE approval is sought on the basis of the consequences of the bounding events and the associated risks. These authorization bases, however, may not identify the defense-in-depth measures or the level of protection provided for workers conducting specific activities in the facility (because a detailed *process* hazard analysis [PrHA] as recommended by DOE may not have been performed) as illustrated in Figure 3-1.

DOE-STD-3009-94 (U.S. Department of Energy, 1994), recommends that, “references such as *Guidelines for Hazard Evaluation Procedures* (1992) provide acceptable guidelines for selecting hazard evaluation techniques.... The techniques used for hazard evaluation can range from simple checklists or What-If-analyses to systematic parameter examinations such as Hazard and Operability Analyses (HAZOPS).... Application of a graded approach is based on the judgement and experience of the analysts....” This process, however, has been recommended for performing hazard analyses in preparation of the SARs meeting Order 5480.23 (U.S. Department of Energy, 1992) requirements. This process has rarely been applied to the preparation of BIOs even though it is a recommended and acceptable approach by DOE for identification of hazards and their associated controls.

Since the BIO for this type of facility is, in many cases, based on older documents, the activities analyzed are often related to the original programmatic mission of the facility. At the level of a bounding analysis, the hazards and accident consequences are relatively independent of the specific activities in the facility, and therefore the original bounding analyses may still be largely applicable as a facility transitions from operations to cleanup and decommissioning. The controls identified for these bounding scenarios, however, should be examined against the hazards identified for the new activities to ensure adequacy. At the activity level, however, the controls needed to harness the hazards presented during the short-lived operation, deactivation, deinventory, and decommissioning can be significantly different from those identified for the bounding scenarios shown in the BIO. For this reason, these BIOs need to be supplemented by an appropriately tailored PrHA for each hazardous activity that is intended to be performed during the remaining life of the facility, but was not adequately analyzed in the BIO. Controls need to be identified that will limit the consequences to the public and workers to acceptably low values for scenarios that are bounded by those in the BIO.

Such improvements to facility safety bases are appropriate ISM activities, following the Phase II ISM verification now being completed across the complex. Since the safety basis may be tailored for each operation (which may itself be a hazardous but short-duration activity), the development and documentation of the activity-level safety basis are often best handled outside the BIO. The contractor should have already identified, as part of its contract with DOE, the requirements for site safety management programs (e.g., radiation protection and criticality safety). The contractor should also have developed some manuals of practice for implementation of those requirements at the site. Implementation of the requirements in these manuals is therefore contractually binding, and they may not need to be specifically identified and described in the BIO unless there are deviations from these manuals to be documented. Likewise, it may be appropriate to expand on some of the requirements to provide necessary details on safety programs relative to a particular activity. A reasonable alternative to revising the BIO for these reasons would be incorporation of the deviations in the Authorization Agreement.

-  **Bounding Accidents**
-  **Hazardous Environment to Facility Workers**
-  **Hazardous Environment to Collocated Workers**

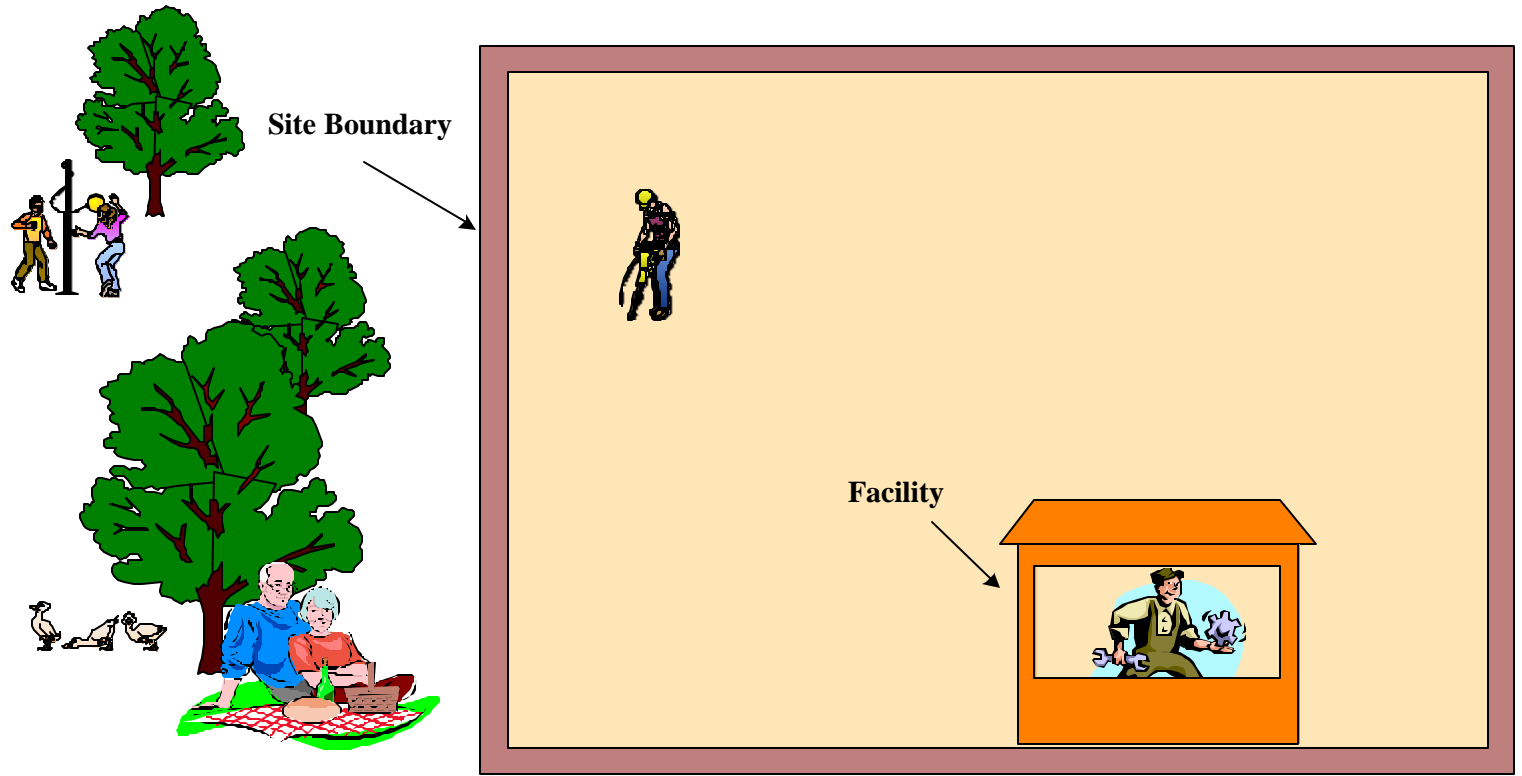
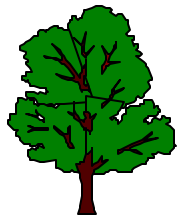


Figure 3-1. Hazardous Environment and Potential Receptors

***Suggestion:** As has been proposed by DOE, the existing authorization bases (i.e., the BIO), supplemented by PrHAs for activities to be performed in the facility, may serve as an adequate safety basis for the operations of these facilities with short remaining operational lifetimes. The commitment to perform a PrHA for any hazardous activity intended to be performed and to identify and implement the necessary controls, along with any other terms and conditions, may be stipulated in the Authorization Agreement for the facility. This may be accomplished by amending existing Authorization Agreements for facilities with this type of BIO as their authorization basis.*

3.2 EXISTING FACILITIES WITH LONG REMAINING LIFE

A large number of defense nuclear facilities fall in this category of facilities that have been built during the last 50 years and will be supporting defense missions in the foreseeable future. These facilities house activities that range from processing of nuclear materials and waste, to assembling and disassembling of nuclear weapons, to staging and storing of nuclear weapons and special nuclear materials. These facilities are specifically the focus of the requirements in DOE Order 5480.23 (U.S. Department of Energy, 1992), which expects safety analysis upgrades that includes:

- ! Addressing institutional and human factors in addition to relying on safety design and hardware features.
- ! Defining clearly the technical commitments for the safety envelope of anticipated facility operations.
- ! Providing the current facility safety bases to support programmatic decisions.
- ! Keeping the documented safety analyses current and up to date.
- ! Making appropriate use of new safety analysis methods to identify and analyze hazards, as well as the controls needed to eliminate, prevent, or mitigate those hazards.

Over the last eight years DOE contractors have attempted to revise and upgrade their authorization basis documents. In many cases this effort has generated volumes of information that have little or no added safety benefits. The discussions in this section are focused on the technical contents of authorization basis documents and how safety can be improved with minimum administrative burden and elimination of redundant or unnecessary activities to prepare them.

The guidance provided in the attachment to the Order and its supporting standard, DOE-STD-3009-94 (U.S. Department of Energy, 1994), describe in detail DOE's expectations and the methodologies that can help meet those expectations. The intent is to provide an up-to-date safety basis for

operations at defense nuclear facilities to ensure that the public, the workers, and the environment will be adequately protected. To that extent, the Order and its implementing guides are consistent with the Board's Recommendation 95-2. The Order, however, was issued several years before Recommendation 95-2 and the advent of ISM. The

ISM System provides a safety basis for the operation of defense nuclear facilities that is more comprehensive and seamless. DOE Order 5480.23 (U.S. Department of Energy, 1992) was written generically to be applicable to both new and existing defense nuclear facilities. Although DOE-STD-3009-94 (U.S. Department of Energy, 1994) was issued to describe in more detail those aspects of the Order that required additional guidance for existing facilities and operations, the standard does not reflect contractors' infrastructure developed from the implementation of ISM at their sites. The following proposes an alternative approach aimed at meeting the requirements of the Order in the context of ISM and reducing redundancy in the generation of certain documents required under both methodologies.

DOE-STD-3009-94 (U.S. Department of Energy, 1994) describes in detail the format and content of SARs based on the requirements of DOE Order 5480.23 (U.S. Department of Energy, 1992). Table 3-1 lists the 17 specified chapters of a SAR and their correlation with the requirements of the Order. Chapters 6 through 17 describe the safety management programs applicable to the facility. The foreword to DOE-STD-3009-94 (U.S. Department of Energy, 1994) states that "the programmatic chapters, including Chapters 6-17, provide a summary description of the key features of the various safety programs as they relate to the facility being analyzed. These chapters are not meant to be used as the vehicle for the determination of adequacy of these programs." These programs are identified by the standard as being of such significant safety importance that they must be described in the SAR. This may have been a recommended approach and commercial practice at the time the directives were published; with the emergence of ISM and its implementation at defense nuclear facilities, however, the standard's approach may need to be revisited.

Table 3-1. Comparison Requirements in DOE Order 5480.23 with Contents of a Safety Analysis Report Recommended in DOE-STD-3009-94

Topic	STD-3009-94 Chapter	DOE Order 5480.23 Topic 8.b.(3)
Executive Summary	Unnumbered	(a)
Site Characterization	1	(c)
Facility Description	2	(d)
Hazard Analysis	3	(e)
Accident Analysis	3	(k)
Safety Structures, Systems, and Components	4	(d)
Derivation of TSRs	5	(p)
Criticality Safety Program	6	(h)
Radiation Protection	7	(i), (k)
Hazardous Material Protection	8	(j), (k)
Waste Management	9	(g), (k)
Surveillance and Maintenance Program	10	(o)
Operational Safety	11	(q)
Procedures and Training	12	(m)
Human Factors	13	(n)
Quality Assurance	14	(r)
Emergency Management	15	(s)
Provision for Deactivation and Decommissioning	16	(t)
Institutional Safety Program	17	(l)

DOE issued its Department of Energy Acquisition Regulations (DEAR) clause, 48 Code of Federal Regulations (CFR) § 970.5204-78, as a step in the implementation of ISM at defense nuclear facilities. This DEAR clause states that “in performing work, the contractor shall comply with the requirements of applicable

Federal, State, and local laws and regulations (List A),” and “those Department of Energy directives, or parts thereof, identified in the List of Applicable Directives (List B) appended to the contract.” The requirements for developing the safety programs identified in DOE-STD-3009-94 (U.S. Department of Energy, 1994) as Chapters 6 through 17 of the SAR should therefore be identified in List A (e.g., Radiation Protection) or List B (e.g., Criticality Safety) and appended to the contract for existing facilities. The contractor is obligated to prepare program plans to comply with these requirements and implement them according to the contract. Identification and description of these safety programs (which are contractually binding) in the SAR would add neither to the safety of operations nor to the contractors’ obligations. If they are applicable to the facility or activity on the basis of its scope of work, they should be identified in the Administrative Controls section of the TSRs briefly as programs that are relied upon for safety and should be tracked as terms and conditions of the Authorization Agreement. If the mission of the facility or scope of the activity does not warrant commitment to the site programs (or requires a different program), this should be noted in the safety basis, supplemented by those specific attributes that are identified in the hazard analysis.

In fact, implementation of the DEAR clause would result in Lists A and B that should include the requirements for these programs, identified and appended to the contract. In other words, DOE and the contractor should agree on a set of requirements for each safety program that is deemed necessary for operating a facility (or facilities) at the site at the time of signing the contract or its amendments. These requirements lend themselves to the contractor’s preparation of manuals of practice to ensure that the contract is implemented. DOE can review these manuals and ensure that they meet the requirements and the intended needs. As the SAR is developed, rather than rewriting a description of these programs, the SAR can simply refer to these manuals as they should be implemented at the site. The extent to which these programs are credited for controlling the identified hazards should be reviewed by the contractor to ensure consistency and integration with the safety bases of the operations. If there are deviations from the site programs that are deemed appropriate for a specific facility, they may be identified in the SAR or in the corresponding section of the Authorization Agreement.

There may be some instances in which additional statements are needed to demonstrate how the site safety programs are implemented at the facility. For example, there may be a site hazardous waste management program that complies with all government regulations; however, the safety analysis needs to demonstrate how the site program is implemented at the specific facility and for its pertinent operations.

On the other hand, portions of Chapters 1 through 5 may have been described in other documents as discussed in Section 2 of this report. For example, site characterization or natural phenomena hazards may have been described in a Site Generic Safety Analysis document. The facility or activity safety analysis may be further consolidated by referencing such documents and reducing duplication of information provided to DOE.

Suggestion: *An adequate Safety Analysis can be reduced to Chapters 1 through 5 as shown in Table 3-1 and described in DOE-STD-3009-94 (U.S. Department of Energy, 1994) (with reference to the required manuals of practice for safety programs) without reducing the rigor of the safety basis. A graded approach for preparation of the Safety Analysis should be applied using the guidance provided in the Order and its attachment.*

The guidance given in the standard for these five chapters (as supplemented by the Board's letter of July 8, 1999), if implemented properly, should result in an adequate safety basis for operations conducted at existing defense nuclear facilities.

The requirements of the Order for preparation of updated safety bases and their documentation in a SAR, however, have been applied only to a few hazard category 2 facilities. The majority of the existing facilities have submitted authorization basis documents in the form of BIOs, which have been approved by DOE. These documents are not referred to as Safety Analyses because they do not meet the requirements of DOE Order 5480.23 (U.S. Department of Energy, 1992). They could be revised to meet the requirements of the Order, guided by the approach proposed in this report, and employed as the safety bases for the ongoing operations in the facilities.

3.3 NEW ACTIVITIES WITHIN EXISTING FACILITIES

DOE owns a wide variety of nuclear facilities, many of which are one-of-a-kind and encompass numerous different technologies. As facility owner, DOE accepts the residual risk of operating these facilities through the review and approval process of their authorization bases. To allow contractors flexibility to conduct operations, make physical or procedural changes, or perform tests and experiments prior to the owner's approval, DOE has issued Order 5480.21, *Unreviewed Safety Questions* (USQ) (U.S. Department of Energy, 1991). The requirements of this Order and the guidance included in its attachment provide detailed information on the application of the Order and associated DOE expectations.

In the past, however, many situations have arisen that indicate misapplication or misunderstanding of the intent of Order 5480.21 (U.S. Department of Energy, 1991) at defense nuclear facilities. The problem relates to the performance of new hazardous activities within existing facilities. The issues become more significant when the activities are planned to be performed in facilities that do not have a DOE-approved authorization basis, or when the new hazardous activity would establish a higher hazard categorization for the facility than already approved by DOE. The following discussion is intended to clarify some of the expectations related to such situations. As stated earlier, the goal is to perform hazardous activities safely and not to generate additional unnecessary administrative burden or paper work.

A hazards evaluation (e.g., PrHA) needs to be performed for any new hazardous activity, regardless of the outcome of the USQ screening or determination. This hazards evaluation is to satisfy the DOE requirements for a "safety evaluation" to support the USQ process. The hazards evaluation should be tailored to the activity and the level of hazard that it poses. It may vary from a work permit and simple check list to a detailed PrHA as recommended by DOE-STD-3009-94 (U.S. Department of Energy, 1994). Performance of this evaluation is consistent with the ISM methodology currently implemented at defense nuclear facilities. The safety evaluation should systematically identify the hazards associated with the activity, analyze the hazards, and identify the necessary controls to ensure that the activity will be performed safely. The USQ process is used to determine whether the new activity is within the bounds of the approved authorization basis

of the facility where it is planned to be performed, or DOE approval is needed. The hazards evaluation should include a PrHA of the activity, an assessment of the impact of external events on the activity, and considerations for natural phenomena hazards (NPH). If the activity is planned to be performed within an existing facility with an approved authorization basis, the hazards common to the facility (e.g., NPH) may have been addressed. The scope of the hazard analysis, therefore, may be limited to the hazards posed by the activity (identified through a PrHA) and the hazards posed to the activity by the facility (e.g., from other activities being performed therein). Thus a safety envelope may be generated for the new hazardous activity within an existing facility.

Sometimes, activities are planned to be performed in a facility that does not have an approved authorization basis, or the approved authorization basis is for a lower hazard category than that posed by the planned activity. The safety envelope discussed above may be generated for such activities in the form of a BIO or an amendment to the existing authorization basis, consistent with the guidance provided in this report, and submitted to DOE for review and approval.

The approach presented here is consistent with existing DOE guidance provided in the attachments to Orders 5480.23 (U.S. Department of Energy, 1992) and 5480.21 (U.S. Department of Energy, 1991). Although DOE has been conducting training sessions on the USQ process, a persistent problem exists in this area that has led to misuse or misapplication of the process. The lack of familiarity with or understanding of the USQ process by DOE and its contractors' personnel can lead to inadequate safety bases for many new activities.

Suggestion: *DOE needs to improve its guidance on the applicability and implementation of the USQ process at defense nuclear facilities to properly maintain configuration management of the facilities' authorization bases. A complex-wide review of the USQ programs at defense nuclear facilities is needed to identify the relevant contents of a training program. The training program should encompass the purpose, rationale, use, and application of the USQ process; practical examples of real cases across the complex; and identification of shortfalls.*

4. QUALIFICATION OF CONTROLS

In an existing facility, the ability to reengineer processes to avoid hazards completely may be limited. Consequently, safety analyses for existing facilities tend to be focused on preventing accidents or mitigating their consequences. Constraints associated with an existing facility also affect the philosophical hierarchy for selection of controls. As a general practice, safety controls based on engineered hardware (e.g., SSCs) are preferred to administrative controls because they are usually more reliable and more predictable. In existing facilities the engineered systems available to provide safety controls may be limited, resulting in additional reliance on administrative controls.

An implicit assumption behind the premise that engineered controls are more reliable than administrative controls is that the equipment specified is known to be of appropriately high quality from design, to fabrication, to maintenance. Unfortunately, this quality state cannot be assuredly assumed for many of the SSCs in existing facilities. Their design and fabrication history is not that well documented. Lack of pedigree does not necessarily equate to unreliability but does make for uncertainty. Where such uncertainty exists, more frequent surveillance should be exercised.

In many older enduring facilities, the safety SSCs that are required by the hazard analysis consist of controls that have been in place for many years to mitigate the effects of accidental events should they occur. In general, principally because of budget constraints, little effort is made to identify and implement the engineered controls that would, ideally, prevent an accident. Instead, the existing controls are relied upon, in many cases to mitigate rather than prevent an accident, and additional administrative controls are instituted as compensatory measures.

4.1 IDENTIFICATION OF CONTROLS

During the implementation of ISM at existing facilities,¹ the safety analyst should identify a minimum set of engineered controls (e.g., SSCs) using the results of the hazard analysis, with due consideration of defense-in-depth and the hierarchy of controls. The functional classification of these controls should be determined using the process described in DOE-STD-3009-94 (U.S. Department of Energy, 1994) (or its revision) and its Appendix A. The analyst should address a number of questions in the process of identifying the necessary controls for a specific hazard:

- ! What is the primary control that is relied upon to prevent or mitigate the hazard?
- ! What is the secondary or backup control that is expected to function should the first line of defense fail?
- ! What other controls are provided for defense-in-depth?

¹ This identification of an adequate set of engineered controls may be accomplished as a result of feedback and improvement and implementation of Phase III, continuous assessment and upgrading, as reflected in a letter from Board Chairman Conway to Deputy Secretary of Energy T. J. Glauthier dated March 2, 2000.

- ! Are these controls independent, such that the failure of one would not result in the failure of others?
- ! Would the identified controls accomplish the objectives of the analysis?
 - Are they designed to function in that hazardous environment?
 - Are they designed with the appropriate quality and necessary pedigree?
 - Are their reliabilities commensurate with the hazard?
- ! What kind of evidence or data is available to support the assumptions made in crediting the controls?
- ! Most important, what would be the preferred design feature or SSC to eliminate or prevent the identified hazard (regardless of whether that SSC exists)?

More often than not, the controls identified in the authorization bases of existing facilities are determined on the basis of the availability of such SSCs. Frequently, a set of existing controls is identified and applied to the hazard, without ample consideration for a preferred alternative.

The lack of SSCs needed to control the identified hazards leads to the use of administrative controls to do the job. For example, if the potential for a criticality accident is identified in a tank containing fissile material solution, administrative controls are used that involve sampling and characterizing the solution before it enters the tank. The preferred controls, of course, would be to design the process to eliminate the hazard—in this case, replacing the tank with a geometrically safe tank or using raschig rings. Doing so would require making some modifications to the existing process. Yet while administrative controls may be acceptable for ensuring safe operation, their generally lower reliability, compared with engineered controls, should be evaluated carefully when choosing safety measures for long-term hazardous activities.

As currently implemented at DOE, administrative controls usually fall into two categories. First is the set of requirements, usually contained in contractor programs and policies, that describe the organization and management of an activity or function and the performance of common tasks or functions such as change control or training. Administrative controls in this category are usually described in chapters 6 through 17 of a SAR and can be replaced with the combination of List A and List B requirements of the DEAR clause 48 CFR § 970.5204-78 and the contractor's ISM System description. The second category deals more directly with individual accident scenarios and includes specific requirements for operator action (e.g., responses to alarms) and the establishment of specific conditions not associated with SSCs (e.g., hazardous material inventory controls or fire loading limits). The guidance on identification, analysis, and use of administrative controls in this category is sparse and generally inadequate.

Additional guidance is required to ensure consistent selection and use of specific administrative controls, particularly for determining the effectiveness of an administrative control to reduce the likelihood or consequence of an accident. This guidance must also provide useful information on attributes of administrative controls that can be applied using the graded approach. This latter aspect is particularly important when using administrative controls to compensate for the lack of adequate safety SSCs in an existing facility. In general, even the most robust administrative control (i.e., one that applies all or most of the attributes discussed below) can only be credited with reducing the likelihood of an event by a factor of about 100. It appears as though many DOE BIOs and even SARs assign this reliability a priori to any administrative control proposed. Therefore, in some cases the collection of administrative controls in place do not adequately compensate for the lack of robust safety-class or safety-significant SSCs.

Human actions, taken either in response to an event or taken proactively to establish desired conditions are subject to errors of omission or commission. Sets of administrative controls are prone to common cause failure. Therefore, administrative controls are generally considered less reliable than properly developed engineered controls. However, the following attributes, which can be tailored as appropriate, can increase reliability:

- ! use of reader / worker / checker systems
- ! independent verification
- ! positive feedback systems
- ! human factors analysis
- ! operator training and certification
- ! continuing training and requalifications
- ! abnormal event response drills
- ! ergonomics considerations in procedures

Suggestion: DOE needs to promulgate guidance on the use of specific administrative controls, specifically when used in lieu of safety-class or safety-significant SSCs, including expectations for evaluating their reliability. The guidance should set expectations for the attributes of these administrative controls consistent with the consequences of the accidents they are intended to help prevent or mitigate.

Another situation is created when safety-class or safety-significant SSCs are identified for an existing facility; that is, existing SSCs are selected to perform a safety function even though they were not designed to do so. The implementation guides for DOE Order 420.1, *Facility Safety* (U.S. Department of Energy, 1995), provide

some guidance and recommended design and procurement considerations for such SSCs only for new designs or major modifications to existing facilities. Questions remain, however, as to what safety-class or safety-significant means for existing facilities; what criteria and characteristics these SSCs should meet; and what sort of reliability is expected from these SSCs that have already been designed and installed, probably with no such expectations.

The average life of existing defense nuclear facilities is more than 30 years. The SSCs now identified as safety-class or safety-significant may have been maintained without such designation for decades. Redesignating these SSCs as safety-related in the process of upgrading the safety bases does not inherently improve their reliability. Some incremental improvement may be made in the functionality and reliability of these SSCs by providing predetermined routine surveillance and maintenance, as some contractors have done, but it is not clear where these SSCs would fall on the scale of reliability and functionality on demand as compared with DOE's new expectations (e.g., DOE Order 420.1, [U.S. Department of Energy, 1995]). The Board has recommended that DOE (Recommendation 2000-2, *Configuration Management, Vital Safety Systems* [Defense Nuclear Facilities Safety Board, 2000]) assess the readiness state of vital safety systems and further amplified its expectation in a letter dated September 8, 2000 (Conway to Richardson, 2000).

4.2 FEEDBACK AND IMPROVEMENT

A major element of ISM is feedback of the experience gained during performance of activities into the processes and operations to enhance safety. As work is performed at defense nuclear facilities, lessons are learned that can show line management how safety can be improved. This education, however, is currently limited by the boundaries of the approved authorization bases for the activities or facilities. In other words, it is assumed that the existing controls are adequate and fully capable of mitigating the hazards when an incident occurs or the unexpected comes to pass, even if there may be a better set of controls that, if considered at the time of the hazard analysis, might have prevented the incident from happening.

Feedback and improvement, however, is frequently a reactive process resulting from lessons learned through discovery of deficiencies or failures causing problems or undesirable incidents. Rather than identifying needed improvements after the occurrence of an incident or injury, a proactive process to identify improvements prior to the occurrence of an incident could greatly enhance health and safety, and be cost beneficial as well.

Recently, the Board identified the need for a continuing upgrade program at defense nuclear facilities to improve the quality of the facilities' authorization bases (Letter, Conway to Glauthier, March 2, 2000). Such a program would enable the contractors to proactively identify hazards and potential new controls, or improve the quality of existing controls.

An authorization basis upgrade program should have two distinct elements: (1) better identification of hazards, and (2) better provision of controls to address the identified hazards. The former is discussed in detail in Section 3 of this report. The latter results in two types of controls:

- ! Those that result from upgrading the safety bases. In other words, the new hazard analysis, if implemented properly (using the guidance provided in Section 4.1 of this report), may lead to the identification of controls (e.g., SSCs or design features) that do not currently exist and are necessary to ensure adequate protection of health and safety.
- ! Those that result from designation of existing SSCs as safety-class and safety-significant in the TSRs as a direct result of the application of DOE Order 5480.23 (U.S. Department of Energy, 1992) and its supporting standard to meet the evaluation guidelines and adequately protect workers.

DOE Guide 420.1-1 (U.S. Department of Energy, 1995) provides an approach for the design, procurement, and installation of safety controls identified for new facilities or major modifications to existing facilities. DOE does not currently have any guidance for a systematic approach to reviewing the performance and design adequacy of existing safety controls to ensure adequate protection of the health and safety of workers and the public commensurate with the hazards and remaining life of the facility.

***Suggestion:** Implementation of new systems or modifications to existing SSCs resulting from the safety basis upgrade programs at defense nuclear facilities should not be deterred by the lack of a predetermined process that could facilitate their identification, cost-benefit analysis, design, procurement, review, and approval. What is needed in light of the requirements for safety basis upgrades under way for existing facilities is a directive that would allow for assessment of the design, performance, reliability of existing design features and SSCs identified in the authorization bases as related to meeting the expected evaluation guidelines for the public and ensuring the safety of the workers. Appendix B summarizes a process that might be adopted by DOE or its contractors and applied to existing defense nuclear facilities when the requirements for safety basis upgrade programs are implemented.*

APPENDIX A. TECHNICAL SAFETY REQUIREMENTS

TSRs consist of requirements applicable to active and passive engineered design features, and administrative controls that are identified through safety and hazard analyses to protect the health and safety of the public, and to minimize the potential risk to workers from significant hazards. The information provided in this appendix is not intended to replace requirements in DOE Order 5480.22 (U. S. Department of Energy, 1992) or the format and content guidance in DOE-STD-3011-94 (U.S. Department of Energy, 1994). The DOE guidance was adopted directly from the commercial nuclear industry and was not tailored for defense nuclear facilities. The guidance provided in this appendix clarifies some of the terminology in the DOE guidance; defines associated characteristics; and provides a hierarchy for the TSR elements consistent with the concept presented in DNFSB/TECH-5 (DiNunno, Defense Nuclear Facilities Safety Board, 1995).

A.1 PASSIVE ENGINEERED DESIGN FEATURES

This is the set of safety-related passive design features that, if altered or modified, would have a significant effect on safe operation of the facility or activity. The TSRs should contain the following information on these features:

- ! Safety limits—those characteristics associated with the passive SSCs and design feature whose deviation from a preset value would result in failure and uncontrolled release of hazardous materials.
- ! Limiting Conditions of Operation—associated characteristics or attributes that should not be deviated from during normal operation to ensure functionality upon demand.
- ! Surveillance requirements—the specifications and routine examination of the parameters important to safety to ensure reliability and operability as credited in the analyses.

A.2 ACTIVE ENGINEERED DESIGN FEATURES

This is the set of safety-related systems and components, their support systems, and process parameters required for safe operation of the facility or activity. The TSRs should contain the following requirements applicable to these active controls:

- ! Safety limits—associated with process variables or preventive measures whose deviation from a preset value would potentially result in system failure that could lead to an uncontrolled release of radioactive material.

! Operating limits.

- Limiting Control Settings (LCS)—the settings on preventive measures to ensure that safety limits are not exceeded. LCSs may be the settings for automatic actuation of support systems designed to prevent exceedance of the safety limits. LCSs are set below the safety limits with a margin that consists of a safety margin plus system uncertainty to allow for instrumentation calibration, drift, response time, and accuracy.
- Limiting Conditions of Operation—the lowest functional capabilities for engineered design features or process variables identified in the authorization basis. They should also describe the actions to be taken in case they are exceeded.
- Surveillance requirements—specifications regarding the preventive measures that should be taken to ensure the reliability of the systems and components, as well as methodical and routine examination of important parameters to maintain system operability within the assumed envelope.

A.3 ADMINISTRATIVE CONTROLS

This is the set of requirements applicable to the organization, management, and performance of activities necessary to control significant hazards. Some of these controls may be tailored to the consequences of the hazards. For example, level of training and qualification or frequency of maintenance and surveillance may be determined based on the hazards associated with the activities. Specific operator actions in the procedures can also be determined based on the hazards; specific hazardous activities may require independent operator verification of a particular step in the procedure before the activity can proceed.

The following are the categories of administrative controls, along with examples of what should be included in each category:

! Contractor responsibility and organization

- On-site and off-site organizations
- Lines of authority, responsibility, and communication
- Performance indicators
- Independent review program
- Quality assurance program

- Occurrence reporting system
- ! Operating support
 - Operating support functions, responsibility, training, and qualification
 - Training and placement programs
 - Retraining and replacement programs
- ! Safety programs
 - Prevention
 - Radiological control/protection
 - Waste management
 - Environmental protection
 - Nuclear criticality safety
 - Occupational safety and health
 - Fire protection
 - Industrial hygiene
 - Preservation
 - Conduct of operations
 - Configuration management and change control
 - Document control
 - Maintenance and surveillance
 - Process control and in-service inspection

- Mitigation
 - Emergency management/preparedness

! Integration and management infrastructure

- TSR basis control
- Linking database
- Procedure writing
- Reviews and audits

APPENDIX B. DESIGN AND PERFORMANCE ADEQUACY REVIEW

B.1 INTRODUCTION

Implementation of ISM at defense nuclear facilities should result in a set of contractor manuals and procedures that identify the codes and standards used, or to be used, for design, procurement, and construction of SSCs. These codes and standards are usually categorized based on the SSCs' importance to safety. In other words, there are different sets of requirements for safety-class, safety-significant, and general-purpose SSCs. The codes and standards for new facilities may differ from those used for the design and procurement of the safety SSCs identified in the safety basis of an existing facility. It is suggested that a systematic and methodical evaluation of operational and maintenance history of these SSCs (identified in the safety basis of existing facilities as safety-class or safety-significant) could provide insight into appropriate and reasonable compensatory measures that may include upgrades to the existing SSCs. This evaluation, called *design and performance adequacy review*, might be initiated by various situations or events, such as the following:

- ! An activity-specific hazard analysis may identify a new function for an existing SSC that would eliminate or prevent (preferred mode) the hazard, rather than relying on the existing function to mitigate the consequences.
- ! A set of existing SSCs may be reclassified as safety-class or safety-significant as a result of SAR upgrades even though they were not originally designated as such.
- ! An Unreviewed Safety Question Determination may identify the potential for inadequacy of the existing SSCs to perform their intended safety function.
- ! The commercial or DOE occurrence reporting and processing system may identify situations in which the assumptions or standards applied to the SSCs may lead to potential inadequacy in the SSCs' functional performance.
- ! DOE may require the contractor, through the Authorization Agreement, to comply with certain conditions that may affect the safety SSCs' design or operability.

Design and performance adequacy reviews should follow a graded approach, with the rigor of analysis increasing in accordance with its importance from a safety view point. Significant engineering judgment and managerial expertise are needed to implement the process in a cost-effective manner. The intent is to (1) assess the adequacy of the existing design, (2) identify attributes that may need additional specification (or modification) to ensure the reliability and functionality required, or (3) determine the need for design modifications or replacement of the SSCs in question. At each step in the process, consideration should be given to the estimated risk reduction versus the cost of upgrading or replacement. It is the responsibility of the organization in charge to provide the necessary direction at any given juncture.

B.2 PRINCIPAL ELEMENTS OF DESIGN AND PERFORMANCE ADEQUACY REVIEW

Certain elements are essential to an effective review process. Some of these elements may already exist and may need only to be proceduralized; others are specific to this process and need to be carefully crafted and implemented. The following is a suggested set of major elements of this review process that may be tailored to the needs of a specific site or facility. These elements are consistent with the Board's expectations for implementation of its Recommendation 2000-2.

Identification of Safety Systems. Safety systems may have been identified in a variety of authorization basis documents, as discussed in Section 2. A comprehensive review of these documents should be performed to identify a complete list of the safety systems that have been credited for protection of the public and the workers. It should be noted that not all systems of interest may have been identified in the TSRs as safety systems. For example, a chlorine detection and alarm system may have been identified in the Emergency Hazard Assessment for a waste treatment facility at the site, and may play a vital safety function in protecting workers, but not be identified in the TSRs for the nuclear facilities.

The next step after preparation of the list of safety systems is to make a qualitative assessment of the state of readiness of these systems. As discussed earlier, reliability of these systems to function when needed depends on their operational history and may vary from system to system or facility to facility. The qualitative assessment does not need to be elaborate at this stage of the performance adequacy review, but it will be useful later in the process in determining when more detailed analysis may be needed. The assessment of the state of readiness may be based on some easily identifiable attributes that can be generated from the available information, e.g., the age of the system, whether or not it has been under the control of an effective configuration management and/or surveillance and maintenance program, and data on the most recent occurrence when the system failed to operate or failed a planned test. Such attributes, although not quantitative, would provide a qualitative indication of the operational readiness of the system.

Designation of a Responsible or Cognizant System Engineer. In most operating facilities the facility manager has the overall responsibility for operational readiness of safety systems. The facility manager, in turn, relies on the facility maintenance group to perform the necessary maintenance to ensure that the system is ready when called upon to function if it is in a stand-by mode (e.g., fire sprinkler system), or continue to operate if it is in operational mode (e.g., ventilation system). The functional capabilities and expectations for safety system operation are initially identified by safety analysts and later maintained by authorization basis and engineering or design groups. Configuration control of safety systems is the responsibility of yet a different group, as are its design requirements. There is a need for a System Engineer who is cognizant of the status of the system, knowledgeable of its safety basis and design basis, and responsible for its reliability and performance.

The System Engineers need to meet certain qualification and training requirements to ensure that they have the requisite competence to satisfactorily perform their assigned responsibilities. Important qualification and training topics include the following:

- ! Education in an area pertaining to the designated system. It is important, but not necessary, for the System Engineer to understand the function and design of the safety system by having knowledge or training in a related field. For example, an electrical engineer may know the intricacies of an uninterruptible power supply system, or a mechanical engineer may understand the components of a ventilation system more readily.
- ! Knowledge of the authorization basis, and hazard and accident analyses related to functional requirements of the system. This includes knowledge of the functional classification, operational requirements, design parameters and their bases, and TSR commitments to ensure that the credits taken for the functionality of the system are understood and preserved by the System Engineer.
- ! Knowledge of the applicable codes and standards, industry data on reliability and failure modes of similar components, and best practices for surveillance and maintenance of the system. Membership in the associated technical societies or working groups would facilitate technical exchange and communication of current problems and practices pertinent to safety systems.
- ! Working knowledge of the facility's operation and the activities authorized for the facility. The interaction of different systems in a facility and the hazards they pose may affect the operability of a safety system or its reliability in functioning when needed.
- ! Familiarity with the as-designed/in-situ condition of the safety system. This may be accomplished by identifying the quality assurance and procurement requirements of the system, followed by a system walkdown to confirm its configuration and the condition of its associated components.

The System Engineer should have access to all pertinent documents related to system safety basis, design, operation, maintenance, etc., to enable effective execution of his (her) responsibilities. The System Engineer may also prepare a system description document that contains the information necessary for maintaining its functional capability and reliability as expected according to the authorization basis documents.

DOE, on the other hand, needs to identify the organization or the individual with the expertise necessary to provide oversight of the contractor System Engineer activities that ensure vital safety systems' operational readiness.

Reliability Assessment of Safety Systems. Designation of a System Engineer is necessary for long-term operability and for maintaining the reliability of safety systems. A determination of the

reliability of these systems as they currently exist, however, may require more in-depth knowledge of various aspects of the system. A team of experts may be needed to evaluate a system's ability to perform its intended safety functions. DOE, with cooperation from its contractors and other industry experts, may identify certain common safety systems that are relied upon more widely in the complex (e.g., confinement ventilation, fire protection, electrical power distribution), and designate a focal group or team of experts to perform this evaluation for each such system.

The expert team should be chartered to provide guidelines for systematic and methodical evaluation of the existing safety systems for identification of their operational readiness. The reliability of a safety system depends on several factors that should be considered collectively in this step of the process:

- ! The original design and construction or installation requirements,
- ! The operational record and upkeep,
- ! The historical surveillance and maintenance,
- ! Industry data on system performance and failures, and
- ! The remaining life of the SSC in question; and comparison with the remaining life of the facility.

This information may need to be supplemented with a reliability or failure modes and effects analysis of a system. This effort may substantiate the operability and functional performance of the SSCs in question or the weaknesses of the system and the necessary compensatory measures, including increased maintenance or equipment upgrade to improve them.

The expert team should have capabilities in a variety of related areas so it can provide the necessary guidelines. The team's expertise should include such areas as ISM verification, system design, reliability/safety analysis, equipment operation and performance, equipment maintenance, nuclear explosive safety, fire safety, and human factors.

The evaluation guidelines developed by the expert team should also include assessments of other systems whose operation is essential to support the safety systems (e.g., electrical power, instrumentation and control systems). These assessments should evaluate the general condition of the supporting systems and determine their ability to adequately support the effective operation of the safety system under review. This preliminary review of supporting systems will indicate if they are capable of providing their intended support function under all requisite operating environments.

During the assessment of operational readiness of safety systems at specific sites or facilities, deficiencies could be identified that affect the functional performance expected in the authorization bases. Compensatory measures need to be identified to make up for these deficiencies until the necessary repair or replacements are complete. Care should be exercised to avoid inappropriately prolonged reliance on compensatory measures.

The review teams need to verify that the operational readiness of each safety system is adequate to perform the required function. They may identify alternatives for demonstrating the design and performance adequacy of existing SSCs. These alternatives may include a combination of using the existing SSCs with some design modifications, using the existing SSCs with backup SSCs to provide the same level of reliability for the intended functions, or using the existing SSCs supplemented by additional maintenance and administrative controls to achieve the intended goal. Use of administrative controls to improve the operational readiness of a safety system, however, should be considered only on a temporary basis (as a compensatory measure) and should not be used as a long-term solution.

Cost-Benefit Analysis. A cost-benefit analysis may need to be performed to determine whether an upgrade to the existing SSCs is warranted, alternative SSCs need to be identified, or the specific SSCs needs to be replaced. It is incumbent upon the contractors to recommend the appropriate path forward for DOE, considering several factors:

- ! The program mission associated with the activities performed in the facility,
- ! The remaining life of the facility or the specific SSCs,
- ! The cost of replacement or modifications,
- ! The availability of other alternatives to the SSCs to support the authorization basis of the facility, based on the outcome of the design and performance adequacy review, and
- ! The potential downtime of the facility for the recommended upgrade or replacement versus the potential future facility downtime due to unavailability of the required SSCs to support normal operation (i.e., down time due to lack of TSR compliance).

The contractors are responsible for proposing to DOE the preferred approach to continuing their mission program activities in a manner that protects the health and safety of the public and workers.

Independent Review. A design and performance adequacy review is conducted to support the operability and functionality of SSCs important to safety. As such, any analytical evaluation of the reliability of safety systems needs to have the same quality and appropriate technical justification as other analyses related to preparation of the authorization basis of a facility or activity. Therefore, an independent review of the reliability analysis may be needed.

B.3 OTHER ELEMENTS OF DESIGN AND PERFORMANCE ADEQUACY REVIEW

A design and performance adequacy review may result in modifications to safety SSCs, changes to authorization basis-related documents, or alterations to the facility layout. Special consideration should be given to ensuring that the facility and its authorization basis are consistent with the outcome of the review when it is completed. The following are examples of areas in which such considerations may be warranted:

- ! The authorization basis, and perhaps the Authorization Agreement, of the facility needs to be updated to incorporate any changes resulting from the review process.
- ! The system description documents and their associated records and drawings need to be updated for any changes resulting from the review process.
- ! Any new changes to the safety SSCs need to be incorporated into the facility's configuration management program to prevent future deviations or violations.
- ! Facility personnel may need to be trained for the modifications to the facility, changes to operational or maintenance procedures or the authorization basis to ensure proper conduct of operations and reduce undesired occurrences.

Special consideration should be given to identifying compensatory measures that will ensure safe operation of the facility or activity while the results of the design and performance adequacy review are being implemented. Additional administrative or defense-in-depth controls may be required to compensate for the temporary shortcomings of the existing safety SSCs.

REFERENCES

Bamdad, F., 1998, *Authorization Agreements for Defense Nuclear Facilities and Activities*, DNFSB/TECH-19, Defense Nuclear Facilities Safety Board, Washington, D.C., April.

Code of Federal Regulations (48 CFR), 1999 Edition, Chapter 9, Section 970.5204-78, *Laws, regulations, and DOE directives*, Washington, D.C., October 1.

Conway, J. T., Chairman, Defense Nuclear Facilities Safety Board, 1999, Letter to T. J. Glauthier, Deputy Secretary of Energy, concerning the long-standing safety practice in the design construction and operation of nuclear facilities, Washington, D.C., July 8.

Conway, J. T., Chairman, Defense Nuclear Facilities Safety Board, 1999, Letter to T. J. Glauthier, Deputy Secretary of Energy, concerning a review of the status of safety analyses and safety analysis documentation at Oak Ridge Y-12 Plant during period June 28–July 1, 1999, Washington, D.C., October 6.

Conway, J. T., Chairman, Defense Nuclear Facilities Safety Board, 2000, Letter to T. J. Glauthier, Deputy Secretary of Energy, concerning self-assessment performed by Los Alamos National Laboratory regarding the quality of authorization bases for a number of facilities, Washington, D.C., March 2.

Conway, J. T., Chairman, Defense Nuclear Facilities Safety Board, 2000, Letter to B. Richardson, Secretary of Energy, concerning DOE's request for an additional 45 days to transmit the implementation plan for Recommendation 2000-2, Washington, D.C., September 8.

Defense Nuclear Facilities Safety Board, 1995, Recommendation 95-2: *Integrated Safety Management*, Washington, D.C., October 11.

Defense Nuclear Facilities Safety Board, 2000, Recommendation 2000-2: *Configuration Management, Vital Safety Systems*, Washington, D.C., March 8.

DiNunno, J. J., 1995, *Fundamentals for Understanding Standards-Based Safety Management of Department of Energy Defense Nuclear Facilities*, DNFSB/TECH-5, Defense Nuclear Facilities Safety Board, Washington, D.C., May 31.

Kouts, H. J. C. and DiNunno, J. J., 1995, *Safety Management and Conduct of Operations at the Department of Energy's Defense Nuclear Facilities*, DNFSB/TECH-6, Defense Nuclear Facilities Safety Board, Washington, D.C., October 6.

U.S. Department of Energy, 2000, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1, Facility Safety*, DOE G 420.1-1, Washington, D.C., March 28.

U.S. Department of Energy, 1991, *Unreviewed Safety Questions*, DOE Order 5480.21, Washington, D.C., December 24.

U.S. Department of Energy, 1992, *Technical Safety Requirements*, DOE Order 5480.22, Washington, D.C., February 25.

U.S. Department of Energy, 1992, *Nuclear Safety Analysis Reports*, DOE Order 5480.23, Washington, D.C., April 30.

U.S. Department of Energy, 1995, *Comprehensive Emergency Management System*, DOE Order 151.1, Washington, D.C., September 25.

U.S. Department of Energy, 1995, *Facility Safety*, DOE Order 420.1, Washington, D.C., October 13.

U.S. Department of Energy, 1994, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, DOE-STD-3009-94, Washington, D.C., July.

U.S. Department of Energy, 1994, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans*, DOE-STD-3011-94, Washington, D.C., November.

GLOSSARY OF ACRONYMS

BFO	Basis for Operation
BIO	Basis for Interim Operation
Board	Defense Nuclear Facilities Safety Board
CFR	Code of Federal Regulations
DEAR	Department of Energy Acquisition Regulations
DOE	U.S. Department of Energy
EHA	Emergency Hazard Assessment
ES&H	Environment Safety and Health
FHA	Fire Hazard Analysis
ISM	Integrated Safety Management
LCS	Limiting Control Settings
NPH	Natural Phenomena Hazards
PrHA	Process Hazard Analysis
SAR	Safety Analysis Report
SSC	Structures, Systems, and Components
TSR	Technical Safety Requirements
USQ	Unreviewed Safety Questions