NOT MEASUREMENT SENSITIVE

DOE-STD-3009-2014
November 2014

DOE STANDARD
PREPARATION OF NONREACTOR NUCLEAR FACILITY DOCUMENTED SAFETY ANALYSIS

U.S. Department of Energy **AREA SAFT**
Washington, DC 20585

FOREWORD

1. This Department of Energy (DOE) Standard (STD) has been approved to be used by DOE, including the National Nuclear Security Administration (NNSA), and their contractors.

2. Beneficial comments (recommendations, additions, and deletions), as well as any pertinent data that may be of use in improving this document, should be addressed to:

   Office of Nuclear Safety (AU-30)
   Office of Environment, Health, Safety and Security
   U.S. Department of Energy
   19901 Germantown Road
   Germantown, MD 20874
   Phone: (301) 903-3331
   Facsimile: (301) 903-6172

3. Title 10 of the Code of Federal Regulations (C.F.R.) Part 830, *Nuclear Safety Management*, establishes requirements for the documented safety analyses (DSAs) for nuclear facilities. This Standard provides an acceptable methodology for meeting the 10 C.F.R. Part 830 requirements for the preparation of DSAs for both new and existing nonreactor nuclear facilities.

4. Throughout this Standard, the word "shall" denotes actions that are required to satisfy this Standard. The word "should" is used to indicate recommended practices. The use of "may" with reference to application of a procedure or method indicates that the use of the procedure or method is optional. To use this Standard as an acceptable methodology for meeting 10 C.F.R. Part 830 requirements for preparing DSAs, all applicable "shall" statements need to be met.

5. This Standard is a significant revision of and successor document to DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis.* This revision is intended to clearly identify those portions of the Standard that are required to meet 10 C.F.R. Part 830 requirements if this methodology is used for DSA preparation. This Standard also updates requirements to reflect experience and lessons learned.

6. The goal of this revised Standard is to provide clearer criteria and guidance to support effective and consistent DSAs based upon lessons learned in implementing DOE-STD-3009-94. Individual facilities, sites, and program offices may choose or be directed to apply this revision for upgrading a facility or site DSA, if desired.

7. If a facility, site, or program office chooses to use this DOE-STD-3009 revision for upgrading an existing DSA, then this revision is required by 10 C.F.R. Part 830 to be implemented in its entirety (i.e., all applicable "shall" statements are met) if it is used as the safe harbor. Where DSA upgrades support changes to the identified hazard controls, such changes should be carefully considered to ensure a conservative approach is preserved.

CONTENTS

DEFINITIONS

Note: The origins of the definitions below are indicated by references shown in square brackets. If no reference is listed, the definition originates in this Standard and is unique to its application.

Accident. A specific event or progression of a sequence of events resulting from an initiating event that is followed by any number of subsequent events that may lead to a release of radioactive or other hazardous material and/or exposure to a predefined receptor.

Accident analysis. The process of deriving a set of formalized design/evaluation basis accidents from the hazard evaluation and determining their consequences. Accident analysis results are used to identify the need to designate safety class and safety significant controls.

Administrative controls (ACs). Provisions relating to organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility. [10 C.F.R. § 830.3]

Beyond design/evaluation basis accident (BDBA/BEBA). An accident that exceeds the severity of the design/evaluation basis accident.

Decommissioning. Those actions taking place after deactivation of a nuclear facility to retire it from service, and include surveillance and maintenance, decontamination, and/or dismantlement. [10 C.F.R. Part 830, Appendix A, Table 3]

Decontamination. The removal or reduction of residual radioactive and hazardous materials by mechanical, chemical, or other techniques to achieve a stated objective or end condition. [10 C.F.R. Part 830, Appendix A, Table 3]

Design basis. The set of requirements that bound the design of structures, systems, and components within the facility. Some, but not necessarily all, aspects of the design basis are important to safety.

Design basis accidents (DBAs). Accidents explicitly considered as part of the facility design for a new facility (or major modifications) for the purpose of establishing functional and performance requirements for safety class and/or safety significant controls.

Documented safety analysis (DSA). A documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety. [10 C.F.R. § 830.3]

Evaluation basis accidents (EBAs). When an adequate set of design basis accidents does not exist, the representative and unique accidents evaluated in the accident analysis for the purposes of determining the need for safety class and safety significant controls in an existing facility where design basis accidents were not used for this purpose.

Evaluation guideline (EG). The criterion for the dose of ionizing radiation that the safety analysis evaluates against. The EG is established for the purpose of identifying the need for and evaluating safety class controls.

Facility. A defined assembly of equipment, structures, systems, processes, excavations, or activities that fulfills a specific purpose. Examples include accelerators, storage areas, fusion research devices, nuclear reactors, production or processing plants, radioactive waste disposal systems and burial grounds, environmental restoration activities, testing laboratories, research laboratories, transportation activities and accommodations for analytical examinations of irradiated and non-irradiated components.

Note: For the purpose of implementing this Standard, the definition most often refers to buildings and other structures, their functional systems and equipment, and other fixed systems and equipment installed therein to delineate a facility. "Facility" also encompasses any operations that may be outside of, but associated with, a physical structure. Specific operations and processes independent of buildings or other structures such as waste retrieval and processing, waste burial, remediation, groundwater or soil decontamination and decommissioning are also encompassed by "facility."

Fissionable materials. A nuclide capable of sustaining a neutron-induced chain reaction (e.g., uranium-233, uranium-235, plutonium-238, plutonium-239, plutonium-241, neptunium-237, americium-241, and curium-244). [10 C.F.R. § 830.3]

Graded approach. The process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement in this Standard is commensurate with:

- The relative importance to safety, safeguards, and security;
- The magnitude of any hazards involved;
- The life cycle stage of a facility;
- The programmatic mission of a facility;
- The particular characteristics of a facility;
- The relative importance of radiological and non-radiological hazards; and
- Any other relevant factor. [10 C.F.R. § 830.3]

Hazard. A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to a person or damage to a facility or to the environment (without regard to the likelihood or credibility of accident scenarios or consequence mitigation). [10 C.F.R. § 830.3]

Hazard analysis. The identification of materials, systems, processes, and plant characteristics that can produce undesirable consequences (hazard identification), followed by the assessment of hazardous situations associated with a process or activity (hazard evaluation). Qualitative techniques are usually employed to pinpoint weaknesses in design or operation of the facility that could lead to accidents. The hazard evaluation includes an examination of the complete spectrum of potential accidents that could expose members of the public, onsite workers, facility workers, and the environment to radioactive and other hazardous materials.

Hazard categorization. Evaluation of the consequences of unmitigated radiological releases to categorize facilities in accordance with the requirements of 10 C.F.R. Part 830. Note: 10 C.F.R. Part 830 requires categorization consistent with DOE-STD-1027, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*.

Hazard controls. Measures to eliminate, limit, or mitigate hazards to workers, the public, or environment, including: (1) physical design, structural, and engineering features; (2) safety structures, systems, and components; (3) safety management programs; (4) technical safety requirements; and (5) other controls necessary to provide adequate protection from hazards. [10 C.F.R. § 830.3] Note: "hazard controls" include "specific administrative controls."

Hazard scenario. An event or sequence of events associated with a specific hazard, having the potential to result in undesired consequences identified in the hazard evaluation.

Hazardous material. Any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise could adversely affect the health and safety of the public or the workers or harm the environment.

Initiating event. The first event, such as an earthquake or an electric short, in a sequence of events in an accident or hazard scenario.

Limiting conditions for operation (LCOs). The limits that represent the lowest functional capability or performance level of safety structures, systems, and components required for safe operations. [10 C.F.R. § 830.3]

Limiting control settings (LCSs). Settings on safety systems that control process variables to prevent exceeding a safety limit. [10 C.F.R. § 830.3]

Mitigative control. Any structure, system, component, or administrative control that serves to mitigate the consequences of a release of radioactive or other hazardous materials in a hazard or accident scenario.

Nonreactor nuclear facility. Those facilities, activities, or operations that involve, or will involve, radioactive and/or fissionable materials in such form and quantity that a nuclear or a nuclear explosive hazard potentially exists to workers, the public, or the environment, but does not include accelerators and their operations and does not include activities involving only incidental use and generation of radioactive materials or radiation such as check and calibration sources, use of radioactive sources in research and experimental and analytical laboratory activities, electron microscopes, and X-ray machines. [10 C.F.R. § 830.3]

Nuclear facility. A reactor or a nonreactor nuclear facility where an activity is conducted for or on behalf of DOE and includes any related area, structure, facility, or activity to the extent

necessary to ensure proper implementation of the requirements established by 10 C.F.R. Part 830. [10 C.F.R. § 830.3]

Preventive control. Any structure, system, component, or administrative control that eliminates the hazard; terminates the hazard scenario or accident; or reduces the likelihood of a release of radioactive and/or hazardous materials.

Process safety management (PSM). A process or activity involving the application of management principles as defined in 29 C.F.R. § 1910.119, *Process Safety Management of Highly Hazardous Chemicals*.

Public. All individuals outside the DOE site boundary.

Risk. The quantitative or qualitative expression of possible loss that considers both the likelihood that an event will occur and the consequences of that event.

Safety analysis. A documented process to: (1) provide a systematic identification of both natural and man-made hazards associated with a facility; (2) evaluate normal, abnormal, and accident conditions; (3) derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, and demonstrate their adequacy; and (4) define the characteristics of the safety management programs necessary to ensure the safe operation of the facility.

Safety basis. The documented safety analysis and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely in a manner that adequately protects workers, the public, and the environment. [10 C.F.R. § 830.3]

Safety class structures, systems, and components (SC SSCs). 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 determined from safety analyses. [10 C.F.R. § 830.3]

Safety limits (SLs). Limits on process variables associated with those safety class physical barriers, generally passive, that are necessary for the intended facility function and that are required to guard against the uncontrolled release of radioactive materials.
[10 C.F.R. § 830.3]

Safety management program. A program designed to ensure that a facility is operated in a safe manner that adequately protects workers, the public, and the environment by covering a topic such as quality assurance; maintenance of safety systems; personnel training; conduct of operations; inadvertent criticality protection; emergency preparedness; fire protection; waste management; or radiological protection of workers, the public, and the environment.
[10 C.F.R. § 830.3]

Safety significant structures, systems, and components (SS SSCs). Structures, systems, and components which are not designated as safety class SSCs but whose preventive or mitigative

function is a major contributor to defense-in-depth and/or worker safety as determined from safety analyses. [10 C.F.R. § 830.3]

Safety structures, systems, and components (safety SSCs). Both safety class structures, systems, and components, and safety significant structures, systems, and components. [10 C.F.R. § 830.3]

Site boundary. For the purpose of implementing this Standard, the DOE site boundary is a geographic boundary within which public access is controlled and activities are governed by DOE and its contractors, and not by local authorities. A public road or waterway traversing a DOE site is considered to be within the DOE site boundary if DOE or the site contractor has the capability to control, when necessary, the road or waterway during accident or emergency conditions.

Specific administrative control (SAC). An administrative control that is identified to prevent or mitigate a hazard or accident scenario and has a safety function that would be safety significant or safety class if the function were provided by a structure, system or component. Note: DOE-STD-1186-2004, *Specific Administrative Controls*, or successor document, provides additional information about SACs.

Technical safety requirements. The limits, controls, and related actions that establish the specific parameters and requisite actions for the safe operation of a nuclear facility and include, as appropriate for the work and the hazards identified in the DSA for the facility: safety limits, operating limits, surveillance requirements, administrative and management controls, use and application provisions, and design features, as well as a bases appendix. [10 C.F.R. § 830.3]

ABBREVIATIONS AND ACRONYMS

AC	Administrative Control
AEGL	Acute Exposure Guideline Level
ANS	American Nuclear Society
ANSI	American National Standards Institute
ARF	Airborne Release Fraction
BDBA	Beyond Design Basis Accident
BEBA	Beyond Evaluation Basis Accident
C.F.R.	Code of Federal Regulations
CSP	Criticality Safety Program
DBA	Design Basis Accident
DOE	U.S. Department of Energy
DOE-STD	DOE Standard
DR	Damage Ratio
DSA	Documented Safety Analysis
EBA	Evaluation Basis Accident
EG	Evaluation Guideline
EPA	Environmental Protection Agency
ERPG	Emergency Response Planning Guideline
FMEA	Failure Modes and Effects Analysis
G	Guide
HAZOP	Hazard and Operational Analysis
HC	Hazard Category
HDBK	Handbook
HEPA	High Efficiency Particulate Air
IC	Initial Condition
LCO	Limiting Condition for Operation
LCS	Limiting Control Setting
LPF	Leakpath Factor
MAR	Material at Risk
MOI	Maximally-exposed Offsite Individual
NCS	Nuclear Criticality Safety
NPH	Natural Phenomena Hazards
NRC	Nuclear Regulatory Commission
OSHA	Occupational Safety and Health Administration
PAC	Protective Action Criteria
PDSA	Preliminary Documented Safety Analysis
PRA	Probabilistic Risk Assessment
RF	Respirable Fraction
SAC	Specific Administrative Control
SC	Safety Class
SCAPA	Subcommittee on Consequence Assessment and Protective Action
SL	Safety Limit
SS	Safety Significant
SSC	Structures, Systems, and Components

STD	Standard
TED	Total Effective Dose
TEEL	Temporary Emergency Exposure Limit
TSR	Technical Safety Requirement
TWA	Time-weighted Average

SECTION 1. INTRODUCTION

1.1 PURPOSE

This Department of Energy (DOE) Standard (STD), DOE-STD-3009-2014, describes a method for preparing a Documented Safety Analysis (DSA) that is acceptable to DOE for nonreactor nuclear facilities.

1.2 APPLICABILITY

This Standard applies to nonreactor nuclear facilities as identified in the Code of Federal Regulations (C.F.R.) in 10 C.F.R. Part 830, *Nuclear Safety Management*, Subpart B, *Safety Basis Requirements*, Appendix A, Table 2.

1.3 USE OF THIS DSA PREPARATION METHODOLOGY

Section 830.204(a) of 10 C.F.R. Part 830 requires that "[T]he contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility must obtain approval from DOE for the methodology used to prepare the documented safety analysis for the facility unless the contractor uses a methodology set forth in Table 2 of Appendix A to this Part."

This Standard is an acceptable methodology for meeting the requirements of 10 C.F.R. Part 830 for the preparation of DSAs for both new and existing nonreactor nuclear facilities. Throughout this Standard, the word "shall" denotes actions that are required to satisfy this Standard. The word "should" is used to indicate recommended practices. The use of "may" with reference to application of a procedure or method indicates that the use of the procedure or method is optional. To use this Standard as an acceptable methodology for meeting 10 C.F.R. Part 830 requirements for preparing DSAs, all applicable "shall" statements need to be met.

The goal of this revised Standard is to provide clearer criteria and guidance to support effective and consistent DSAs based upon lessons learned in implementing DOE-STD-3009-94. Individual facilities, sites, and program offices may choose to use this revision to upgrade a facility (or site) DSA if desired. If a Program Office chooses to use this DOE-STD-3009 revision for upgrading an existing DSA, then this revision should be implemented completely. Where DSA upgrades support changes to the identified hazard controls, such changes should be carefully considered to ensure a conservative approach is preserved.

1.4 OVERVIEW OF CHANGES IN THIS REVISION

This revision of and successor document to DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*, is intended to clearly identify those portions of the Standard that are required to meet 10 C.F.R. § 830.204 requirements if this methodology is used for DSA preparation. It also updates requirements to reflect experience and lessons learned. This revision:

- Clarifies use of the Evaluation Guideline;
- Clarifies use of bounding parameters;

- Clarifies unmitigated and mitigated hazard evaluations to protect the workers, public, and environment;
- Clarifies standard industrial hazards and chemical hazards screening or further hazard evaluation;
- Establishes a clear criterion for use of the hierarchy of controls and requires documentation of the rationale;
- Clarifies major contributors to defense-in-depth for selection of safety significant controls;
- Incorporates methodologies for co-located workers and chemical hazard evaluations;
- Refines methods for air dispersion calculations;
- Provides specific criteria for determining the functional adequacy of safety class and safety significant structures, systems, and components; and
- Reduces the level of description required in DSAs for safety management programs.

1.5 OVERVIEW OF THE STANDARD

Section 2 describes the overall DSA preparation process and application of the graded approach.

Section 3 provides detailed criteria and guidance for implementing the fundamental tasks of hazard analysis, accident analysis, and hazard control selection.

Section 4 outlines the products, content, and format of the DSA.

Appendix A provides background on key DSA concepts. Appendix B provides guidance on the development of a DSA for facilities that already have a preliminary documented safety analysis (PDSA) that was developed in accordance with DOE-STD-1189-2008, *Integration of Safety into the Design Process*.

SECTION 2. DSA PREPARATION PROCESS AND THE GRADED APPROACH

2.1 DSA PREPARATION PROCESS

Hazard analysis and accident analysis are performed to identify specific controls and improvements that feed back into overall safety management. Consequence and likelihood estimates obtained from this process also form the bases for selecting the level of detail and control needed in specific safety management programs, using a graded approach. The result is documentation of the safety basis that emphasizes the hazard controls needed to maintain safe operation of a facility.

The level of detail provided in the DSA depends on numerous factors. Applying the guidance for the graded approach in Section 2.2 of this Standard will help the preparer to select an acceptable level of detail.

The foundation for effectively preparing a DSA is the assembly and integration of an experienced preparation team. The size and makeup of the team depend on the magnitude and type of facility hazards and the complexity of the processes that the DSA will address. In determining the makeup of the preparation team, careful consideration should be given to developing an effective hazard analysis, a key activity that takes place early in the process and forms the basis for many subsequent activities.

The safety analysis team should include, at a minimum, individuals experienced in process hazard and accident analyses, facility systems engineers, and process operators. Individuals with experience in specific subjects, such as nuclear criticality, radiological safety, fire safety, chemical safety, or facility operations and process operations, may contribute to the hazard analysis on a regular basis or as needed. Such individuals will typically be needed during development of the programmatic DSA chapter(s) as well. Consistent and accurate exchange of information among the team members is important and can be improved through integration of the required tasks.

The following are the major tasks inherent in the development of the DSA:

- Identify site characteristics;
- Identify facility characteristics and the scope of work performed;
- Identify process and operations characteristics;
- Identify hazards and perform hazard evaluation;
- Perform hazard categorization;
- Perform accident analysis;
- Select hazard controls;
- Describe the hazard controls;
- Derive technical safety requirements (TSRs);
- Summarize criticality safety; and
- Summarize safety management programs.

The organization and content of information to be included from these tasks in the DSA are discussed in Section 4 of this Standard.

2.2 APPLICATION OF THE GRADED APPROACH

Section 830.7 of 10 C.F.R. Part 830 prescribes the use of a graded approach for the effort expended in safety analysis and the level of detail presented in the associated documentation. The graded approach, applied to initial DSA preparation and subsequent updates, is intended to produce an effective and efficient safety analysis and a DSA that is sufficient to assure DOE that a facility has acceptable safety provisions, without providing unnecessary information. As described in 10 C.F.R. § 830.3, the graded approach adjusts the magnitude of the preparation effort to the characteristics of the subject facility based on:

- The relative importance to safety, safeguards, and security;
- The magnitude of any hazard involved;
- The life cycle stage of a facility;
- The programmatic mission of a facility;
- The particular characteristics of a facility;
- The relative importance of radiological and non-radiological hazards; and
- Any other relevant factor (e.g., short operational life).

The DSA is thus developed based on the relationship between the facility and these factors. For example, hazard category (HC) 3 facilities, or facilities that have a short operational life, may require only a limited (but adequate) analysis, with documentation at a level less than that required for a HC-2 facility. In addition, facilities with short operational lives (less than five years) should consider using DOE-STD-3011-2002, *Guidance for Preparation of Basis for Interim Operation (BIO) Documents*, to meet the requirements of 10 C.F.R. Part 830. At the opposite end of the spectrum, a new and complex HC-2 facility with a long operational life will warrant extensive analysis and detailed documentation.

The application of the graded approach may allow for much simpler analysis and documentation for some facilities. However, the DSA is still required to provide a systematic evaluation of hazards and an appropriate set of controls commensurate with the results of the hazard evaluation. For HC-3 facilities with low inventory of radiological and chemical hazards, the DSA should be simple and short. Safety management programs constitute an important means for worker protection for such facilities, with any further controls typically consisting of specific administrative controls (SACs) or safety significant (SS) structures, systems, and components (SSCs). Specific minimum levels of detail for these facilities are given in options #3 and #8 in Table 2 of Appendix A to 10 C.F.R. 830, Subpart B.

At a minimum, the scope of a DSA for a HC-3 facility should address the following three elements in a simplified fashion:

- Basic description of the facility and its operations;
- A qualitative hazard analysis; and
- The hazard controls (including safety SSCs, inventory limits, safety management programs, and their bases).

2.3 QUALITY ASSURANCE REQUIREMENTS

The activities necessary to develop the DSA are required to be performed in accordance with applicable quality assurance requirements, as defined by Subpart A of 10 C.F.R. Part 830, "Quality Assurance," DOE O 414.1D, *Quality Assurance* (or the contractually required DOE O 414.1 revision), and the DOE-approved quality assurance program. These activities include development, review, and approval of engineering calculations and documents, among other quality assurance activities that affect the DSA.

Preparation of the DSA frequently involves use of computer models such as MACCS2, PipeFlo, ALOHA, CFAST, and Hotspot, and engineering calculations performed using utility software such as MS Excel, Mathematica, and MATLAB. Attachment 4 to DOE O 414.1D (or the contractually required DOE O 414.1 revision) requires that computer models and engineering calculation user files be evaluated for meeting the definition of nuclear safety software and an appropriate level of safety software quality assurance controls be applied. DOE has provided pre-approval of some computer codes as compliant with the DOE quality assurance requirements. A listing of these "toolbox codes" can be found on the DOE Safety Software Central Registry.

SECTION 3. HAZARD ANALYSIS, ACCIDENT ANALYSIS, AND HAZARD CONTROL SELECTION

Although all elements of the DSA preparation are important, three elements—hazard analysis, accident analysis, and hazard control selection—are fundamental, because they determine the hazard controls needed to provide protection for workers, the public, and the environment. This section provides detailed criteria and guidance for performing these three elements.

Criteria and guidance for identifying site and facility characteristics, deriving TSRs, summarizing criticality safety and safety management programs to support the development and documentation of the DSA are found in Section 4 of this Standard.

The process described in this Section is consistent with the process identified in DOE-STD-1189-2008 for development of a PDSA.

DOE is developing an Accident Analysis Handbook, which will provide additional information to support the development of the DSA in accordance with the criteria and guidance established in this Standard and examples of good practices in its implementation.

3.1 HAZARD ANALYSIS

"830.202 (b) In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: . . . (2) Identify and analyze the hazards associated with the work;" [10 C.F.R. § 830.202, "Safety Basis"]

"830.204 (b) The documented safety analysis for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility: . . . (2) Provide a systematic identification of both natural and man-made hazards associated with the facility;" [10 C.F.R. § 830.204, "Documented Safety Analysis"]

The initial analytical effort for all facilities is a hazard analysis that systematically identifies and evaluates facility hazards, potential accidents, and controls. The hazard evaluation focuses on evaluating the complete spectrum of hazards and accidents. This largely qualitative effort forms the basis for the entire safety analysis, including the identification of worker safety controls and the subset of accidents to be analyzed.

3.1.1 Hazard Identification

The methodology used for hazard identification shall ensure comprehensive identification of the hazards associated with the full scope of facility processes, associated operations, such as handling of fissionable materials and hazardous waste, and work activities covered by the DSA. The methodology shall include characterization of hazardous materials (radiological and non-radiological) and energy sources, in terms of quantity, form, and location. Commercial industry practices for hazard identification, such as those described in the Center for Chemical Process Safety's *Guidelines for Hazard Evaluation Procedures* may be used.

Bounding inventory values of radiological or hazardous materials shall be used, consistent with the maximum quantities of material that are stored and used in facility processes. Inventory data may be obtained from flowsheets, vessel sizes, contamination analyses, maximum historical inventories, and similar sources. Other possible sources of information supporting hazard identification include fire hazard analyses, health and safety plans, job safety analyses, and occurrence reporting histories.

Although the hazard identification process is comprehensive of all radiological and non-radiological hazards, DSAs are not intended to analyze and provide controls for standard industrial hazards such as burns from hot surfaces, electrocution, and falling objects. These hazards are adequately analyzed and controlled in accordance with 10 C.F.R. Part 851, *Worker Safety and Health Program*, and are analyzed in a DSA only if they can be an accident initiator, a contributor to a significant uncontrolled release of radioactive or other hazardous material (for example, 115-volt wiring as initiator of a fire), or considered a unique worker hazard such as explosive energy. The basis for any identified hazards excluded from further evaluation shall be provided. See Appendix A, Section A.1 of this Standard for further discussion on screening of standard industrial hazards and Section A.2 for a discussion on screening certain chemicals (e.g., low quantities, low hazard).

3.1.2 Hazard Categorization

> *"830.202 (b) In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: . . . (3) Categorize the facility consistent with DOE–STD–1027–92 (''Hazard Categorization and Accident Analysis Techniques for compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports,'' Change Notice 1, September 1997);"* [10 C.F.R. § 830.202, "Safety Basis"]

Hazard identification provides the basis for hazard categorization. The facility hazard category is determined by application of DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, Change Notice 1, September 1997. Where segmentation has been employed, segment boundaries and individual segment classifications should be justified in terms of independence under postulated accident scenarios.

3.1.3 Hazard Evaluation

This section provides general criteria and guidance applicable to the hazard evaluation process and also addresses special cases for evaluation of chemical and criticality hazards.

3.1.3.1 General

The hazard evaluation shall provide (a) an assessment of the facility hazards associated with the full scope of planned operations covered by the DSA and (b) the identification of controls that can prevent or mitigate these hazards or hazardous conditions. The hazard

evaluation shall analyze normal operations (e.g., startup, facility activities, shutdown, and testing and maintenance configurations) as well as abnormal and accident conditions. In addition to the process-related hazards identified during the hazard identification process, the hazard evaluation shall also address natural phenomena and man-made external events that can affect the facility.

A graded approach should be applied to the selection of hazard evaluation techniques. The selection should be based on several factors including the complexity and size of the operation being analyzed, the type of operation, and the inherent nature of hazards being evaluated. For example, a hazard evaluation technique such as "What-If" or "What-If/Checklist Analysis" is appropriate for analyzing many HC-3 facilities, as well as simple HC-2 operations such as waste packaging, storage, or transport. More elaborate methods such as Hazard and Operability (HAZOP) Studies or Failure Modes and Effects Analysis (FMEA) should be used for facilities with higher complexity operations such as chemical processing. In special situations requiring detailed analysis of one or more specific hazardous conditions of concern, higher-level techniques such as Fault Tree Analysis, Event Tree Analysis, and Human Reliability Analysis should be considered. The rationale supporting the selected hazard evaluation technique(s) shall be discussed and justified in the DSA. A discussion of hazard evaluation techniques and recommendations on their selection can be found in Part I of the Center for Chemical Process Safety's *Guidelines for Hazard Evaluation Procedures*.

As part of the hazard evaluation, an unmitigated hazard scenario shall be evaluated for each initiating event by assuming the absence of preventive and mitigative controls. Initial conditions may be necessary to define the unmitigated evaluation; further guidance is provided in Section A.3 of Appendix A of this Standard. The consequences and the likelihood of the unmitigated hazard scenario shall be estimated using qualitative and/or semi-quantitative techniques. Hazard scenario consequence estimates shall address potential effects on facility workers, co-located workers, and the public (maximally-exposed offsite individuals [MOIs]), consistent with the consequence levels described in Table 1 below. Similarly, hazard scenario likelihood shall be estimated consistent with the classification bins in Table 2 below. Additional considerations for unmitigated consequences and likelihoods are provided in Section 3.2.2 of this Standard.

Table 1: Consequence Thresholds

Consequence Level	Public[1,4]	Co-located Worker[2,4]	Facility Worker[3]
High	≥25 rem TED or ≥PAC[5]-2	≥100 rem TED or ≥PAC-3	Prompt death, serious injury, or significant radiological and chemical exposure.
Moderate	≥5 rem TED or ≥PAC-1	≥25 rem TED or ≥PAC-2	No distinguishable threshold
Low	<5 rem TED or <PAC-1	<25 rem TED or <PAC-2	No distinguishable threshold

[1] Maximally-exposed Offsite Individual (MOI) - A hypothetical individual defined to allow dose or dosage comparison with numerical criteria for the public. This individual is an adult typically located at the point of maximum exposure on the DOE site boundary nearest to the facility in question (ground level release), or may be located at some farther distance where an elevated or buoyant radioactive plume is expected to cause the highest exposure (airborne release) – see Section 3.2.4.2. The MOI used here is not the same as the Maximally Exposed Individual or the Representative Person used in DOE Order 458.1 for demonstrating compliance with DOE public dose limits and constraints.

[2] A co-located worker at a distance of 100 meters from a facility (building perimeter) or estimated release point.

[3] A worker within the facility boundary and located less than 100 meters from the release point.

[4] Although quantitative thresholds are provided for the MOI and co-located worker consequences, the consequences may be estimated using qualitative and/or semi-quantitative techniques.

[5] DOE's Protective Action Criteria are defined by Advanced Technologies and Laboratories International, Inc in "Protective Action Criteria (PAC): Chemicals with AEGLs, ERPGs, & TEELs," Rev 27, February 2012. This is available at: http://www.atlintl.com/DOE/teels/teel.html.

Table 2: Qualitative Likelihood Classification

Description	Likelihood Range (/year)	Definition
Anticipated	Likelihood $>10^{-2}$	Events that may occur several times during the lifetime of the facility (incidents that commonly occur).
Unlikely	10^{-2}>likelihood $>10^{-4}$	Events that are not anticipated to occur during the lifetime of the facility. Natural phenomena of this likelihood class include: Uniform Building Code-level earthquake, 100-year flood, maximum wind gust, etc.
Extremely Unlikely	10^{-4}>likelihood $>10^{-6}$	Events that will probably not occur during the lifetime of the facility.
Beyond Extremely Unlikely	Likelihood $<10^{-6}$	All other accidents.

Risk ranking/binning may be used to support the selection of Design Basis Accidents (DBAs)/ Evaluation Basis Accidents (EBAs) and hazard controls (See Appendix A, Section A.4 for information on risk ranking/binning). If risk ranking/binning is used, the consequence and likelihood thresholds in Tables 1 and 2 shall be used.

To ensure an informed and defensible qualitative evaluation, the determination of facility worker consequences should be based on a combination of the following:

- The magnitude, type, and form of radioactive and hazardous materials involved in a hazard scenario;

- The type and magnitude of energy sources involved in a hazard scenario;
- Characteristics of the hazard scenario such as duration and the location where it may occur (e.g., in unmanned areas such as tank vaults); and
- The potential for a hazard to impact workers' mobility or ability to react to hazardous conditions.

The facility worker's mobility or ability to react to hazardous conditions should not be used as the sole or primary basis for determining facility worker impacts. As an example, an assumption that a worker within a building is unaffected by release from a building fire based on hazard recognition and timely evacuation would have to consider the location and characteristics of the fire relative to radioactive or hazardous material that may be affected by the fire (considering quantity, form, and dispersibility).

Facility worker consequences, due solely to a standard industrial hazard, do not need to be categorized in the hazard evaluation if screened out per Section 3.1.1. However, the evaluation of radiological or chemical hazards that result in a prompt death or serious injury should be assigned a high consequence per Table 1. Examples of such hazards might include the generation of flammable/explosive hydrogen gas by electrolysis of uranium in water or a spill of sodium hydroxide used in radioactive waste processing.

The qualitative evaluation for the facility worker may be supported by scoping calculations, engineering judgment, and historical experience. This qualitative approach is used because quantitative estimates are sensitive to a variety of possible assumptions such as facility worker position, circumstance, and proximity to the point of release.

Consequence determinations used for co-located workers in the hazard evaluation shall be supported by an adequate technical basis such as scoping calculations consistent with Section 3.2.4. Alternately, the quantitative evaluation of co-located worker consequences used to compare to Table 1 thresholds may be performed in the accident analysis and reported in the DSA Section [3.4].

Probabilistic calculations are not required to inform likelihood estimates. However, if probabilistic risk assessment (quantitative risk assessment) results are used to assign qualitative likelihood estimates in Table 2, the process for performing these analyses described by DOE-STD-1628-2013, *Development of Probabilistic Risk Assessments for Nuclear Safety Applications*, shall be used. The results of such analyses shall not redefine the criteria described in Tables 1 and 2 above.

Other quantitative calculations may also be appropriate to assign qualitative likelihood estimates in Table 2. For example, DOE-STD-3014-2006, *Accident Analysis for Aircraft Crash into Hazardous Facilities*, provides quantitative guidance for determining the likelihood of an aircraft crash into a nuclear facility. See Section 3.2.2 and Appendix A, Section A.4 for additional guidance for determining accident likelihood.

For hazard evaluation of operational accidents, use of a lower binning likelihood threshold such as 10^{-6}/yr (i.e., beyond extremely unlikely) is not appropriate and should not be used as an

absolute cutoff for dismissing physically possible low probability operational accidents such as "red oil" explosions. This distinction is made to ensure objective evaluation of hazards and identification of available preventive and mitigative controls, whether any controls warrant safety classification, and whether the accident scenario should be considered a candidate for further accident analysis as a design/evaluation basis accident. However, hazard scenarios of operational accidents that are deemed not plausible per the criteria in Section 3.2.1, "Design/Evaluation Basis Accident Selection," may be excluded from the hazard evaluation also.

For each of the unmitigated hazard scenarios, the controls (SSCs, administrative and/or programmatic) that can prevent or mitigate the hazard scenario shall be identified. A mitigated hazard evaluation shall be performed to determine the effectiveness of SS[1] controls (following the preferred hierarchy as described in Section 3.3 of this Standard) by estimating hazard scenario likelihood with preventive controls and consequences with mitigative controls. This evaluation of control effectiveness may be accomplished using one of the following two options:

1. Perform the mitigated analysis and include results for hazard scenarios directly in hazard evaluation tables; or
2. Perform the mitigated analysis and include as a summary evaluation in DSA Section [3.3.2.3].

In either case, the analysis should include SS controls for hazard scenarios having high estimated chemical consequences to the public, or high radiological or chemical consequences to workers (i.e., as defined by Table 1). This information, along with safety functions for these controls, shall be included in the hazard evaluation, unless determined as part of the accident analysis (see Section 3.2). Additional considerations for mitigated hazard evaluation are provided in Section 3.2.3 of this Standard. Hazard control classification is described in Section 3.3 of this Standard.

Public and worker safety issues are the traditional focus of hazard evaluations. However, the DSA hazard evaluation shall also examine the potential for large-scale environmental contamination and identify preventive and mitigative controls to protect the environment. These controls will typically be the same as those necessary to protect the workers and the public. The criteria for safety control selection presented in Section 3.3 are not based on environmental contamination, unless a significant spill to the environment outside the facility can contribute to radiological exposures as discussed in Section 3.2.4.2.

[1] Since unmitigated high or moderate radiological consequences to the public could challenge the Evaluation Guideline and are required by Section 3.2 to be evaluated as Design Basis Accidents, or as representative or unique Evaluation Basis Accidents, a mitigated analysis for the public is optional for the DSA hazard evaluation.

3.1.3.2 Criticality Hazards

An inadvertent criticality accident represents a special case for hazard evaluation. The criticality safety program requirements[2] are derived from the hazard analysis process established in the American National Standards Institute/American Nuclear Society (ANSI/ANS)-8 series of national standards, which require a documented criticality safety evaluation demonstrating that operations with fissionable material remain subcritical under both normal and credible abnormal conditions (see Appendix A, Section A.5 of this Standard for details). In addition, the DSA hazard evaluation shall include:

- Events where consequences (from the criticality itself or subsequent impact to hazardous material) exceed the high radiological consequence thresholds for either the co-located workers or the MOI in Table 1, unless it has been determined that an unmitigated criticality accident is not credible; and
- Situations where an active engineered control(s) is required by the Nuclear Criticality Safety (NCS) analysis to ensure subcriticality.

If the NCS program requires a criticality accident alarm system, then the criticality accident alarm system shall be discussed in the hazard evaluation and carried forward to evaluation in accordance with Section 3.3 of this Standard.

In addition, Chapter 6 of the DSA will provide a general discussion of criticality control strategies and of the parameters used for the prevention of inadvertent criticality.

3.1.3.3 Chemical Hazards

Chemical hazards are screened for evaluation by applying the criteria in Section A.2 of this Standard. Chemicals that are screened out in this manner still need to be considered for their possible impact on radiological or other chemical accident initiation or progression, or potential adverse impact on safety systems. Chemical properties such as reactivity, toxicity, and incompatibility with other chemicals should be included in the hazard evaluation.

Qualitative evaluation of chemical consequences is generally sufficient to provide a basis for comparison to Table 1 thresholds. However, quantitative analysis should be performed to determine impacts to co-located workers and the public when the chemical hazards have the potential to exceed the Section 3.3.2 SS control selection criteria, based on the guidance in Section 3.2.4.3. Determination of chemical quantities sufficient to challenge the criteria may be supported by scoping calculations using the methods presented in Section 3.2.4.3 or by engineering judgment based on previous safety basis calculations, emergency planning calculations, or consensus standards.

[2] Criticality safety program requirements are established in DOE O 420.1C. This Order states that DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Non-Reactor Nuclear Facilities*, is the required method for performing criticality safety evaluations, unless DOE approves an alternate method.

3.2 ACCIDENT ANALYSIS

"830.204 (b) The documented safety analysis for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility: . . . (3) Evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility;" [10 C.F.R. § 830.204, "Documented Safety Analysis"]

Accident analysis entails the formal characterization of a limited subset of accidents, referred to as DBAs/EBAs,[3] and the determination of consequences and hazard controls associated with these events. For the purpose of identifying safety class (SC) SSCs, estimated consequences to the MOI are compared to the evaluation guideline (EG) discussed further in Section 3.3.1 of this Standard. Accident analysis is not necessary for facilities with unmitigated offsite consequences that do not have the potential to challenge the EG. Scoping calculations performed during hazard evaluation may be used to show that accident analysis is not needed.

For the purpose of identifying SS SSCs, an evaluation of co-located worker consequences and offsite chemical consequences is also required and is performed as part of either: (1) the hazard evaluation as described in Sections 3.1.3.1 and 3.1.3.3 of this Standard or (2) the accident analysis addressed in this section. The need for SS controls to protect the facility worker is determined by the qualitative hazard evaluation discussed in Section 3.1.3 of this Standard.

The effectiveness of SC and SS controls is determined by performing a mitigated analysis (see Section 3.2.3). The assumptions and process for calculating mitigated and unmitigated dose are described in the following sections.

3.2.1 Design/Evaluation Basis Accident Selection

Accidents to be analyzed in a DSA are termed "design basis accidents" when they are or were defined as part of the facility design for a new facility (or major modifications). DOE-STD-1189-2008 provides guidance for selecting and analyzing facility-level radiological and/or hazardous material release events in the DBAs. When an adequate set of DBAs does not exist, EBAs are selected from:

- Operational accidents – process deviations (e.g., high temperature and high pressure) and initiating events internal to the facility (e.g., fire, explosions, loss of power);
- Natural events such as earthquakes, floods, tornadoes, and wildfires; and
- Man-made external events such as an aircraft crash, vehicular accident, or gas pipe break.

EBAs are derived from the spectrum of hazard scenarios developed in the hazard evaluation. Two types of EBAs shall be defined for further analysis: representative and unique. EBAs may

[3] Appendix A, Section A.6 discusses the concept of EBAs.

also be developed for determining the need for SS controls based on co-located worker consequences or chemical consequences to the MOI, if such consequences are not quantitatively evaluated in the hazard evaluation.

Representative EBAs bound a number of accidents with a similar control set (e.g., the worst fire, for a number of similar fires). At least one bounding accident from each of the major types determined from the hazard evaluation that have the potential to challenge the EG (fire, explosion, spill, etc.) shall be selected. Other accident types involving the co-located worker or toxic exposures may also be presented in the accident analysis, unless the hazard evaluation concludes that the public and co-located worker radiological or toxicological consequences for a major accident type are "low" in accordance with Table 1. In the context of representative accidents, the word "bounding" is intended to refer to the accident with the highest consequences among a group of similar accidents.

Representative EBAs shall be defined such that:

- The control(s) applicable to the EBA are similar and will perform the same function as the controls of the represented hazard scenarios; and
- The accident environment associated with the EBA envelopes the environment expected from the represented hazard scenarios.

Unique EBAs are those events that may be bounded by other events, but have their own unique control set or other hazard/accident characteristics. For example, assume that four different explosions with potentially high consequences can occur in a facility. Three explosions are functionally identical and have the same control set. The fourth explosion, though slightly smaller in consequence, is unrelated to the other three and has its own unique control set. For accident analysis, it is acceptable to select the bounding representative EBA for the three related scenarios. Failure to analyze the fourth explosion case separately, however, could result in overlooking necessary preventive or mitigative controls. The fourth explosion is, therefore, a unique EBA that should also be selected for accident analysis.

Natural phenomena hazard (NPH) EBAs are those required for existing nuclear facilities by DOE O 420.1C (or applicable successor documents) and its associated NPH implementation standards. The likelihood of the initiating event is the NPH return period of the appropriate HC-1, HC-2, or HC-3 nuclear facility, which is the inverse of the annual probability of exceedance, as adjusted for existing facilities per the guidance from DOE-STD-1020-2012, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities*. Potential NPH impacts that should be considered include the cumulative effects of releases from NPH-induced structural and equipment failures (e.g., impacts, spills, fires, explosions).

Hazard scenarios that have the potential to challenge the EG shall be considered as candidates for DBA/EBA accident analysis except for: (1) operational events that are deemed not plausible as described below; (2) natural phenomena initiators of greater magnitude than those required by DOE O 420.1C (or applicable successor documents); or (3) external man-made accidents with a cutoff likelihood of 10^{-6}/yr, conservatively calculated.

An operational event is not considered plausible if it is either:

- A process deviation that consists of a sequence of many unlikely human actions or errors for which there is no reason or motive. In evaluating this criterion, a wide range of possible motives, short of intent to cause harm, should be considered. Necessarily, no such sequence of events may ever have actually happened in any nonreactor nuclear facility; or
- A process deviation for which there is a convincing argument, given physical laws, that they are not possible. The criterion cannot be used if the argument depends on any feature of the design or materials controlled by the facility's safety features or administrative controls (ACs).

The above two criteria are not based on quantitative factors.

Use of a lower binning likelihood threshold such as 10^{-6}/yr (i.e., beyond extremely unlikely) for screening operational events from selection as DBA/EBAs for the accident analysis, is not appropriate. However, in those situations when it is too costly to implement or impractical to identify SC controls in accordance with the requirements of this Standard, a quantitative analysis that is completed in accordance with DOE-STD-1628-2013, including the development of a probabilistic risk assessment (PRA) plan (approved by DOE), may be used to support decisions regarding the need for SC or SS controls for operational events. In such cases, PRA results shall include an integrated assessment of accident probability and consequences of the accident event to establish the event's risk significance. When PRA results are used, key assumptions and initial conditions shall be identified and protected (see Section 3.2.2 of this Standard).

As stated in Section 3.1.3.1 of this Standard, accident likelihoods are qualitatively assigned in the hazard evaluation for the mitigated and unmitigated analyses, and detailed probabilistic calculations are neither expected nor required. That subsection also states that other quantitative likelihood calculations may be appropriate to inform the hazard evaluation, which is also appropriate for the DBA/EBA accident analysis. For example, DOE-STD-3014-2006, *Accident Analysis for Aircraft Crash into Hazardous Facilities*, provides quantitative guidance for determining the likelihood of an aircraft crash into a nuclear facility.

When quantitative estimates are used, accident likelihood calculations are needed to provide supporting information for the analytical and decision-making processes. Guidance for likelihood calculation for the unmitigated hazard or accident analysis is provided in Section 3.2.2, and in Section 3.2.3 for the mitigated analysis.

3.2.2 Unmitigated Analysis

Both the hazard evaluation and the accident analysis require an unmitigated analysis of the consequences and likelihood of accidents (note: the term "accident" as used in this subsection also includes "hazard scenarios"). An unmitigated consequence analysis shall be performed for plausible accident scenarios, NPH events, and external events. The hazard evaluation also presents the unmitigated dose consequence from a criticality accident as required by Section 3.1.3.2. The material quantity, form, location, dispersibility, and interaction with available energy sources are identified and documented. The intent is to provide a conservative estimate

of the consequences to the facility worker, co-located worker, and MOI assuming that mitigative controls do not perform their safety functions. This estimate may be done either qualitatively in the hazard evaluation or quantitatively (for DBAs/EBAs) using the methodology prescribed in Section 3.2.4 of this Standard.

The initial conditions and assumptions for the analysis shall be documented and evaluated to determine if controls are needed to maintain the validity of the evaluation. If the presence of an assumed passive SSC prevents significant consequences, it shall be classified as either SS or SC. Section A.3 in Appendix A of this Standard discusses initial conditions further.

The unmitigated source term should characterize both the release fractions and the energies driving the release in accordance with the physical realities of the accident phenomena at a given facility, activity, or operation. As a result, some additional assumptions may be necessary in order to define a meaningful accident scenario, and such assumptions may also affect the magnitude of the resultant consequences. An assumption that an SSC exists does not automatically require SC or SS designation. However, assumptions shall be protected at a level commensurate with their importance. For example, if a passive barrier is assumed to survive a fire that would otherwise lead to a significant consequence, then the barrier's configuration would need to be protected as a TSR design feature.

The following assumptions may be appropriate to establish a physically meaningful accident scenario:

- Passive safety controls not affected by the accident scenario are deemed available. This assumption is valid for facility-wide, secondary, and common cause events that are directly caused by natural events, such as earthquake-induced fires and explosions. For example, in the case of a process vessel rupture, it should be assumed that other vessels shown not to be affected by the accident are not ruptured or otherwise unavailable; and
- Passive safety controls affected by the accident scenario are deemed available based on an assessment that they will survive accident conditions. For example, in the case of a container drop in which the impact of the drop is shown not to challenge container integrity, it should be assumed that the contents of the container are not released. Similarly, if the facility has permanently-installed resilient flooring that prevents an undesired consequence of such a drop, an assessment of the drop against an unyielding surface is not meaningful.

Such defining assumptions may need to be protected by means of designating certain SSCs as SS or SC. In the above examples, the container and the flooring may warrant designation as SS or SC design features, depending upon whether the container design and construction are critical to the validity of the assumption and consequences of the design feature not performing as assumed.

The following conditions shall not be assumed to be available for unmitigated analysis of plausible accident scenarios defined in Section 3.2.1:

- Active safety controls, such as ventilation filtration systems in the case of a spill or fire suppression in the case of a fire;
- Passive safety controls that produce a leakpath reduction in source term, such as building filtration;
- Operator intervention actions that may abort the progression of the event; that is, assume the event occurs with no operator intervention; and
- ACs or safety management programs in the unmitigated analysis. For example, combustible controls may not be used as an initial condition to show that a full facility fire is not plausible. Material at risk (MAR) values, and other process physical attributes such as waste acceptance criteria on radiological or fissile concentrations that establish inventory limits, are considered an exception to not crediting ACs for the unmitigated analysis, because they are considered initial conditions if addressed by a SAC (see Appendix A, Section A.3). MAR limits are a special case and have historically been allowed for the unmitigated analysis since these limits define the initial conditions for the hazard evaluation and accident analysis. Examples include limiting the inventory in a HC-3 facility or limiting the inventory to low-level waste based on Waste Acceptance Criteria that prohibits transuranic wastes or higher fissile concentrations. Other ACs, such as combustible controls, that are elevated to a SAC as an initial condition for the unmitigated analysis would circumvent the control selection process considering the hierarchy of preferences, and place greater reliance on ACs over available engineered controls.

The unmitigated consequence calculation determines the need for safety-designated controls and provides the framework for designating these controls. If the unmitigated consequences of a release scenario exceed established chemical or radiological thresholds in Sections 3.3.1 and 3.3.2, SC and/or SS controls will need to be established. If it is clear from this analysis that the unmitigated consequences will far exceed the EG, the actual consequences need not be determined[4] because the need for SC controls has already been identified. However, the mitigated consequences will be calculated in accordance with Section 3.2.3 if the application of preventive controls does not eliminate the hazard or terminate the accident scenario and prevent a release of radioactive or other hazardous materials.

The following guidance should be used to support a determination of the accident likelihood as required in the unmitigated analysis of plausible accident scenarios defined in Section 3.2.1:[5]

- The likelihood of an unmitigated accident is generally the likelihood of the initiating event. The unmitigated likelihood estimate does not include subsequent enabling events that represent the failure probability of preventive controls, that is, the unmitigated likelihood estimate assumes that preventive controls do not provide their safety functions.

[4] A determination of the magnitude of the consequences relative to the EG may be necessary in order to implement NPH design requirements (see DOE-STD-1020-2012).
[5] When likelihoods are determined by a PRA, this unmitigated guidance does not apply.

As an example, if a vehicle crash associated with facility operations is anticipated, the vehicle crash and subsequent fire may be justified as unlikely based on highway transportation accident rates. Likelihood estimates do not consider the probability that an individual will be under the plume centerline and remain there for the assumed duration of time. Dispersion analysis assumptions are addressed in Section 3.2.4.2 of this Standard.

- If an accident is caused by failures associated with human errors, the unmitigated likelihood generally should be assumed to be anticipated unless a rationale for supporting a lower estimate is provided (for example, the accident requires multiple independent errors of commission or omission or the activity in which the error occurs is rarely performed).
- Likelihood estimates for NPH events generally have a lower initiating event likelihood and are based on design and evaluation criteria provided in DOE's NPH design requirements such as DOE O 420.1C and DOE-STD-1020-2012. This unmitigated estimate should not consider the likelihood that the NPH events will lead to fires or explosions. For example, the likelihood of fire caused by an earthquake would be set equal to the likelihood of the initiating NPH event.

3.2.3 Mitigated Analysis

A mitigated analysis shall be performed to determine the effectiveness of SS and SC controls to protect co-located workers and the public. This analysis should be the same as the unmitigated analysis except that accident (note: the term "accident" as used in this subsection also includes "hazard scenarios") likelihood is estimated with preventive controls available, and consequences are estimated with mitigative controls available.

Where preventive controls are credited as SS or SC, the DSA shall evaluate the effectiveness of the controls to either eliminate the hazard or terminate the accident and prevent a release of radioactive or other hazardous materials. If hazard elimination or accident termination cannot be accomplished, the effectiveness of the credited controls is evaluated in terms of the overall reduction in the likelihood of the accident. Examples of how to determine effectiveness of preventive controls are provided in Appendix A, Section A.4. For each initiating event, the likelihood estimate of the initiating event (from the unmitigated analysis) is combined with estimates of probabilities of subsequent events such as failure of preventive controls that have to occur to result in harm to workers or the public.

A mitigated consequence analysis is required if the credited preventive controls do not eliminate the hazard or terminate the accident. This analysis shall demonstrate how SC mitigative SSCs and/or SACs reduce consequences below the EG and how SC (if identified) and SS mitigative SSCs and/or SACs reduce co-located worker consequences below 100 rem. Further, it is DOE's goal that the combined effectiveness of the suite of credited controls (SC and SS) for a given accident is such that the event is either prevented or mitigated to reduce offsite doses well below the EG.[6]

[6] This goal is not associated with a particular value, and therefore is not an explicit requirement.

The results of the mitigative analysis are then presented in Sections [3.4.3.X.5] or [3.3.2.3] of a DSA where the effect of hazard controls is shown.

3.2.4 Consequence Calculation

Accident consequence quantification starts with formal descriptions of the accident scenarios. Basic event trees may support such descriptions. The next step is the determination of accident source terms, which are obtained through phenomenological and system response calculations. Once a source term has been determined, consequences are calculated. As with every phase of the analysis, the effort expended is a function of the estimated consequence.

Calculations shall be made based on technically-justified input parameters and underlying assumptions such that the overall consequence calculation is conservative. Conservatism is assured by the selection of bounding accident scenarios, the use of a conservative analysis methodology, and the selection of source term and input parameters that are consistent with that methodology.

For some input parameters, this section identifies default or bounding values that may be used without further justification. Unless otherwise stated for a particular input value, this section allows use of alternative values when supported by an adequate technical basis. When an input parameter used is not a default or bounding value, an acceptable technical basis of the value describes why the value selected is appropriate for the physical situation being analyzed, and references relevant data, analysis, or technical standards. The completeness and level of detail in the technical basis should increase as the parameters depart from default or bounding values. DOE is developing an Accident Analysis Handbook which will provide additional discussion on conservative consequence calculations.

The accident analysis relies upon well-founded assumptions that are protected at a level commensurate with their importance. TSRs are used to protect the validity of significant assumptions. The two main steps in the accident dose calculation are: (1) the determination of the *source term*, which is the amount of respirable radioactive or other hazardous material that is released as a result of the postulated accident scenario, and (2) the *radiological dose calculation*, which is a function of the location and exposure time of the receptor, dispersion of the material to the receptor location, radiotoxicity of the material as characterized by dose coefficients, or toxicity of other hazardous materials whose consequences are calculated in terms of exposure concentrations. These steps are described in the next three subsections.

3.2.4.1 Radiological Source Term

The radioactive airborne source term is typically calculated as the product of five factors: (1) the MAR; (2) the damage ratio (DR); (3) the airborne release fraction (ARF); (4) the respirable fraction (RF); and (5) the leakpath factor (LPF). ARF and RF are commonly presented as a single value and therefore are discussed together below. The source term parameters are discussed in detail in DOE-HDBK-3010-94, *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities.*

Material at Risk

The MAR is the bounding quantity of radioactive material that is available to be acted upon by a given physical stress from a postulated accident. The MAR may be the total inventory in a facility or a portion of this inventory in one location or operation, depending on the event. MAR values used in hazard and accident analysis shall be consistent with the values noted in hazard identification/evaluation, and shall be bounding with respect to each accident being evaluated.[7] While DOE-STD-1027-92 excludes material in Department of Transportation Type B containers from consideration for the purposes of hazard categorization, the existence of such material shall be acknowledged in the DSA and the material excluded from the source term for a particular accident scenario only if the containers can be shown to perform their safety functions under accident conditions.

Damage Ratio

The DR is the fraction of material that is actually affected by the accident-generating conditions. DOE-HDBK-3010 notes that some degree of ambiguity can result from overlapping definitions of MAR and DR. A given DSA should use one consistent definition throughout. A DR of 1.0 shall be used unless there is an applicable standard or technical basis for a different value. For example, DOE-STD-5506-2007 contains specific DRs (and associated MAR guidance) that may be used in transuranic waste operations.

Airborne Release Fraction and Respirable Fraction

The ARF is the coefficient used to estimate the amount of a radioactive material that can be suspended in air and made available for airborne transport under a specific set of induced physical stresses. The RF is the fraction of airborne radionuclide particles that can be transported through air and inhaled into the human respiratory system. The RF is commonly assumed to include particles of 10-μm Aerodynamic Equivalent Diameter and less. Bounding estimates, and in many cases median estimates, for radionuclide ARFs and RFs for a wide variety of MAR and release phenomena are presented in DOE-HDBK-3010. The bounding estimates shall be used unless a different value is provided in an applicable standard or is otherwise technically justified. In cases where direct shine may contribute significantly to dose, that contribution should be evaluated without the use of the RF, and without the use of the ARF if due to a spill release resulting in exposure to a pool. ARFs and RFs are selected based on physical conditions and stresses anticipated during accidents. DOE-HDBK-3010 defines bounding ARFs and RF mechanisms and airborne release rates based on physical context.

Leakpath Factor

The LPF is the fraction of material that passes through some confinement deposition or filtration mechanism. Several leakpaths may be associated with a specific accident, such as the fraction

[7] For facilities that provide retrieval, handling, storage or processing of transuranic waste containers, a bounding MAR may be determined in accordance with DOE-STD-5506-2007, *Preparation of Safety Basis Documents for Transuranic (TRU) Waste Facilities*.

passing from a glovebox, the fraction passing from a room, or the fraction passing through a leaking door. The LPF used in the common five-factor formula is the total fraction of respirable airborne material released during the accident that escapes from the building to the environment. For purposes of the unmitigated release calculation, the LPF shall be set to unity. For mitigated analysis, analytical tools used in calculating the LPF shall be appropriate to the physical conditions being modeled, including the use of input parameters, such that the overall LPF would be conservative.

3.2.4.2 Radiological Dose Consequence

Radiological consequences are presented as a Total Effective Dose (TED) based on integrated committed dose to all target organs, accounting for direct exposures as well as a 50-yr commitment. The dose pathways to be considered are inhalation, direct shine, and ground shine. Direct shine and ground shine from gamma emitters only need to be evaluated if they cause an upward change in the consequence level as defined in Table 1. Slowly-developing dose pathways, such as ingestion of contaminated food, water supply contamination, or particle resuspension, are not included. However, quick-release accidents involving other pathways, such as a major tank rupture that could release large amounts of radioactive liquids to water pathways, should be considered. In this case, potential uptake locations should be the evaluation points for radiological dose consequences.

In most cases, the airborne pathway is of primary interest for nonreactor nuclear facilities. This position is supported by NUREG-1140, *A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees*, which states that "for all materials of greatest interest for fuel cycle and other radioactive material licenses, the dose from the inhalation pathway will dominate the (overall) dose." For some types of facilities such as liquid processing with the potential for significant spills to the environment outside the facility, the surface and groundwater pathways may be more important, and accident releases usually would be expected to develop more slowly than airborne releases. More time would also be available for implementing preventive and mitigative measures.

The relevant factors for dose estimation are receptor location, atmospheric dispersion, and dose coefficients. Specific guidance or criteria for each is provided below.

<u>Atmospheric Dispersion</u>

This Standard defines the general methodology and parameters that may be used in the dispersion analysis. Criteria and guidance for collecting meteorological data and applying dispersion models are intended to yield conservative estimates of the potential impact of a release of radioactive material. These estimates, in turn, are used to select safety controls. Site or facility specific factors may be considered in choosing a dispersion model and the parameters to be used in that model.

One of the following options, as described in this subsection, shall be used to evaluate atmospheric dispersion and the resulting χ/Q:

- Option 1: Follow a process based on Nuclear Regulatory Commission (NRC) Regulatory Guide 1.145, *Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants;*[8]
- Option 2: Use a DOE-approved toolbox code and apply the conservative parameters as discussed below; or
- Option 3: Use site-specific methods and parameters as defined in a site/facility specific DOE-approved modeling protocol.

Meteorological Data

For the calculation of offsite doses, five years of representative, recent meteorological data shall be used as input to the dispersion model. If five years of data are not available, justification for using a smaller data set shall be provided in the DSA. If representative meteorological data is not available, Pasquill stability class F and one meter/second wind speeds may be used for radiological dispersion consistent with NRC's and DOE's long-standing practice.

In the case of Option 1, follow the meteorological data guidance within NRC's Regulatory Guide 1.23, *Meteorological Monitoring Programs for Nuclear Power Plants*. For Options 2 and 3, the guidance in both Reg Guide 1.23 and in Environmental Protection Agency (EPA)-454/R-99-005, *Meteorological Monitoring Guidance for Regulatory Modeling Applications,* are acceptable means of generating the meteorological data upon which dispersion is based. These two guidance documents should be evaluated for their applicability to the site or facility being evaluated. In the development of the meteorological database for Option 3, the impact of local surface roughness on the data may be considered.

For accident phenomena defined by weather extremes (such as tornadoes or high straight-line winds), actual meteorological conditions associated with the phenomena may be used for comparison of the dose from immediate releases to the EG for SC control selection, and for comparison to the co-located worker SS control selection criteria. For releases associated with weather extremes, the event could be followed by a rapid return to less dispersive conditions.

Receptor Location

For the purposes of comparison to the EG, the comparison point shall be the location of a hypothetical MOI. This MOI is typically located either at the shortest distance to the DOE site boundary (directionally independent), or at the site boundary location with the highest directionally-dependent dose based on a ground level release. The directionally-dependent MOI is to be calculated in a manner consistent with the procedure outlined in Regulatory Position 1.2 of Reg Guide 1.145. The directional dependence of the distance for the receptors may be calculated for 16 compass directions (22.5-degree sectors centered on true north, northeast, etc.). For each of the 16 sectors, the distance to the receptor at the site boundary corresponds to the

[8] Referred to hereafter as Reg Guide 1.145.

minimum distance to the site boundary within a 45-degree sector centered on the compass direction of interest.

In the case of an elevated or buoyant release, the MOI could be beyond the DOE site boundary. In such cases, the MOI is evaluated where the ground level consequence is maximized. The presence of complex terrain should be evaluated during the analysis of elevated or buoyant releases and the model choices should reflect the existence of complex terrain.

Release and Exposure Durations

For Option 1, the release and exposure durations should reflect Regulatory Position 1.3 in Reg Guide 1.145. For other options, the dose estimate, unless otherwise established, is calculated based on an exposure duration of two hours. This nominal exposure time may be extended to a period not to exceed eight hours for scenarios that are slow to develop, as defined by the source term release rate (e.g., evaporation from a pool). Similarly, the nominal exposure time may also be shortened to a period no less than three minutes (e.g., explosions and small fires). The exposure period begins when the plume reaches the MOI. Exposure is defined in terms of plume passage at receptor location. The accident progression should not be defined using only input variables that maximize dispersion and minimize exposure and should ensure internal consistency between the accident release, exposure duration, and factors such as plume meander. It is not acceptable to use a release rate that is specifically intended to expose the MOI to only a small fraction of the total material released, to define the time and wind speed so that the plume does not reach the MOI, or to enhance meander factors beyond what the release characteristics would warrant.

Determination of the Offsite χ/Q

The parameter χ/Q represents the dilution of the radioactive plume via dispersion and deposition as it travels from the facility during an accident. Appropriate χ/Q values at the MOI shall be determined using a method consistent with application of Reg Guide 1.145, using either the directionally independent or directionally dependent method. For directionally independent assessments, this calculation represents the 95^{th} percentile, as described in Reg Guide 1.145, Section C.3, Regulatory Position 3, *Determination of 5 Percent Overall Site χ/Q Value*. For directionally-dependent calculations this calculation represents the 99.5^{th} percentile, as described in Reg Guide 1.145, Section C.2, Regulatory Position 2, *Determination of the Maximum Sector Values*. While the three options allow for alternative methods to calculate the χ/Q values, all three options shall evaluate the dose at the MOI using either a 95^{th} percentile for a directionally independent method or a 99.5^{th} percentile for a directionally dependent method. When multiple years of meteorological data are used, the appropriate percentile χ/Q is calculated for each year, and the mean value of the result used to determine the maximum impact.

The use of this guidance is consistent with consensus standards for dispersion modeling, which incorporate appropriate conservatism in the parameters with the use of unfavorable meteorological conditions. The use of unfavorable meteorological conditions represents actual conditions that can be expected to occur in a given year, not a statistical distribution around an expected mean value.

In the case of Option 1, Reg Guide 1.145 allows for the application of a plume meander that incorporates the effects of light winds and buildings. Additional guidance on the applicability of the plume meander factors, which were developed using the dispersion coefficients included in Reg Guide 1.145, is provided in NUREG/CR-2260, *Technical Basis for Regulatory Guide 1.145.* Dispersion coefficients used within Option 1 should be consistent with those provided by Reg Guide 1.145. Appropriate parameters will not automatically represent maximally bounding values.

Regarding Option 2, DOE-approved, code-specific guidance for each toolbox code should be consulted. This is especially true with respect to developing χ/Q values using dispersion models. Many of these toolbox codes allow for setting a specific parameter within the calculations. These parameter choices may either use the conservative parameters and options established in this section (Option 2) or reflect site-specific conditions to more accurately represent the accident scenario (Option 3). The parameter choices presented for use in Option 2 are given to provide a simple method for determining an appropriate χ/Q value, and the level of overall conservatism established is not reflective of what is required via the other acceptable options.

For codes that do not contain fixed values or calculate the parameters internally, the following parameters[9] shall be used for ensuring conservative calculation of offsite doses in accordance with Option 2:

- Non-buoyant, ground level, point source release;
- Plume centerline concentrations for calculation of dose consequences;
- Rural dispersion coefficients;
- A deposition velocity of 0.1 cm/sec for unfiltered release of particles(1-10 μm Aerodynamic Equivalent Diameter), 0.01 cm/sec for filtered particles, or 0 cm/sec for tritium/noble gases;
- A surface roughness of 3 cm;
- A minimum wind speed of 1 m/s;
- Plume meander may be used, consistent with the accident release duration and the appropriate code guidance; and
- Building wake factors should not be credited in the plume dispersion, outside of those already incorporated into plume meander.

Option 3 allows the use of site-specific methods and parameters as defined in a site/facility specific modeling protocol. Site-specific methods should make use of DOE-approved tool box codes and DOE-approved methods for determining site-specific parameters, where available and applicable. Codes that are not listed on the DOE Safety Software Central Registry may be a viable approach if the safety software quality assurance requirements of DOE O 414.1D are met, and the approach is approved via the modeling protocol. Accidents with unique dispersion characteristics, such as fires and explosions, may be modeled using phenomenon-specific codes that more accurately represent the release conditions. These phenomenon-specific dispersion

[9] This set of parameter values is intended to provide a conservative result when used together. However, the use of these individual parameters needs to be technically justified in the modeling protocol if used in Option 3.

characteristics may include buoyancy and thermal lofting. When Option 3 is used, the modeling protocol shall address the appropriateness of the model to the site-specific situation, show that the overall result (i.e., radiological dose consequence) is conservative, and be submitted to the DOE Safety Basis Approval Authority for approval prior to use. For new facilities and for the major modifications to existing facilities that are designed in accordance with DOE-STD-1189, the modeling protocol may be included as part of a Safety Design Strategy or other DOE-approved safety design basis document. Appendix A.7 provides a summary of the contents of the modeling protocol.

Determination of the Onsite χ/Q

A χ/Q value of 3.5×10^{-3} sec/m^3 shall be used for ground-level release evaluation at the 100 meter receptor location, unless an alternate onsite χ/Q value is justified. This value may not be appropriate for certain unique situations such as operations not conducted within a physical structure. When an alternate value is used, the DSA shall provide a technical basis supporting the need for the alternate value and the value selected.

Dose Coefficients and Breathing Rate

Dose coefficients consistent with International Commission on Radiological Protection Publication 68, *Dose Coefficients for Intakes of Radionuclides by Workers*, and Publication 72, *Age-dependent Doses to Members of the Public from Intake of Radionuclides*,[10] for adults shall be used.

A breathing rate of 3.3×10^{-4} meter^3/second, which corresponds to light activity breathing rate for adults should be assumed for the MOI and co-located worker.

3.2.4.3 Chemical Source Term and Consequence

Hazardous chemicals not screened out during the hazard analysis and with potential for consequences that exceed the SS control selection criteria in Section 3.3.2 are required by Section 3.1.3.3 to be quantitatively evaluated in the hazards evaluation or accident analyses. Similar to the radiological consequence analysis, chemical consequence analysis should use appropriately conservative values for the parameters related to material release, dispersal in the environment, and health consequences.

Chemical Source Term

The MAR is the bounding quantity of chemicals that is available to be acted upon by a given physical stress from a postulated accident. Chemical source terms may be evaluated using DOE-HDBK-3010 if appropriate for a nonreactive chemical release phenomenon (e.g., airborne

[10] DOE STD-1196-2011, *Derived Concentration Technical Standard*, (Appendix A) includes dose coefficients for adults consistent with ICRP Publication 72 dose coefficients. DOE has determined that the adult dose coefficients are appropriate for hazard scenario consequence estimates. However, in other situations such as determining collective dose to the public from a release, reference person coefficients from DOE-STD-1196-2011 are appropriate.

particulates suspended from accident stress on solids or liquids or aerodynamic entrainment over time), or by the application of a DOE "Toolbox code" that may also evaluate more complex release mechanisms such as a pressurized gas release, choked-flow, or two-phase flows. Another option for source term calculations is to apply the 40 C.F.R. Part 68 methodology for worst-case scenario development provided in "*Risk Management Program Guidance for Offsite Consequence Analysis*" (EPA 550-B-99-009, March 2009, or successor document); in particular, Chapter 3 of EPA 550-B-99-009 is generally appropriate for determining quantities and release rates for toxic gases and liquids, except where it may conflict with this Standard. The result of the chemical source term calculation is either a release rate (mass/time) or total release quantity (mass) and specified release duration. These results are applied along with the chemical dispersion analysis to estimate concentrations to the co-located worker and public. The concentrations are then compared to the Protective Action Criteria (PAC) from Section 3.3.2 to determine the need for SS controls.

ARFs and RFs are selected based on physical conditions and stresses anticipated during accidents. The EPA methodology for calculating chemical releases from gases and liquid evaporation is preferred. If the EPA methodology does not provide relevant guidance for the accident situation being modeled, DOE-HDBK-3010 defines bounding ARFs and RF mechanisms based on the physical context of the accident stress (e.g., boiling liquid from a fire, shock or blast effects from an explosion). It also provides airborne release rate recommendations that are applicable to aerodynamic entrainment of radioactive materials as a function of time, and those recommendations may also be applicable to chemical releases, e.g., wind suspension of powders.

If the chemical source term is not calculated as an airborne release rate or pool evaporation rate, the total airborne release quantity is divided by the release duration consistent with the postulated scenario assumptions, or by recommended conservative estimates from the guidance documents referenced above. If the source term is calculated as a release rate, the accident duration is not used to calculate a peak airborne concentration. Toxicological consequences of a release are based on the peak air concentration at the receptor location that occurs any time during the duration of the release.

Chemical Dispersion Analysis and Consequences

Atmospheric dispersion for hazardous chemicals may be modeled in a manner similar to radiological material dispersion where the material transport characteristics are similar. However, a number of variables can influence the chemical dispersion and generation of the source term. When a radiological dispersion model is known or suspected to be invalid for chemical application, the chemical dispersion analysis should use a DOE "Toolbox code" and applicable DOE guidance documentation, or an alternate model using industry accepted methods. Chemical releases involving gases that are cryogenic or have a density substantially heavier than air may require analysis using approved software codes designed and validated to handle the atmospheric dispersion for such gases. Another unique consideration for chemical releases requires application of a suitable code to evaluate chemical transformations that occur due to contact with air which can alter the toxicity of a plume by changing its chemical composition (as in the case of uranium hexafluoride). If neither a radiological dispersion analysis nor a DOE "Toolbox code" is used for the chemical dispersion analysis, a modeling

protocol shall address the appropriateness of the model to the site-specific situation (including source term characterization), show that the overall result (i.e., chemical consequence) is conservative, and be submitted to the appropriate DOE Safety Basis Approval Authority for approval prior to use.

If representative meteorological data is not available, Pasquill stability class F and one meter/second wind speed may be used for chemical dispersion based on 40 C.F.R. Parts 68 and 355 recommendations from EPA for worst-case modeling assumptions.

A χ/Q value of 3.5×10^{-3} sec/m^3 may be used for ground-level release evaluation for chemical releases at the 100 meter receptor location, unless an alternate onsite χ/Q value is justified. The use of an alternate onsite χ/Q value may be considered for unique situations such as operations not conducted within a physical structure, or unusual release and dispersion characteristics. When an alternate value is used, the DSA shall provide a technical basis supporting the need for the alternate value and the value selected.

The dispersion analysis is used to estimate chemical consequences in terms of a peak air concentration that occurs any time during the duration of the release to the MOI or co-located workers. Section A.2 of this Standard provides guidance for the calculation of exposure concentrations.

3.3 HAZARD CONTROLS

"830.202 (b) In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: . . . (5) Establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment." [10 C.F.R. § 830.202, "Safety Basis"]

"830.204 (b) The documented safety analysis for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility: . . . (4) Derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use;" [10 C.F.R. § 830.204, "Documented Safety Analysis"]

If an SC or SS control is found necessary, all preventive and mitigative controls associated with the sequence of failures that result in a given release scenario are candidates for consideration. Preventive or mitigative controls are selected using a judgment-based process considering a hierarchy of controls that gives preference to passive engineered safety features over active ones; engineered safety features over ACs or SACs; and preventive over mitigative controls.

When the hierarchy of controls is not used for situations requiring SC/SS controls (e.g., a SAC is selected over an available SSC), the DSA shall provide a technical basis that supports the controls selected. This is included as part of the mitigated analysis discussed in Section 3.2.3. The hierarchy of controls is further discussed in Appendix A, Section A.8.

The identification of hazard controls shall incorporate a defense-in-depth approach that builds layers of defense against release of radioactive or other hazardous materials so that no one layer by itself, no matter how effective, is completely relied upon. The overall approach to defense-in-depth is further discussed in Appendix A, Section A.9, and typically includes multiple independent layers of defense, including accident prevention, accident management, and accident mitigation layers. Section 3.3.2 below discusses a particular use of defense-in-depth as it applies to SS controls. The DSA shall describe the facility's approach to defense-in-depth for protection of workers and the public from the release of radioactive or other hazardous material.

In some cases, safety-SSCs rely upon supporting SSCs to perform their intended safety functions. For new facilities, Attachment 3 of DOE O 420.1C requires that support SSCs be designed as SC or SS SSCs if their failures prevent safety-SSCs or SACs from performing their safety functions. For existing facilities, support SSCs shall be designated at the same classification (SC or SS) as the safety controls they support, or else compensatory measures shall be established to assure that the supported safety-SSC can perform its safety function when called upon.

SSCs whose failure would result in losing the ability to complete an action required by a SAC shall be identified. These SSCs shall be designated as SC or SS based on the SAC safety function, or justification provided if not so designated.

3.3.1 Safety Class Controls

If the unmitigated release consequence for a DBA/EBA exceeds the EG, SC controls shall be applied to prevent the accident or mitigate the consequences to below the EG. If unmitigated off-site doses between 5 rem and 25 rem are calculated (i.e., challenging the EG), SC controls should be considered, and the rationale should be described for decisions on whether or not to classify controls as SC. It is expected that new nuclear facilities will reflect, through their design, construction and operation, a very low likelihood for accidents that could result in the release of any significant amount of radioactive material. Design basis accidents for new facilities will either be prevented or their consequences mitigated to below the EG. Further, it is DOE's goal that the combined effectiveness of the suite of SC and/or SS controls will be such that accident consequences would be well below the EG.[11] Appendix A, Section A.10 provides additional background on the EG.

As stated above, if the need for an SC control is determined, all preventive and mitigative controls associated with the sequence of failures that result in a given release scenario are candidates for an SC SSC designation. Not every SC candidate will necessarily be designated as SC. The process of designating one or more controls as SC is judgment-based and depends on multiple factors, such as: hierarchy of available controls, the control's effectiveness as determined per Section 3.2.3, and relative reliability of selected controls.

If the selection of sufficient preventive controls does not eliminate the hazard or terminate the accident scenario and prevent a release of radioactive or other hazardous materials, then an iterative process of mitigative control selection should be performed. This involves taking credit for mitigative features incrementally and comparing the results to the EG until below it. The extent of reduction in dose consequences is a function of the effectiveness of the mitigative control, such as high efficiency particulate air (HEPA) filters, or reduction in MAR.

<u>Existing Facilities with Mitigated Offsite Consequence Estimates over the EG</u>

In circumstances where no viable control strategy exists in an existing facility to prevent or mitigate the consequence of one or more of the accident scenarios from exceeding the EG, the following information shall be provided in the DSA, or an attachment to the DSA:

- Identification of the accidents that cannot be mitigated or prevented, including the likelihood of the event(s) and the mitigated consequences associated with the event(s), based on calculations following the methodology described in this Standard.
- A discussion of the credited controls, including their reliability and adequacy, and an analysis of the expected likelihood and mitigated offsite consequence estimates of the associated accident(s). The analysis should include a discussion of the significant

[11] This goal is not associated with a particular value, and therefore is not an explicit requirement.

contributors to uncertainties in both the likelihood and consequence evaluations. The analysis should compare the risk (i.e., likelihood and consequences) based on calculations performed per Section 3.2 of this Standard to the risk calculated using mean or best estimate values for source-term and dispersion input parameters (with supporting technical basis).

- A discussion of the available controls[12] that could reduce the likelihood and/or consequences of the associated accident(s), including their potential failure modes, their potential impact on accident mitigation, any relevant cost/benefit results, and the reasons why they are not selected as credited controls to reduce the consequences to below the EG.
- A discussion of any planned operational or safety improvements, including potential facility modifications, reductions in MAR, and/or additional compensatory measures, and associated schedules, to further reduce the likelihood and/or mitigate consequences of an accident. Note: Where DOE has accepted a path forward, the path forward may be used to support this discussion.
- A qualitative or semi-quantitative comparison of the facility risk from the identified scenarios and total facility risk (i.e., cumulative risk estimate for facility accidents) with the quantitative safety objectives provided in DOE Policy 420.1. Discuss the level of risk and the basis why this risk is acceptable, taking into account an evaluation of available alternatives, the benefits to the public of the alternatives, and the costs to the public of the alternatives.

The level of detail for the analysis above may be implemented on a graded approach that considers the remaining operating life of the facility and the extent of deviation from the EG. For example, where the remaining lifetime of the facility is less than five years, a detailed analysis using mean values and making comparisons to the DOE Policy 420.1 safety goals is not necessary, but a discussion of available controls considered and planned safety improvements and associated schedules is expected.

Once this condition (i.e., mitigated offsite consequence estimates over the EG) is identified in the DSA, the associated DSA content required above (including planned safety improvements and associated schedules) shall be updated in each subsequent annual update until the condition is prevented or mitigated below the EG, and may be removed from the DSA once resolved.

3.3.2 Safety Significant Controls

SS control designation shall be made on the basis of the control's contribution to: (1) defense-in-depth; (2) protection of the public from release of hazardous chemicals; (3) protection of co-located workers from hazardous chemicals and radioactive materials; and (4) protection of in-facility workers from fatality, serious injury, or significant radiological or chemical exposure. The applicable quantitative and qualitative criteria for these various categories of affected

[12] Controls considered but not identified as safety class controls include existing controls that were not elevated to safety class status, as well as new controls that could have been established through changes to the facility or to its operations. This includes controls to reduce the radiological source term. Controls can include SSCs and ACs.

persons are defined below. Similar to the SC control selection, the process of designating one or more controls as SS is judgment-based and iterative.

Safety Significant Controls Providing Major Contribution to Defense-in-Depth

Controls that provide a major contribution to defense-in-depth shall be designated as SS. These controls (SSCs and SACs) should be technically defensible, based on candidate controls in the hazard evaluation or accident analysis, and established based on the following:

- If a candidate control is common to multiple hazard/accident scenarios with moderate or high unmitigated consequences, its relative contribution to defense-in-depth should be considered for designating the control as an SS SSC or SAC. This consideration should be in the context of all of the hazard/accident scenarios taken together across the spectrum of hazards.
- If a support SSC is common to several SS SSCs (but not necessarily required to ensure operability alone of any single SS SSC) then it should be considered, from a reliability perspective, as a candidate for SS classification.
- If a candidate control further significantly reduces the consequences of a hazard/accident scenario already assigned an SC or SS control, then this control should be considered for designation as an SS SSC or SAC.
- If a candidate control that further significantly reduces the likelihood of a hazard/accident scenario already assigned an SC or SS control, then this control should be considered for designation as an SS SSC or SAC.
- If a candidate control appreciably reduces the risk of significant energetic events that potentially threaten multiple safety systems, then this control should be considered for designation as an SS SSC or SAC.
- If the reliability of a single control (preventative or mitigative) is not as high as desired, candidate controls designed to increase reliability by providing multiple layers of protection should be considered as SS SSCs or SACs.

An example of these criteria is the case where only one SC control is relied on to prevent or mitigate an accident. SSCs that could provide a major contribution to defense-in-depth in this situation include (1) a facility-level ventilation system with HEPA filtration, that provides mitigation as backup to a SC preventive control, (2) a glove box ventilation system that provides a second mitigative SSC to back up a facility-level ventilation system, or (3) a fire protection system that provides a second means to mitigate an accident in addition to a facility level ventilation system.

Designation of the major contributors to defense-in-depth is made following selection of SC and other SS controls (e.g., co-located worker, chemical releases, worker safety). The SS controls used for defense-in-depth should be independent from each other and any controls they support. It should be shown qualitatively that multiple SS and SC SSC failures would not occur in the same hazard/accident scenario.

Safety Significant Controls Providing Protection to the Public from Chemicals

SS designation of controls for protection of the public from chemical releases shall be based on a peak 15 minute time-weighted average air concentration, measured at the receptor location, that exceeds PAC-2 (Acute Exposure Guideline Level (AEGL)-2, Emergency Response Planning Guideline (ERPG)-2, and/or Temporary Emergency Exposure Limit (TEEL)-2). The TEEL table, however, includes many more chemicals than the industrial safety standards covered in AEGL-2 and ERPG-2. Analysis is not expected for a chemical on the TEEL list when it is apparent that due to releasability or dispersibility considerations, there would be limited, if any, concern for downwind release and exposure.

Safety Significant Controls Providing Co-located Worker Safety

For radiation hazards, a conservatively calculated unmitigated dose of 100 rem TED to a receptor located at 100 meters from the point of release shall be used as the threshold for designation of SS controls. The methodology used to determine consequences shall be consistent with that described in Section 3.2. SS designation for protection of co-located workers from chemical releases shall be based on a peak 15 minute time-weighted average air concentration at the receptor location that exceeds PAC-3.

For existing facilities, a situation could occur where no viable control strategy exists that could either prevent or mitigate one or more of the hazard/accident scenarios from exceeding the above onsite radiological or chemical consequence thresholds. In such a case, the DSA may determine co-located worker consequences at receptor distances further than 100 meters, if it consistent with the actual location of adjacent facilities. If the mitigated dose still exceeds 100 rem, or adjacent facilities are located at 100 meters or less from the point of release, the DSA shall provide a technical basis for the acceptance of the mitigated analysis results, including the reasons why other controls were not credited to reduce consequences below 100 rem.

Safety Significant Controls Providing for Facility Worker Safety

Safety management programs provide an important part of the overall strategy for protecting facility workers. However, SS controls (SSCs or SACs) shall be selected for cases where a fatality, serious injury, or significant radiological or chemical exposure to a facility worker may occur. The term “serious injury” refers to an injury requiring medical treatment for immediately life-threatening or permanently disabling injury such as the loss of an eye or limb. SS controls are not designated solely to address standard industrial hazards (see Appendix A.1). Examples of conditions that warrant consideration of SS designation include:

- High concentrations of radioactive or chemically toxic materials in areas where a facility worker could be present;
- Explosions or over-pressurizations within process equipment or confinement/containment structures or vessels, where serious injury or death to a facility worker may result from the fragmentation of structures or vessels; and
- Unique hazards that could result in asphyxiation or significant chemical/thermal burns.

3.3.3 Other Hazard Controls

The hazard evaluation process may identify preventive or mitigative controls that do not rise to the level of SC or SS but still enhance the safety of the facility. These controls are identified in the hazard evaluation table, but not explicitly credited with a SC/SS designation as identified in the DSA. Such controls are maintained in accordance with safety management programs and the Unreviewed Safety Question process.

Other hazard controls may also include specific controls required by DOE in its Safety Evaluation Report (see DOE-STD-1104-2009 for further guidance).

3.3.4 Criticality Safety Controls

The Criticality Safety Program ensures that operations remain subcritical under normal and credible abnormal conditions. NCS controls derived in accordance with the DOE-approved NCS Program are required to be implemented in accordance with 10 C.F.R. Part 830, *Subpart A, Quality Assurance Requirements*, commensurate with the importance of the safety functions performed. Explicit criticality controls required as a result of hazard evaluation criteria established in Section 3.1.3.2 shall be documented in the DSA and classified in accordance with requirements of Sections 3.3.1 and 3.3.2.

3.4 DESIGN OF HAZARD CONTROLS

For new facilities, DOE has established design requirements for SC and SS controls. These design requirements, specified in DOE O 420.1C or applicable successor document, include specific criteria for identification and use of industry codes and standards, as well as DOE technical standards such as DOE-STD-1189-2008 and DOE-STD-1020-2012. A system evaluation supporting the adequacy of safety SSCs and SACs, required to be included in the PDSA in accordance with DOE-STD-1189-2008, shall be incorporated into the DSA using guidance provided in Appendix B of this Standard.

For existing facilities, an engineering evaluation shall be conducted to assess the performance capabilities of safety SSCs. The evaluation shall determine the adequacy of the safety SSCs and demonstrate that they meet or exceed performance criteria (i.e., operational responses and capabilities) for the SSCs to ensure designated functional requirements are met under postulated accident conditions such as elevated pressures and temperatures. If performance criteria are not met, the evaluation shall identify noted deficiencies and any compensatory measures necessary to ensure the safety function of the SSCs. These compensatory measures may need to be identified as additional TSR controls, subject to the considerations for safety classification of controls described in Section 3.3.

The engineering evaluation shall address the relevant design capabilities of safety SSCs by one of the following methods:

- Providing a technical basis that includes an evaluation against the code of record, to the extent known, and augmented as needed with calculations, performance tests, or reliability evidence from operating history or industry databases;

- Comparing the safety SSC design attributes to DOE O 420.1C (or applicable successor document) design requirements, and associated codes and standards that are applicable, to demonstrate compliance; or
- Demonstrating that the existing SSCs satisfy equivalent design requirements of current design codes and standards.

The evaluation of SC and SS SSC adequacy is then documented in the DSA (see Section 4, Subsections [4.3.X.4] and [4.4.X.4] of this Standard for further discussion). Other hazard controls (i.e., not SC and SS) identified pursuant to Section 3.3.3 above are expected to be designed to the applicable industry code/standard for the given type of non-safety SSC. No specific evaluation of their adequacy is required to be documented in the DSA.

3.5 BEYOND DESIGN/EVALUATION BASIS ACCIDENTS

Section 830.204 of 10 C.F.R. Part 830 requires consideration of the need for analysis of accidents which may be beyond the design basis of the facility. Accidents that are excluded from accident analysis based on application of the criteria in Section 3.2.1 shall be scrutinized to determine whether they should be further evaluated as beyond design basis accidents (BDBAs) or beyond evaluation basis accidents (BEBAs).

The purpose of an analysis of accidents beyond the design or evaluation basis of the facility is to provide: (1) a perspective of the residual risk associated with the operation of the facility, and (2) additional perspectives for accident mitigation. These analyses provide valuable insights and can serve as bases for cost-benefit evaluation of improvements, modifications, or enhanced emergency management response capabilities. Such cost-benefit analysis is performed outside the DSA. It may also be appropriate to include some of these BDBA/BEBA considerations in the emergency plans of the DOE and non-DOE organizations that could be called upon to respond to a BDBA/BEBA.

Operational BDBAs/BEBAs are operational accidents with more severe conditions or equipment failures than are estimated for the corresponding DBA/EBA identified in the unmitigated analysis, or with likelihood of beyond extremely unlikely based on PRA results as described in Section 3.2.1. NPH BDBAs/BEBAs are defined by the initiating likelihood of the natural event itself (i.e., return period greater than the DBA/EBA return period for the next higher level as defined in DOE-STD-1020-2012). Man-made external events determined to be less than 10^{-6}/yr, conservatively calculated, do not require further evaluation in the DSA.

BDBA/BEBAs need not be analyzed to the same degree of detail as DBA/EBAs. The analysis is intended to provide insight into the magnitude of consequences of such events and to identify potential facility vulnerabilities. The analysis has the potential, therefore, for identifying additional facility features that could prevent or reduce severe accident consequences. Unlike the unmitigated conservative analysis for DBAs/EBAs, a realistic analysis of potential BDBA/BEBA consequences may be performed to determine whether accidents have a much larger consequence (a “cliff edge effect”) than the largest DBA/EBA.

If an operational accident or NPH event is determined to be a BDBA/BEBA, it should be evaluated to understand what hazard controls and accident mitigation plans may be appropriate to put in place. Realistic analysis may be used to understand the impact of the accident on radioactive or other hazardous materials and safety systems and to provide an assessment of actions that can be taken to mitigate the event, via post-accident planning, procedures, and hardware or other emergency planning enhancements. For example, if an accident is slow in progressing (takes multiple days to progress to where conditions of concern would occur), it may be appropriate to have instrumentation that is available to monitor accident progress, and actions that have been identified which can eliminate, limit, or mitigate the hazards in the timeframe in which the accident evolves.

These BDBA/BEBA actions, systems or controls do not need to be designated, designed, and controlled as SC or SS. However, measures need to be in place to help ensure their availability to prevent or reduce the impact of a BDBA/BEBA in accordance with programs, policies, and procedures discussed in the DSA. The BDBA/BEBA analysis provides further confirmation that a robust control set over the broad range of accident conditions that could occur in the facility has been identified, and that the most important controls were selected for TSR coverage.

3.6 PLANNED DESIGN AND OPERATIONAL SAFETY IMPROVEMENTS

As part of the hazard and accident analyses, the need for additional design or operational safety improvements may be identified. Due to capital costs, the need for further study of costs or technical feasibility, procurement lead times, or other complications, it may not be feasible to implement such design or operational improvements before the DSA is submitted. DSA completion should not be delayed until planned improvements are completed. The DSA may include a commitment to implement a future improvement. These improvements are described in Section [3.6] of the DSA.

It is not permissible to rely on incomplete upgrades to meet the requirements of this Standard. Interim controls may be necessary until such upgrades are completed. The scope of improvements appropriate for the DSA could be related to enhancements to credited controls or scopes of work addressed in the DSA not yet implemented, pending the completion of planned improvements.

3.7 REFERENCES

(1) 10 C.F.R. Part 830, *Nuclear Safety Management*.

(2) 10 C.F.R. Part 851, *Worker Safety and Health Program.*

(3) 29 C.F.R. § 1910.119, *Process Safety Management of Highly Hazardous Chemicals*.

(4) 29 C.F.R. § 1910.1450, *Occupational Exposure to Hazardous Chemicals in Laboratories.*

(5) 40 C.F.R. Part 68, *Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act.*

(6) 40 C.F.R. Part 355, *Emergency Planning and Notification.*

(7) ANSI/ANS-8.1, *Nuclear Criticality Safety in Operations with Fissionable Material Outside Reactors.*

(8) Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley/American Institute of Chemical Engineers, 2008.

(9) DOE O 414.1D, *Quality Assurance*, April 2011.

(10) DOE O 420.1C, *Facility Safety*, December 2012.

(11) DOE O 440.1B, *Worker Protection Program for DOE (Including the National Nuclear Security Administration) Federal Employees*, May 2007.

(12) DOE O 458.1 Admin Change 3, *Radiation Protection for the Public and the Environment*, February 2011.

(13) DOE G 151.1-2, *Technical Planning Basis, Emergency Management Guide*, July 2007.

(14) DOE-HDBK-3010-94 (Chg 1), *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*, March 2000, Reaffirmed 2013.

(15) DOE-STD-1020-2012, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities*, December 2012.

(16) DOE-STD-1027-92 (Chg 1), *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, September 1997.

(17) DOE-STD-1104-2009, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents*, May 2009.

(18) DOE-STD-1186-2004, *Specific Administrative Controls*, August 2004.

(19) DOE-STD-1189-2008, *Integration of Safety into the Design Process*, March 2008.

(20) DOE-STD-1196-2011, *Derived Concentration Technical Standard*, April 2011.

(21) DOE-STD-1628-2013, *Development of Probabilistic Risk Assessment for Nuclear Safety Applications*, September 2013.

(22) DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*, February 2007.

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

(24) DOE-STD-3014-2006, *Accident Analysis for Aircraft Crash into Hazardous Facilities*, May 2006.

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

(26) EPA-454/R-99-005, *Meteorological Monitoring Guidance for Regulatory Modeling Applications,* Environmental Protection Agency, February 2000.

(27) EPA 550-B-99-009, *Risk Management Program Guidance for Offsite Consequence Analysis*, March 2009.

(28) ICRP Publication 68, *Dose Coefficients for Intakes of Radionuclides by Workers*, International Commission on Radiological Protection, 1994.

(29) ICRP Publication 72, *Age-Dependent Doses to members of the Public from Intake of Radionuclides*, International Commission on Radiological Protection, 1995.

(30) NFPA 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response*, National Fire Protection Association, 2012.

(31) NRC Regulatory Guide 1.145, *Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants*, February 1983.

(32) NRC Regulatory Guide 1.23, *Meteorological Monitoring Programs for Nuclear Power Plants*, Nuclear Regulatory Commission, March 2007.

(33) NUREG-1140, *A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees*, January 1, 1988.

(34) NUREG/CR-2260, *Technical Basis for Regulatory Guide 1.145, "Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants,"* October 1981.

(35) "Protective Action Criteria (PAC): Chemicals with AEGLs, ERPGs, & TEELs," Rev 27, February 2012. Available at: http://www.atlintl.com/DOE/teels/teel.html.

SECTION 4. DSA FORMAT AND CONTENT

"830.202 (b) In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: . . . (4) Prepare a documented safety analysis for the facility;" [10 C.F.R. § 830.202, "Safety Basis"]

Criteria and guidance for the format and content of each of the chapters in the DSA are provided in this section. Each subsection begins with a brief introduction regarding the purpose of the chapter. The DSA shall address applicable DSA sections described below, consistent with the format and content described below. The DSA may include addenda for short-term evolutions (e.g., activities that may be conducted only once) provided the addenda meet the requirements of this Standard.

The DSA chapter sections described here are numbered in a manner that may be used in a DSA. For example, in the DSA Executive Summary, the headings "E.1 Facility Background and Mission" and "E.2 Facility Overview" could be used "as is" in the DSA to capture this information.

The chapter section numbers provided here are shown in brackets (e.g., [1.1]) to eliminate confusion with the actual sections of this Standard.

DSA [EXECUTIVE SUMMARY]

The DSA Executive Summary provides an overview of the facility safety basis and presents information sufficient to establish a top-level understanding of the facility, its operations, and the results of the safety analysis. It summarizes the facility safety basis as documented in detail in the remainder of the DSA.

The Executive Summary is prepared after the other DSA chapters have been completed, since it draws primarily upon the information in those chapters. The information provided in the Executive Summary is at a high-level and does not reproduce the details documented in subsequent chapters. Expected elements of the Executive Summary, as applicable based on the graded approach, include:

- Facility background and mission;
- Overview of the facility, including location and boundaries;
- Description of the facility hazard category (HC);
- Results of the facility safety analysis, including hazards analyzed and TSR controls;
- Acceptability of the facility safety basis; and
- Guide to the structure and content of the DSA (i.e., the "road map").

ORGANIZATION AND CONTENT GUIDANCE FOR THE DSA [EXECUTIVE SUMMARY]

[E.1] Facility Background and Mission

This section identifies the facility for which the DSA has been prepared, presents general information on the history of the facility and its current life-cycle stage, and summarizes the facility's current mission to be analyzed in the DSA. This section outlines any relevant information, such as short facility life-cycle, anticipated future change in facility mission, and approved DOE exemptions, that affect the extent of the safety analysis documented in the DSA, and explains how the graded approach has been used.

[E.2] Facility Overview

This section describes the facility location, its physical and institutional boundaries, relationships and interfaces with nearby facilities, layout, and significant interfaces with external systems and operations such as utilities, fire response, and medical assistance.

[E.3] Facility Hazard Categorization

This section provides a statement of the facility hazard category as determined in accordance with DOE-STD-1027-92. If determination of the hazard category relied upon segmentation of facility hazards or adjustments of release fractions, a brief explanation of the technical basis for such arguments is provided.

[E.4] Safety Analysis Overview

This section provides an overview of facility operations and results of the safety analysis, including:

- A description of the operations analyzed in the DSA;
- A summary of the significant hazards associated with the processes, including DBAs/ EBAs;[13] and
- A summary of TSR controls relied upon in the safety basis.

[E.5] Organizations

This section identifies the prime contractors responsible for facility design, construction, maintenance, and operation, and any subcontractors, consultants, oversight groups, and outside service organizations with significant safety functions. This section also identifies groups or individuals, including consultants, that participated in development of the DSA.

[13] As discussed in Section 3.2 and in Appendix A, Section A.6, for existing facilities the term Evaluation Basis Accident is often used in place of DBAs.

[E.6] Safety Analysis Conclusions

This section provides a brief assessment of the appropriateness of the facility safety basis. As part of this summary, identify any issues that are significant to the facility safety basis and that the facility operators recognize as requiring further resolution, but for which delay in documenting the facility safety basis is not warranted or potential budgetary considerations require DOE involvement in a decision process requiring extensive study (e.g., backfit analysis).

[E.7] DSA Organization

This section provides a guide to the structure and content of the DSA, its chapters, and appendices. If the main body of the DSA parallels the format delineated in this Standard, a simple statement to that effect will suffice.

DSA [CHAPTER 1: SITE CHARACTERISTICS]

This chapter of the DSA describes site characteristics affecting safe operation of the facility. The description locates the facility on the overall site, shows facility boundaries, and identifies nearby facilities that could affect the safety of operations. This chapter also provides information on external accident initiators, both natural and man-caused, to support assumptions used in the hazard and accident analyses.

For HC-3 facilities, it is generally not necessary to discuss meteorological conditions, hydrology, and offsite accident effects, because accident consequences are by definition limited to the facility itself. However, if a HC-3 facility could release hazardous chemicals offsite, this chapter provides information on site meteorology and hydrology.

For HC-2 facilities, the site characteristics description is focused on the area inside the site boundary, unless hazards have the potential to cause offsite consequences of concern. If a HC-2 facility could experience an accident affecting areas outside the site boundary, this chapter provides information on site characteristics beyond the site boundary.

Supporting documentation is referenced wherever relevant, with brief abstracts included to show the relevance of the reference to the discussion.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 1]

[1.1] Introduction

The introduction addresses the objectives and scope of Chapter 1.

[1.2] Requirements

This section lists the design codes, standards, regulations, and DOE Orders required for establishing the safety basis of the facility. The list should be confined to requirements actually used in the safety analysis or this chapter rather than a comprehensive listing of all industrial standards, codes, or criteria.

[1.3] Site Description

This section describes the site boundary and facility area boundary and provides basic geographic information, such as:

- The state and county in which the site is located;
- The location of the site relative to prominent natural and man-made features, such as rivers, lakes, mountain ranges, dams, airports, and population centers;
- A general location map to define the boundary of the site and show the correct distance of significant facility features from the site boundary;
- Any public exclusion areas and access control areas;
- The identification of the point(s) where the EG is applied; and
- Additional detail maps, as needed, to show orientation of buildings, traffic routes, transmission lines, and neighboring structures.

[1.3.1] Demography

This subsection provides population information, based on recent census data, to show the population distribution as a function of distance and direction from the facility. Demographic information emphasizes worker populations and nearby residences, major population centers, and major institutions, such as schools and hospitals, to the degree warranted by potential offsite consequences. The minimum area addressed is defined by the area significantly affected by the accidents analyzed in DSA Chapter 3.

[1.4] Environmental Description

This section describes the site's meteorology, hydrology, and geology.

[1.4.1] Meteorology

This subsection provides meteorological information necessary to understand regional weather phenomena of concern for facility operations and to guide dispersion analyses. Additional information on stability classification methodology, instrumentation type, measurement threshold, and measurement height may be needed to support dispersion analyses.

[1.4.2] Hydrology

This subsection provides hydrological information necessary to understand any regional hydrological phenomena of concern for facility operations and to support dispersion analyses. The discussion addresses relevant groundwater aquifers, drainage plots, soil porosity, and other aspects of the hydrological character of the site, including possible future changes. Average and extreme conditions, as determined by historical data, are described as needed.

[1.4.3] Geology

This subsection provides geological information necessary to understand any regional geological phenomena of concern for facility operations. The subsection describes the nature of

investigations performed and provides the results of these investigations. It also addresses geologic history, soil structures, and other relevant aspects of the geologic character of the site.

[1.5] Natural Event Accident Initiators

This section identifies specific natural events, such as design basis earthquakes and wildfires, that are considered to be potential accident initiators. A summary of assumptions supporting the analysis in DSA Chapter 3 should be included.

[1.6] Man-made External Accident Initiators

This section identifies specific man-made external events associated with the site but not associated with facility operations – such as explosions from natural gas lines or accidents caused by nearby transportation activities – that could be potential accident initiators. Sabotage and terrorism are excluded events. A summary of assumptions supporting the analysis in DSA Chapter 3 should be included.

[1.7] Nearby Facilities

This section identifies any nearby facilities that could affect, or be affected by, the facility being evaluated. A summary of assumptions supporting the analysis in DSA Chapter 3 should be included.

[1.8] Validity of Existing Environmental Analyses

This section compares current site characteristics with existing environmental analyses and impact statements. The section may state that no significant discrepancies exist, or indicate a need to revise and update existing environmental documentation.

DSA [CHAPTER 2: FACILITY DESCRIPTION]

This chapter describes the facility and the processes that will be conducted in it, in support of hazard identification, hazard and accident analysis, and selection of hazard controls. Details of SSCs and the types of work to be performed in the facility should be included. The chapter should provide a model of the facility that would allow an independent reader to understand facility operations and appreciate the facility structure and operations without extensive consultation of controlled references.

The level of detail required in the facility description is based on the facility's hazard classification and complexity of the safety analyses. For a HC-3 facility, a brief description of the facility, processes, and major SSCs may be adequate. Graded information should be provided, based predominantly on complexity.

Supporting documentation is referenced wherever relevant with brief abstracts included to show the relevance of the reference to the discussion.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 2]

"830.202 (b) In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: . . . (1) Define the scope of the work to be performed;" [10 C.F.R. § 830.202, "Safety Basis"]

"830.204 (b) The documented safety analysis for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility: (1) Describe the facility (including the design of safety structures, systems and components) and the work to be performed;" [10 C.F.R. § 830.204, "Documented Safety Analysis"]

[2.1] Introduction

The introduction addresses the objectives and scope of Chapter 2.

[2.2] Requirements

This section lists the design codes, standards, regulations, and DOE Orders required for establishing the safety basis of the facility. The list should be confined to requirements actually used in the safety analysis or this chapter rather than a comprehensive listing of all industrial standards or codes or criteria.

[2.3] Facility Overview

This section includes a brief overview of the current and historical use of the facility, projected future uses, facility configuration, and the basic processes performed therein.

[2.4] Facility Structure

This section provides an overview of facility buildings and structures, including construction details such as floor plans, equipment layout, construction materials, and dimensions relevant to hazard and accident analysis. Sufficient information should be provided for an overall understanding of the facility's structure and the general arrangement of the facility as it pertains to hazard and accident analysis.

[2.5] Process Description

This section describes the individual processes within the facility. It includes details on basic process parameters, including: (1) types and quantities of radioactive and other hazardous materials; (2) process equipment; (3) instrumentation and control systems and equipment; (4) basic flow diagrams; and (5) operations, including major interfaces between SSCs. Sufficient detail should be provided to support accident assessment and the safety analysis.

[2.6] Confinement Systems

This section identifies and describes SSCs that perform confinement functions, such as process vessels, gloveboxes, ventilation systems, and facility walls.

[2.7] Safety Support Systems

This section identifies and describes the principal systems that perform safety support functions not part of specific processes. The purpose of each system is stated, along with an overview of the system and its principal components, operations, and control function. Examples of systems under this heading might include fire protection, criticality monitoring, radiological monitoring (both air monitoring and contamination prevention), chemical monitoring (e.g., hydrogen concentration), and effluent monitoring.

For facilities that use and rely on site-wide safety support services, organizations, and procedures, this section may summarize applicable site-wide documentation provided its interface with the facility is made clear.

The safety support systems should be considered for designation as key elements to be monitored, controlled and maintained in accordance with the specifications of a safety management program and discussed in the DSA Chapter 7.

[2.8] Utility Distribution Systems

This section provides a schematic of utility distribution systems and a description of offsite power supplies and onsite utility components. Details of systems are described at a level necessary for understanding the utility distribution philosophy and facility operations.

[2.9] Auxiliary Systems and Support Facilities

This is a "catch-all" section addressing information not included in preceding sections relevant to conducting hazard and accident analyses.

DSA [CHAPTER 3: HAZARD AND ACCIDENT ANALYSIS, AND CONTROL SELECTION]

This chapter of the DSA provides information on the evaluation of normal, abnormal, and accident conditions to show compliance with the requirements of 10 C.F.R. Part 830. This chapter describes the process used to systematically identify hazards, categorize the facility, and evaluate the potential internal, man-made external, and natural phenomena events that could trigger accidents. These accidents are then evaluated to understand impacts within the facility, onsite and offsite and the need for SC and SS controls. This evaluation also includes a determination of the need for SS controls for chemical accidents and protection of the co-located worker. Topics addressed include hazard identification, hazard categorization, hazard evaluation, accident analysis, and control selection.

Supporting documentation is referenced wherever relevant with brief abstracts included to show the relevance of the reference to the discussion.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 3]

[3.1] Introduction

The introduction addresses the objectives and scope of Chapter 3.

[3.2] Requirements

This section lists the design codes, standards, regulations, and DOE Orders required for establishing the safety basis of the facility. The list should be confined to requirements actually used in the safety analysis or this chapter rather than a comprehensive listing of all industrial standards or codes or criteria.

[3.3] Hazard Analysis

This section describes the hazard identification and evaluation performed for the facility.

[3.3.1] Methodology

This subsection describes the methodology used to identify hazards and to perform a systematic evaluation of hazards.

[3.3.1.1] Hazard Identification

This subsection describes the method used to identify and inventory radioactive and other hazardous materials and energy sources (in terms of quantity, form, and location) associated with facility processes and related operations such as waste handling. This subsection also identifies sources from which information was obtained, such as flowsheet inventories, maximum historical inventories, vessel sizes, and contamination analyses. The interpretation of the data used to derive conservative inventory values is to be provided.

Interfaces with the worker health and safety program required by 10 C.F.R. Part 851 should be described. The technical basis for removing standard industrial hazards or other insignificant hazards from further consideration in the hazard evaluation are provided, as described in Section 3.1.1 of this Standard, and results presented in DSA Section [3.3.2.1].

[3.3.1.2] Hazard Evaluation

This subsection presents:

- The hazard evaluation technique(s) used to identify the complete spectrum of hazards at the facility, along with the rationale for selecting the given technique(s);
- The basic and guidance used in generating qualitative likelihood and consequence estimates in the hazard evaluation; and
- The process and guidance used to identify the need for, and adequacy of, controls found necessary for each hazard scenario.

[3.3.2] Hazard Analysis Results

This subsection describes the results of the hazard analysis.

[3.3.2.1] Hazard Identification

This subsection presents the results of the hazard identification activity. Hazard identification data sheets may be included in the DSA or referenced as needed. This subsection provides a summary table that identifies hazards by form, type, location, and total quantity. The basic set of hazards to be identified include radioactive materials , hazardous chemicals, flammable, and explosive materials used or potentially generated in facility processes, and any mechanical, chemical, or electrical source of energy that may influence the progression of an accident involving such materials. These hazards may be presented as specific hazards or as a general type (e.g., "3 Molar hydrofluoric acid" or simply "acid") so long as the assessment in the hazard analysis addresses the hazards that are likely in facility operations. This section includes a comprehensive identification of the inventories of these hazards and the associated basis for their selection.

This subsection summarizes major accidents or hazardous situations such as fires, explosions, and loss of confinement that have occurred in the facility's operating history. The specific details of each occurrence are not required; rather, a general summary by type, with emphasis on the major occurrences, will suffice.

[3.3.2.2] Hazard Categorization

This subsection presents the results of the final hazard categorization activity specified in DOE-STD-1027-92, including the facility hazard categorization, and where segmentation has been employed, describes segment boundaries and individual segment classifications. Where facility segmentation is used, this subsection should also provide the hazard breakdown by segment in a summary table.

Material at Risk (MAR) that was excluded from hazard or accident analysis for any reason (such as use of sealed sources or qualified containers) or from the hazard categorization process is quantified and justified.

[3.3.2.3] Results of Hazard Evaluation

This subsection presents the results of the hazard evaluation activity. Hazard evaluation characterizes the identified hazards in the context of the actual facility process.

The text includes or references hazard evaluation tables or data sheets either as an appendix to the DSA or supporting document(s). Hazard evaluation data are part of the DSA, whether included directly or by reference.

For each hazard scenario, hazard evaluation tables or data sheets document the following:

- Brief unmitigated hazard scenario description and assumptions, such as the initiating event, energy sources, qualitative or quantitative magnitude of radioactive or other hazardous material involved, release pathway(s), and initial conditions, if any;
- Estimated unmitigated likelihood of the hazard scenario;
- Estimated unmitigated consequences of the hazard scenario for the facility worker (qualitative or semi-quantitative), the co-located worker (qualitative or semi-quantitative), and the public;
- Available preventive and mitigative controls;
- Optionally, unmitigated risk binning;
- Optionally, estimated likelihood and consequences with selected controls credited and their safety functions, and mitigated risk binning if used (i.e., mitigated analysis in order to demonstrate the hazard scenario is prevented or adequately mitigated); and
- Operational safety enhancements determined to be necessary, e.g., additional preventive or mitigative controls that may be feasible to implement.

  Note: Appendix G of DOE-STD-1189-2008 identifies additional information that may be captured in the hazard evaluation table such as safety functions and method of detection.

Where a large number of scenarios are involved, simple summaries in terms of hazards, energy sources, causes, preventive and mitigative features, unmitigated consequence estimates, and unmitigated frequency estimates may be presented in this subsection. It is derived from examining the raw information in the hazard evaluation tables or data sheets. This presentation may use relevant hazard scenarios to frame and focus the discussion.

The mitigated hazard evaluation, if not presented in the DBA mitigated analysis in DSA Section [3.4.3.X.5], is also documented in this section to provide the rationale for designation as SS SSCs or SACs as well as their safety functions. The mitigated analysis also demonstrates the effectiveness of SS controls in terms of the effects of crediting preventive and mitigative controls. This may be addressed in a general summary that discusses the hierarchy of controls for each category of hazard scenarios (e.g., fires, explosions, spills/loss of confinement) requiring SS controls.

Detailed bases of engineering judgments are not required to be formally documented in the DSA; however, summaries of the underlying rationale should be provided related to hazard evaluation assumptions and selection of SS controls. Pertinent documentation is referenced as necessary.

The DSA hazard evaluation also examines the potential for large-scale environmental contamination. This subsection documents pathways for uncontrolled release of large amounts of hazardous materials to the environment identified in the hazard evaluation. Further consideration of environmental protection is addressed in the DSA [3.3.2.6].

[3.3.2.4] Defense-in-Depth

This subsection provides an evaluation of the facility's approach to defense-in-depth for protecting workers and the public from the release of radioactive or other hazardous material. (See Appendix A, Section A.9, for a discussion of defense-in-depth.)

For controls that are selected from the hazard evaluation or the DBA/EBA evaluation in Section [3.4.3.5] as major contributors to defense-in-depth, provide the rationale for designation as SS SSCs or SACs as well as their safety functions.

[3.3.2.5] Facility Worker Safety

This subsection provides an evaluation of the facility's approach to facility worker safety, exclusive of standard industrial hazards, with focus on protection from radiological and chemical hazards, potential explosions and over-pressurizations, and unique hazards. It provides a general overview of worker safety in terms of SSCs and administrative features. This subsection also includes a list of any SS controls (SSCs or SACs), the safety function of each control, and the key elements of safety management programs relevant to facility worker safety. Interfaces with the worker health and safety program required by 10 C.F.R. Part 851 should be described.

It is derived from examining the raw information in the hazard evaluation tables or data sheets and distilling it into a clear overview of worker safety features at the facility. This presentation may use relevant hazard scenarios to frame and focus the discussion, but need not duplicate the hazard evaluation already provided in or appended to the DSA, and summarized in Section [3.3.2.3], "Hazard Evaluation."

This subsection provides documented evidence that worker safety features are an integral part of facility design and operation, that basic facility operations for worker safety are adequate, and that workers are protected by a number of means including safety management programs described elsewhere in the DSA. With the exception of SS SSCs and SACs, TSR designation is made in the form of ACs for overall programs only for worker safety. Typical safety management programs include criticality protection, radiation protection, hazardous material protection, institutional safety provisions, procedures and training, operational safety, and emergency preparedness. Specifically identify programs that will be provided TSR coverage as ACs in Chapter 5, "Derivation of Technical Safety Requirements."

For controls selected from the hazard evaluation to protect the facility worker, provide the rationale for designation as SS SSCs or SACs as well as their safety functions. If the basic function of a worker safety feature has already been discussed in Section [3.3.2.3], that feature may simply be identified by name and referenced.

[3.3.2.6] Environmental Protection

This subsection provides an evaluation of the facility's approach to environmental protection. This section should focus on unique issues not addressed elsewhere.

This subsection summarizes the design and operational features that reduce the potential for

large material releases to the environment and documents that no large release with the potential to cause significant environmental insult exists for which an obvious and easily implemented design or operational change could minimize. For example, consider widespread river or groundwater contamination due to spills from the contents of a tank. It would not be an appropriate conclusion to accept such a risk if a simple dike around the tank would alleviate the problem and yet had not been installed. Conversely, consider the handling of plutonium in a facility with gloveboxes, ventilation zones of confinement, and HEPA filters. These measures would be adequate for closure of environmental contamination concerns for process accidents. In the majority of instances, process related TSRs and safety SSCs assigned for defense-in-depth or for worker safety may be sufficient to address environmental concerns.

[3.4] Accident Analysis

This section describes accident selection, DBA and EBA development, designation of SS and SC controls, and the results of mitigated accident analyses. Include identification of whether the quantitative evaluation of chemical accidents or co-located worker radiological consequences to compare to SS control selection criteria from Section 3.3.2 of this Standard are included in this section, or were already evaluated in the DSA Section [3.3.2.3].

[3.4.1] Accident Identification Methodology

This section summarizes the methods used to derive the DBAs and EBAs from the hazard evaluation, quantifies their consequences, designates SC and SS controls, and evaluates the effectiveness of safety controls in preventing or mitigating postulated accidents.

For each analytical tool that is used:

- Computer models should be identified and described;
- Validation for the specific application, including the type and range of data should be discussed; and
- Detailed information supported by references should be provided on algorithms, computational and analytical bases, and software quality assurance measures.

Documentation of a selected methodology includes the following:

- Methods used to estimate source terms for DBA and EBAs, including:
  - The basic approach for estimating physical facility damage;
  - The general basis for assigning MAR quantities not directly derived from hazard identification, if differing values are used; and
  - The basis for release fractions, release rates, and RFs used; and
- Methods used to estimate dose and exposure profiles, consistent with options described in Sections 3.2.4.2 and 3.2.4.3 of this Standard, including assumptions about such variables as meteorological conditions, time-dependent characteristics, and release rates or duration for radioactive or other hazardous materials that could be released to the environment.

[3.4.2] Accident Selection

This section identifies the set of facility DBA/EBAs in terms of:

- Categories of operational accidents, natural events, and man-made external events;
- Accident type (fire, explosion, spill, earthquake, tornado, etc.); and
- Whether the accident is representative or unique.

DBA/EBAs may be identified for other accidents if not quantitatively evaluated in the hazard evaluation and included in DSA Section [3.3.2.3]. Examples include radiological exposures to the co-located worker or chemical exposures to the public and co-located worker.

In the case of representative accidents, the bounded hazard scenarios are identified.

If operational accidents are not selected as DBA/EBAs based on the PRA results, a summary is provided that describes them and that they are further evaluated in the DSA Section [3.5] as beyond DBA/EBAs.

[3.4.3] Analysis of Design Basis/Evaluation Basis Accidents

This section analyzes the DBA/EBAs selected in DSA Section 3.4.2, to quantify conservative likelihoods and consequences, compare radiological consequences to the EG and co-located worker dose threshold, and to compare any chemical consequences to chemical exposure thresholds for the MOI and co-located workers.

For each accident, the unmitigated and mitigated scenarios are sufficiently documented to reveal the thought process used for the analysis, the selection of SC and SS SSCs, and the evaluation of the level of protection provided by the identified controls.

Key parameters used in the unmitigated and mitigated analysis of DBA/EBAs are identified and justified.

The following format is repeated for each (“X”) DBA/EBA.

[3.4.3.X] Accident Designation

Identify the DBA or EBA by individual title, category (operational, natural, or man-made external) and type (e.g., fire, explosion, spill, earthquake, tornado).

[3.4.3.X.1] Scenario Development

This subsection describes the progression of the accident by linking initiating events with preventive and mitigative controls and other contributing phenomena. Each response, action, or indication required to initiate action, is considered relevant to the scenario progression.

The summary for an initiating event for a natural-event DBA or EBA should identify load factors, return periods, amplification factors for the facility, and similar variables that characterize the phenomenon. For operational accidents, the summary should include the magnitude of the energy release and describe the physical conditions (such as temperature or pressures) relevant to accident progression.

This subsection also summarizes facility and equipment response to loads or environmental conditions postulated to be present at the time of a given natural event or accident. In such cases, this subsection should reference the analysis or facility documentation, summarize relevant assumptions, and discuss the degree of conservatism in the evaluation. Because external-event DBAs and EBAs are developed using likelihood criteria, this subsection references the analysis of the external event likelihood or presents its technical basis.

This subsection documents the rationale for the unmitigated likelihood assignment used in the hazard evaluation.

[3.4.3.X.2] Source Term Analysis

This subsection identifies the material and energy released through the pathways of concern during the accident, defines the parameters and phenomenological models used to derive the source term, and addresses the characteristics of the release as it relates to the source term determination. This subsection also includes a discussion of the source term factors described in Section 3.2.4.1 of the Standard. Detailed quantification of uncertainty is not required.

[3.4.3.X.3] Consequence Analysis

This subsection identifies the receptor doses associated with the relevant pathways using guidance provided in Section 3.2.4.1 of this Standard. The subsection provides the receptor location, X/Q, the unmitigated doses for the relevant DBA/EBAs and the mitigated doses as discussed in Section 3.2.3 of this Standard.

[3.4.3.X.4] Comparison to Consequence Thresholds

This section compares the unmitigated consequences of accident scenarios to the EG, the MOI chemical exposure threshold, and the co-located worker thresholds described in Section 3.3.2 of this Standard.

[3.4.3.X.5] Summary of Safety Class and Safety Significant SSCs, SACs, and TSR Controls

This subsection documents the mitigated analysis results and lists the SC and SS SSCs, SACs, and safety management programs that are expected to prevent the scenario or to reduce MOI dose below the EG, provide defense-in-depth, or to provide co-located worker safety. This subsection identifies the safety function(s) for the credited controls to prevent or mitigate the accident and documents the rationale for the overall acceptability of the credited control suite. This section also addresses protection of assumptions on physical conditions (e.g., LPF) that may need to be evaluated for TSR Design Feature designation. The DSA provides a technical basis

whenever engineering controls are not selected, consistent with the preferred hierarchy of controls, as described in Section 3.3 of this Standard.

This hierarchy of controls is applied to: (1) each DBA/EBA where the need for SC/SS controls has been identified; and (2) the summary of hazard evaluation results for each accident category (e.g., fires, explosions, spills/loss of confinement, and NPH) where the need for SS controls has been identified.

If the set of SC/SS controls for DBA/EBAs is informed by PRA results, a summary is provided that describes the basis for decisions on the control set, references the PRA results, and identifies associated key assumptions and initial conditions that will be protected.

[3.5] Beyond Design Basis Accidents (BDBAs) and Beyond Evaluation Basis Accidents (BEBAs)

This section documents the analysis of any BDBA or BEBA defined for the facility by describing the following:

- The scope and method for analysis;
- The results of a realistic analysis of the impact of hazard controls failure;
- The results of analyzing operational accidents or NPH; and
- Potential methods to prevent or mitigate a BDBA or BEBA.

These analyses can provide valuable insights and can serve as bases for cost-benefit analysis of potential safety improvements in hardware or emergency planning. It may also be appropriate to include some of these BDBA/BEBA considerations in the emergency plans of the DOE and non-DOE organizations that could be called upon to respond to a BDBA/BEBA.

BDBA/BEBAs need not be analyzed in the same degree of detail as DBA/EBAs, nor do they serve as a basis for designating safety SSCs.

[3.6] Planned Design and Operational Safety Improvements

This section presents any commitments being made in the DSA to future design and operational safety improvements. For each commitment, provide:

- A general description of the improvement, to the degree that it has been conceptually finalized;
- A summary of the basis for the commitment, in the context of the affected hazard scenarios; and
- Interim controls, if applicable, proposed until the improvement is implemented.

Commitments made in a DSA need to be approved by DOE in the Safety Evaluation Report.

DSA [CHAPTER 4: SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS]

This chapter of the DSA provides information on the SSCs necessary to protect the public and workers and to provide major contributions to defense-in-depth. Details are provided on SACs that significantly reduce the risk of specific accidents. The chapter also describes the attributes (functional requirements and performance criteria) required to support the safety functions identified in the hazard and accident analyses and to support subsequent derivation of TSRs.

This chapter references supporting documentation. A brief summary is included for each such reference, explaining its relevance to this chapter and providing a basic understanding of the reference.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 4]

[4.1] Introduction

The introduction addresses the objectives and scope of Chapter 4.

[4.2] Requirements

This section lists the design codes, standards, regulations, and DOE Orders required for establishing the safety basis of the facility. The list should be confined to requirements specific to this chapter.

[4.3] Safety Class Structures, Systems, and Components

This section provides information on each SC SSC relied on in the facility. The description of each such SSC will contain sufficient detail for an understanding of its safety function and its relationship to the facility safety analysis.

A summary list of SC SSCs is provided in a table that identifies the following information: the SC SSCs, the accidents from DSA Chapter 3 for which the SC designation was made, safety functions, functional requirements, and performance criteria judged to require TSR coverage. Subsections following the table provide details that correlate to the list.

Note: The following format is repeated for each (“X”) SC SSC. The examples provided are for illustration purposes only and not intended as a requirement to designate such systems as SC.

[4.3.X] Safety Class Structure, System, or Component

Identify the SC SSC.

[4.3.X.1] Safety Function

This subsection states the reasons for designating the SSC as SC and describes its preventive or mitigative safety function(s) as determined in the hazard and accident analysis.

Safety function descriptions state the objective of the SSC in a given accident scenario. For example, the safety function of a hydrogen detector in a dissolver vessel offgas line could be stated as: "To monitor hydrogen concentration in the dissolver offgas and provide a signal to shut down the dissolving operation before explosive concentrations of hydrogen are reached."

Every safety function for each control clearly ties back to the hazard evaluation or accident analysis (e.g., if a control is credited for a fire scenario, a seismic scenario, and an operational spill scenario, then this section addresses all appropriate safety functions as credited).

The specific accident(s) or general rationale (e.g., to protect initial conditions of the analysis) associated with the safety function is identified. There may, or may not be, a single accident that, by itself, completely defines the safety function.

[4.3.X.2] System Description

This subsection provides a description of the SC SSC and the basic principles by which it performs its safety function. This subsection also describes boundaries and interface points with other SSCs relevant to the safety function. The discussion should focus on providing information required to support the system evaluation in DSA Section 4.3.X.4, "System Evaluation." SSCs whose failure would result in an SC SSC losing the ability to perform its required safety function are identified.

An SSC description provides a summary of the physical information known about the SSC, including process and instrumentation drawings or a simplified system drawing with references to process and instrumentation drawings. Relevant manufacturer's specifications are discussed. All discussion should focus on information directly related to the safety functions of the SSC rather than general specifications such as overall weight or starting torque. Such details may be included only by referencing the specifications.

[4.3.X.3] Functional Requirements

This section identifies the functional requirements needed to fulfill safety functions. Such requirements are specified for both the SC SSC and any needed support for the SC SSC. Functional requirements are to be described only for the specific accident(s) where the SC SSC is required to function. For example, seismic parameters need not be stated if the accident of interest is not initiated by an earthquake.

Functional requirements specifically address the pertinent response parameters or nonambient environmental stresses related to an accident for which the safety function is relied on. Functional requirements are derived from the hazard and/or accident analysis. In the hydrogen detector example given above, one obvious parameter would be keeping the hydrogen concentration below the explosive limit. If the offgas temperature were significantly above ambient temperatures, operation at that temperature would be a functional requirement as well.

[4.3.X.4] System Evaluation

Performance Criteria

This subsection provides performance criteria imposed on the SC SSC so it can meet functional requirement(s) and, thereby, satisfy its safety function. Performance criteria characterize the specific operational responses and capabilities necessary to meet functional requirements. Performance criteria are typically based on control responses to environmental conditions created by postulated accident scenarios, but may also be parameters identified in applicable codes and standards. For example, a fire suppression system may be required by NFPA codes to have a specified flow rate.

Performance Evaluation

The ability of the SC SSC to meet performance criteria under DBA or EBA conditions is evaluated in accordance with the requirements in Section 3.4 of this Standard. If the control cannot meet the performance criteria, this section identifies the deficiency and compensatory measures necessary to ensure the safety function of the SSC. In such cases, this section also provides a strategy for expeditious removal of compensatory measures. Compensatory measures in this context are not permitted for new facilities or major modifications to existing facilities designed in accordance with DOE-STD-1189-2008 or successor document.

[4.3.X.5] Technical Safety Requirements (TSRs)

This subsection lists the specific attributes of each SC control that require protection by TSRs. TSR protection ensures that assumptions and inputs to the accident analysis are maintained valid.

[4.4] Safety Significant Structures, Systems, and Components

This subsection provides information on each SS SSC relied on in the facility. The description of each such SSC will contain sufficient detail for an understanding of its safety function and its relationship to the facility safety analysis.

A summary list of SS SSCs is provided in a table that identifies the following information: the SS SSCs, the accidents from DSA Chapter 3 for which the SS designation was made, safety functions, functional requirements, and performance criteria judged to require TSR coverage. Subsections following the table provide details that correlate to the list.

Note: The following format is repeated for each ("X") SS SSC. The examples provided are for illustration purposes only and are not intended as a requirement to designate such systems as SS.

[4.4.X] Safety Significant Structure, System, or Component

Identify the SS SSC.

[4.4.X.1] Safety Function

This subsection states the reasons for designating the SSC as SS and describes its preventive or mitigative safety function(s) as determined in the hazard and accident analysis.

Safety function descriptions state the objective of the SSC in a given accident scenario. For example, the safety function of a hydrogen detector in a dissolver vessel offgas line could be stated as "to monitor hydrogen concentration in the dissolver offgas and provide a signal to shut down the dissolving operation before explosive concentrations of hydrogen are reached."

Every safety function for each control clearly ties back to the hazard evaluation or accident analysis (e.g., if a control is credited for a fire scenario, a seismic scenario, and an operational spill scenario, then this section addresses all appropriate safety functions as credited).

The specific accident(s) or general rationale (e.g., to protect initial conditions of the analysis) associated with the safety function is identified. There may, or may not be, a single accident that, by itself, completely defines the safety function.

[4.4.X.2] System Description

This subsection provides a description of the SS SSC and the basic principles by which it performs its safety function. This subsection also describes boundaries and interface points with other SSCs relevant to the safety function. The discussion should focus on providing information required to support the system evaluation in DSA Section 4.4.X.4, "System Evaluation." SSCs whose failure would result in an SS SSC losing the ability to perform its required safety function are identified.

An SSC description provides a summary of the physical information known about the SSC, including process and instrumentation drawings or a simplified system drawing with references to process and instrumentation drawings. Relevant manufacturer's specifications are discussed. All discussion should focus on information directly related to the safety functions of the SSC rather than general specifications such as overall weight or starting torque. Such details are included only by referencing the specifications.

[4.4.X.3] Functional Requirements

This subsection identifies the functional requirements needed to fulfill safety functions. Such requirements are specified for both the SS SSC and any needed support for the SS SSC. Functional requirements are to be described only for the specific accident(s) where the SS SSC is required to function. For example, seismic parameters need not be stated if the accident of interest is not initiated by an earthquake.

Functional requirements specifically address the pertinent response parameters or nonambient environmental stresses related to an accident for which the safety function is relied on. Functional requirements are derived from the hazard and/or accident analysis. In the hydrogen detector given above, one obvious parameter would be keeping the hydrogen concentration

below the explosive limit. If the offgas temperature were significantly above ambient temperatures, operation at that temperature would be a functional requirement as well.

[4.4.X.4] System Evaluation

Performance Criteria

This subsection provides performance criteria imposed on the SS SSC so it can meet functional requirement(s) and, thereby, satisfy its safety function. Performance criteria characterize the specific operational responses and capabilities necessary to meet functional requirements. Performance criteria are typically based on control responses to environmental conditions created by postulated accident scenarios, but may also be parameters identified in applicable codes and standards. For example, a fire suppression system may be required by NFPA codes to have a specified flow rate.

Performance Evaluation

The ability of the SS SSC to meet performance criteria under DBA or EBA conditions is evaluated in accordance with the requirements in Section 3.4 of this Standard. If the control cannot meet the performance criteria, this section identifies the deficiency and any compensatory measures necessary to ensure the safety function of the SSC. In such cases, this section also provides a strategy for expeditious removal of compensatory measures. Compensatory measures in this context are not permitted for new facilities or major modifications to existing facilities designed in accordance with DOE-STD-1189-2008 or successor document.

[4.4.X.5] Technical Safety Requirements (TSRs)

This subsection lists the specific attributes of each SS control that require protection by TSRs. TSR protection ensures that assumptions and inputs to the accident analysis are maintained valid.

[4.5] Specific Administrative Controls (SACs)

This subsection provides information on each SAC relied on in the facility. The description of each such SAC will contain sufficient detail for an understanding of its safety function and its relationship to the facility safety analysis.

A summary list of SACs is provided in a table that identifies the following information: the SACs, the accidents from DSA Chapter 3 for which the SAC is a designated control, safety functions, functional requirements, and performance criteria judged to require TSR coverage. Subsections following the table provide details that correlate to the list.

Note: The following format is repeated for each (“X”) SAC.

[4.5.X] Specific Administrative Control

Identify the SAC.

[4.5.X.1] Safety Function

This subsection describes the rationale for designating an AC as an SAC, states whether the SAC performs an SC or SS function, and identifies its preventive or mitigative safety function(s) as determined in DSA Chapter 3.

Safety function descriptions state the objective of the SAC in a given accident scenario. For example, the safety function of a MAR limit could be stated as "to limit the total quantity of nuclear material present within the facility to no more than 2000 curies."

Every safety function for each control clearly ties back to the hazard evaluation or accident analysis (e.g., if a control is credited for a fire scenario, a seismic scenario, and an operational spill scenario, then this section addresses all appropriate safety functions as credited).

The specific accident(s) or general rationale (e.g., to protect initial conditions of the analysis) associated with the safety function is identified. There may, or may not be, a single accident that, by itself, completely defines the safety function.

[4.5.X.2] SAC Description

This subsection provides a description of the SAC and the basic principles by which it performs its safety function. Also described are boundaries and interface points with any SSCs relevant to the safety function, such as manual actions interfacing with sensors, instrumentation, and other equipment. Reference DSA Section [4.3.X.2] or [4.4.X.2] for the system description if the SSC is classified as SC or SS, and explain how needed to provide the SAC safety function.

If a SAC is used in lieu of safety SSCs, the rationale for this decision is described. In general, engineered safety features are preferable to ACs and SACs, and emphasis is placed on identifying safety SSCs. A discussion of why SSC(s) are not used for accomplishing the safety function should be included.

SSCs whose failure would block the actions required by the SAC should be identified. These SSCs are designated as SC or SS based on the classification of the SAC safety function and guidance in DOE-STD-1186-2004, *Specific Administrative Controls*, as discussed in Section 3.3 of this Standard.

When describing the SAC, provide a basic summary of the physical information known about the SAC, including: tables or drawings showing relevant information (such as instrumentation); other SSCs; physical boundaries; approved storage areas; and, operator routes or locations.

[4.5.X.3] Functional Requirements

This subsection identifies the functional requirements needed to fulfill safety functions of the SAC. Such requirements are specified for both the SAC and any needed supporting SSCs. Functional requirements are to be described only for the specific accident(s) where the SAC may be relied on. Functional requirements for SACs may involve ensuring unimpeded access to

specific rooms or areas, use of certain instrumentation, written procedures or checklists, and special tooling.

As stated in Section 3.3 of this Standard, SSCs whose failure would result in losing the ability to complete an action required by a SAC are designated as SC or SS based on the SAC safety function, or justification provided if not so designated. If supporting SSCs are not classified as SC and addressed in Section 4.3.X.3 and are not classified as SS and addressed in Section 4.4.X.3, then this subsection identifies the SSC functional requirements needed to fulfill SAC safety functions. Functional requirements are to be described only for the specific accident(s) where the SAC is required. Functional requirements specifically address the pertinent response parameters or nonambient environmental stresses related to an accident for which the safety function is relied on. Functional requirements are derived from the hazard and/or accident analysis as necessary to provide the SAC safety function.

[4.5.X.4] SAC Evaluation

Performance Criteria

This subsection provides performance criteria that ensure the SAC can meet functional requirements(s) and, thereby, satisfy its safety function.

If equipment is required to implement the SAC and it is not designated as SC or SS SSC, then this subsection provides performance criteria imposed on the SSC so it can meet functional requirement(s) and, thereby, satisfy the SAC safety function.

Performance Evaluation

The formulation of SACs includes a process to validate that plant operators can perform the task(s) called for within the timeframes assumed in the safety analysis. If SACs require operator action, a human factors evaluation is carried out that examines:

- Adequacy of the description of the task in facility procedures;
- Level of difficulty of the task;
- Design of the equipment and feedback (e.g., indicators and alarms);
- Time available to do the task or recover from an error; and
- Stress caused by noise, heat, light, protective clothing, and similar factors.

Formal engineering calculations may be necessary to ensure that plant operators have the adequate time and resources to carry out required tasks. For example, if an SAC requires that operators take action to locate and isolate a leak, flow rate calculations will be needed to justify the time interval needed to accomplish the task. Consequences of incorrect implementation of the control are evaluated, and measures to prevent control failure are factored into the control formulation.

If equipment is required to implement the SAC and it is not designated as SC or SS SSC, then ability of the SSC to meet its performance criteria under DBA or EBA conditions is evaluated in accordance with the requirements in Section 3.4 of this Standard.

[4.5.X.5] Technical Safety Requirements (TSRs)

SACs are generally implemented in TSRs as Limiting Conditions of Operation (LCOs) or as "Directed Action" ACs found in the AC section of the TSR. Further information can be found in Section 4 of DOE-STD-1186-2004.

DSA [CHAPTER 5: DERIVATION OF TECHNICAL SAFETY REQUIREMENTS]

This chapter of the DSA provides information necessary to support the safety basis requirements for the derivation of TSRs in 10 C.F.R. Part 830.

This chapter describes how TSRs are derived using the information in the previous two chapters. The information in this chapter demonstrates how the selected TSRs comply with 10 C.F.R. § 830.205. Further guidance can be found in DOE Guide 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements.*

Supporting documentation is referenced wherever relevant with brief abstracts included to show the relevance of the reference to the discussion.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 5]

[5.1] Introduction

The introduction addresses the objectives and scope of Chapter 5.

[5.2] Requirements

This section lists the design codes, standards, regulations, and DOE Orders required for establishing the safety basis of the facility. The list should be confined to requirements specific to this chapter.

[5.3] TSR Coverage

This section provides assurance that TSR coverage for the facility is complete. The section lists all controls identified in Chapters 3 and 4 above that protect the public and the workers or provide a major contribution to defense-in-depth.

The list should be presented in table format with the following data included for each control: relevant hazard/accident, associated TSR safety limits, limiting control settings, limiting conditions for operations, surveillance requirements, ACs, and design features.

[5.4] Derivation of Facility Modes

This section discusses the derivation of the operational modes such as startup, operation, and shutdown used by the facility that are relevant to derivation of TSRs. The definition of modes required in this section expands and formalizes the information provided in Chapter 3 regarding operational conditions associated with accidents.

[5.5] TSR Derivation

This information may be organized by the hazard protected against, the specific controls, or by the actual TSRs, if desired. The following format is repeated for each TSR ("X").

[5.5.X] Applicable Hazard/Control/TSR "X"

[Control or TSR Designation]

[5.5.X.1] Safety Limits, Limiting Control Settings, and Limiting Conditions for Operation

This subsection provides information sufficient to derive safety limits (SLs), limiting control settings (LCSs), and LCOs to support TSR documentation required by 10 C.F.R. § 830.205. SLs are those bounds within which the process variables are maintained for adequate control of the operation and are not exceeded in order to protect the integrity of the physical system that is designed to guard against the uncontrolled release of radioactivity. LCSs are settings for automatic alarm or protective devices related to those variables having significant safety functions. Where a LCS is specified for a variable on which a SL has been placed, the setting is chosen so that the protective action, either automatic or manual, will correct the abnormal situation before a SL is exceeded. LCOs are the lowest functional capability or performance levels of equipment required for safe operation of the facility. LCSs and LCOs act to keep operating conditions below the SLs, however most LCOs are assigned without an accompanying SL.

Mitigation of releases is generally not amenable to the useful definition of SLs. For example, a ventilation system that directs airflow through HEPA filters to keep offsite radiological dose below the EG during an accident is mitigative and is more appropriately addressed by an LCO. Temporary loss of this ventilation system's function during normal operations does not initiate a significant radiological or hazardous material release. An LCO on the system would identify the specific responses necessary to compensate for the loss of safety function. Control of the ventilation system via an SL would be of questionable value for preventing accidents that the ventilation system only mitigates. In contrast, a tank might act as a barrier preventing an uncontrolled release of radioactive or other hazardous material exceeding the EG without ventilation mitigation. If that tank could be ruptured by a hydrogen explosion, the tank's hydrogen concentration may warrant coverage by an SL.

[5.5.X.2] Surveillance Requirements

This subsection provides information necessary to derive surveillance requirements for testing, calibration, or inspection activities to assure that the necessary quality of systems and components is maintained and facility operations remain within SLs, LCSs, and LCOs. This information will be used in developing the TSR Bases Appendix (see DOE G 423.1-1A, *Implementation Guide for Use in Developing Technical Safety Requirements*). Surveillance frequencies and methods are of primary importance. Referencing national consensus codes and standards is an acceptable approach where the application is justified in writing.

[5.5.X.3] Administrative Controls

This subsection provides information necessary to derive TSR ACs, including SACs. This section deals with controls listed in Section [5.3] above. The rationale for using TSR ACs is described.

A special type of TSR AC is one that controls a safety management program. In such cases, the "Administrative Controls" section of the TSR contains commitments to establish, maintain, and implement these programs at the facility. Facility staffing requirements may also be addressed.

SACs, when designated, provide specific actions or conditions related to individual accident scenarios, such as limits on radioactive or other hazardous material inventory and combustible loading.

[5.6] Design Features

This section describes the passive design features that, if altered or modified, could have a significant effect on safe operation. The discussion should address safety functions, performance criteria, and periodic surveillance.

[5.7] Interfaces

This section summarizes TSRs from other facilities and agreements with other responsible entities that affect this facility's safety basis and briefly summarizes the provisions of those TSRs. For example, where an interface facility provides necessary controls to protect this facility, this section identifies those controls and summarizes the associated interface facility's TSRs.

DSA [CHAPTER 6: PREVENTION OF INADVERTENT CRITICALITY]

"830.204 (b) The documented safety analysis for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility: . . . (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." [10 C.F.R. § 830.204, "Documented Safety Analysis"]

This chapter of the DSA provides information that will support the development of a safety basis in compliance with the provisions of 10 C.F.R. § 830.204(b)(6) regarding the definition of a criticality safety program (CSP). If this information is available in a site-wide CSP description and it complies with the rule's requirements, it may be included by reference and summarized in this chapter. This section of the DSA summarizes the key attributes of the CSP and includes, by reference, additional elements of the CSP as required by DOE O 420.1C or applicable successor documents.

Supporting documentation is referenced wherever relevant with brief abstracts included to show the relevance of the reference to the discussion.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 6]

[6.1] Introduction

The introduction addresses the objectives and scope of Chapter 6.

[6.2] Governing Documents

This section identifies and describes the relevant governing documents (i.e., procedures or programs), regardless of whether the governing documents are facility-specific, site-specific, company-specific, or otherwise. If the program is individually implemented at the facility, the governing facility documents are identified, with a summary explanation of their relationship to the safety of the facility. If the program is implemented at an overall site-wide level, the governing site documents are identified, with a summary explanation of their relationship to the safety of the facility. If the program is implemented jointly, both sources are identified.

This identification should focus on top-level documents defining the program and any overall implementation document used at the facility level. There is no requirement to identify all procedures down to the subject matter expert level.

If a separate CSP description document meets the requirements of DOE O 420.1C, then a simple reference to that CSP description document along with a summary abstract is sufficient to meet the requirements of this section. The applicable nuclear criticality safety standards are also required to be listed. Detailed listings of other relevant governing documents are not required in this case, because the CSP description document contains the appropriate content.

However, if Chapter 6 of the DSA is to fulfill the requirements of the DOE O 420.1C for the CSP description document, then all relevant governing documents need to be identified in this section along with text presenting the information above and required from DOE O 420.1C.

[6.3] Criticality Safety Program

This subsection may serve as the CSP description document, in which case the DSA describes all program elements as required by DOE O 420.1 C (or successor document). Alternatively, when the CSP is approved in a separate document, this section of the DSA includes a reference to the DOE-approved CSP description document along with a description of the major characteristics of the CSP that are necessary to ensure safe operation of the facility.

Additional information to be provided in this section includes a general discussion of: (1) criticality control strategy, such as adherence to preferred hierarchy of controls, (2) Criticality safety design strategy and basic features of the design; (3) parameters used for the prevention of inadvertent criticality; (4) basis and analytical approach for deriving operational criticality limits; and, (5) key program elements warranting special emphasis such as nuclear criticality safety staff training and qualifications, based on criticality events discussed in the DSA hazard evaluation.

[6.4] Supporting Safety Management Programs

A group of safety management programs or processes typically work together to support the CSP. Such programs and processes might include configuration management, conduct of operations, quality assurance, initial testing, in-service surveillance and maintenance, training, and work control. In this subsection, identify the programs and processes that provide key support to the CSP and summarize how these programs contribute to ensuring that an inadvertent criticality will not occur and criticality alarm systems will be available when required by the ANS/ANSI standards and criticality safety evaluations.

This section provides a general discussion of the applicability of safety management programs that ensures criticality safety controls are implemented and maintained in accordance with ANSI/ANS-8 series of national standards. At a minimum, this section provides a summary description of how the following programs support the CSP:

- Conduct of operations;
- Initial testing;
- In-service surveillance and maintenance;
- Configuration management; and
- Quality assurance.

DSA [CHAPTER 7: SAFETY MANAGEMENT PROGRAMS]

"830.204 (b) The documented safety analysis for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility: . . . (5) Define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection;" [10 C.F.R. § 830.204, "Documented Safety Analysis"]

This chapter of the DSA provides information that will support the development of a safety basis in compliance with the provisions of 10 C.F.R. § 830.204(b)(5) regarding the definition of safety management programs.

Supporting documentation is referenced wherever relevant with brief abstracts included to show the relevance of the reference to the discussion. If facility management does not wish to modify the programmatic chapters in currently approved DSAs, a consolidated chapter is not required. Review and evaluation of annual updates in such cases should refer to the archived DOE-STD-3009, CN3. See Appendix A, Section A.11 of this Standard for further discussion of safety management programs.

ORGANIZATION AND CONTENT GUIDANCE [CHAPTER 7]

Section 830.204(b)(5) of 10 C.F.R. Part 830 identifies nine safety management programs required to be addressed where applicable. Those programs comprise the following subsections of this chapter:

[7.1] Radiation Protection
[7.2] Fire Protection
[7.3] Maintenance
[7.4] Procedures
[7.5] Training
[7.6] Conduct of Operations
[7.7] Quality Assurance
[7.8] Emergency Preparedness
[7.9] Waste Management

Other programs may be important for individual facilities, and addressed in additional subsections appended to the above list. For example, explosives safety may be judged to warrant its own chapter at a nuclear explosives facility, or hazardous material protection at a facility with chemical hazards.

[7.X] [Name of Program]

This subsection provides a summary description.

[7.X.1] Governing Documents

This subsection identifies and describes the governing procedures and programs, which may be facility-specific, site-specific, company-specific, or otherwise. If the program is implemented only at the facility, the governing facility documents are identified and related to the safety of the facility. If the program is implemented at a site-wide level, the governing site documents are identified and related to the safety of the facility. If the program is implemented jointly, both sources are identified. Only top-level documents defining the program and describing its implementation should be addressed. There is no requirement to identify all procedures down to the subject matter expert level.

[7.X.2] Program Description

This subsection describes the major characteristics of the program necessary to ensure safe operation of the facility.

[7.X.3] Key Elements

This section describes key program elements that will be individually identified under the safety management programs. Key elements are those that: (1) are specifically assumed to function for mitigated scenarios in the hazard evaluation, but not designated an SAC; or, (2) are not specifically assumed to function for mitigated scenarios, but are recognized by facility

management as an important capability warranting special emphasis. It is not appropriate for a key element to be identified in lieu of a SAC (see Section A.12). The basis for selection as a key element is specified, including detail on how the program element: (1) manages or controls a hazard or hazardous condition evaluated in the hazard evaluation; (2) affects or interrupts accident progression as analyzed in the accident analysis; and (3) provides a broad-based capability affecting multiple scenarios.

APPENDIX A: TECHNICAL BACKGROUND OF KEY DSA CONCEPTS

The information in this Appendix provides perspective and technical basis for key Documented Safety Analysis (DSA) concepts. This includes historical and philosophical information used in the development of DOE-STD-3009-94, which remain relevant to this revision.

A.1 Standard Industrial Hazards

The Department of Energy (DOE) recognizes, via Title 10 of the Code of Federal Regulations (C.F.R.) Part 830, the importance of including worker safety in safety analyses by specifically noting the worker as a population of concern. Developing a conceptual basis for the methodology used in this Standard requires answering the fundamental question of how worker safety is most appropriately addressed in the DSA. DSAs include hazard analyses and hazard controls for worker safety, unless the hazards and their potential consequences are due to standard industrial hazards.

Standard industrial hazards are hazards that are routinely encountered in general industry and construction. These workplace hazards are addressed by provisions of 10 C.F.R. 851, *Worker Safety and Health Program*, which requires identification and assessment of worker hazards and compliance with safety and health standards that provide specific safe practices and controls. Based on these provisions, evaluation of standard industrial hazards within DSAs is needed to the extent that these hazards act as initiators or contributors to accidents, or result from chemical or radiological hazards (for example, when an explosion is caused by radiolysis inside a tank). When standard industrial hazards are excluded from further evaluation, Section 3.1.1 of this Standard requires such conclusions to be included in the hazard identification, along with the basis used for exclusion.

Standard industrial hazards that may be considered for exclusion from the DSA hazard evaluation include those in which a national consensus code and/or standard (e.g., Occupational Safety and Health Administration (OSHA) regulation) defines and regulates appropriate worker safety practices. Specifically, the codes and standards required by 10 C.F.R. 851.23, *Safety and Health Standards*, may be considered. Examples of hazards addressed by these requirements include confined spaces, electrocution, falling objects, non-ionizing radiation, hot work, and lasers. Toxicity of hazardous chemicals is addressed in Section A.2 rather than this subsection.

Unique hazards may be present in facilities that are not specifically addressed by the above exclusion criteria, either because of quantities larger than typically used in general industry or because of unique DOE applications or operations. Such hazards may represent a potential hazard to an entire work area affecting multiple workers, or have the ability to impact the safe operation of the facility (e.g., inability to perform a specific administrative control (SAC)). An example of such hazards could be an explosion hazard created by radiolysis in tanks, piping, or containers. Significant quantities of cryogenic material or compressed gases/liquids may also warrant consideration because of asphyxiation hazards that might affect the ability of facility operators to safely manage the facility. Such unique hazards are not treated as standard industrial hazards and are evaluated in the DSA.

Standard industrial hazards that have the potential to be an accident initiator involving chemical or radioactive material releases are retained as part of the DSA hazard evaluation. For example, the existence of 440-volt alternating current cabling in a glovebox could be identified as a potential accident initiator of a fire involving radioactive or other hazardous materials.

A.2 Chemical Hazards

The DSA is not intended to deal extensively with chemicals that can be safely handled by implementation of a hazardous material protection program. Therefore, a screening process is established to select for DSA evaluation only those chemicals of concern (i.e., type and quantity that have the potential for significant health effect on the facility worker, co-located worker, or public) that are present in the facility or activity and present hazard potentials outside the routine scope of the hazardous material protection program. Chemicals that could otherwise be screened out, but have the potential to be an accident initiator involving radioactive or hazardous material releases, or could compromise the ability of the facility operators to safely manage the facility, are retained as part of the DSA hazard evaluation.

Examples of chemicals that may be excluded from the DSA's hazard evaluation include:

- Chemicals with no known or suspected toxic properties. This exclusion may be claimed when a chemical is not listed in OSHA or EPA toxic chemical regulations or is not assigned a PAC 2 or 3 value on the website of the Subcommittee on Consequence Assessment and Protective Actions (SCAPA);
- Materials that have a health hazard rating of 0 or 1, based on National Fire Protection Association (NFPA) 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response*, or equivalent ratings from Global Harmonization System of Classification and Labeling of Chemicals;
- Materials that are commonly available and used by the general public, including any substance to the extent it is used for personal, family, or household purposes and that is present in the same form, quantity, and concentration as a product distributed for use by the general public (e.g., bleach, motor oil); and
- Small-scale use quantities of chemicals similar to the intent of 29 C.F.R. § 1910.1450, *Occupational Exposure to Hazardous Chemicals in Laboratories* (i.e., containers that are designed to be easily and safely manipulated by one person). A general guideline, as described in DOE Guide (G) 151.1-2, *Technical Planning Basis, Emergency Management Guide*, is individual containers with capacities less than approximately 5 gallons (19 L) for liquids with densities near that of water, 40 pounds (18 kg) for solids (or heavy liquids), or 10 pounds (4.5 kg) for compressed gases, that are handled under the provisions of an identified safety management program such as the Hazardous Material Protection program.

Materials that represent an extraordinary toxic hazard (e.g., high acute toxicity and dispersibility) may not be excluded using the above screening criteria. Those substances may include, but are not limited to: chemical warfare nerve agents; any substance of similar toxicity [e.g., Acute Exposure Guideline Level (AEGL)-3, Emergency Response Planning Guideline (ERPG)-3, or Temporary Emergency Exposure Limit (TEEL)-3 values less than about 3 ppm] that has been

designed for efficient dispersal as a gas, vapor or aerosol; and compressed gases with acute toxicity in the same range.

When chemical hazards are excluded from further evaluation, Section 3.1.1 of this Standard requires such conclusions to be included in the hazard identification, along with the basis used for exclusion.

Regarding the potential decomposition of chemicals from accidental fires, it is recognized that toxic products of combustion exist from the burning of many types of structural materials, household objects, and other non-hazardous chemicals. The toxic properties of smoke are a well-recognized hazard and are managed and controlled as part of the emergency management and fire protection programs and associated fire protection codes, standards and requirements that are used for design, construction, storage, use, and fire response. The DSA does not evaluate these hazards nor does it establish structures, systems, and components (SSCs) or SACs based on the hazards of these toxic products. However, it is not appropriate to screen decomposition products (e.g., NO_x generation) that are part of a facility process (e.g., incinerator, steam reformer) from evaluation, unless they meet the explicit exclusion criteria stated above.

For hazardous chemical aerosols and gases with a density near that of air, standard Gaussian atmospheric dispersion may be used to estimate chemical consequences. If the toxic material is released at some average rate over some period of time, the peak concentration at the receptor is obtained directly from the definition of the steady state χ/Q'

$$C = Q'\left(\frac{\chi}{Q'}\right)$$

Where:

C = peak concentration (mg/m^3)
Q' = toxic material release rate (mg/s)
χ/Q' = relative concentration (s/m^3)

Exposure to an air concentration greater than the toxic protective action criteria (PAC) criteria for safety significant (SS) control selection is assumed to confer a certain health detriment to the exposed individual. Although a duration of exposure is implicit in the PAC definitions, shorter exposures to higher concentrations of some chemicals can have comparable effects. Accordingly, averaging the concentration from a short-duration release over 30 or 60 minutes may significantly under-predict the hazard. On the other hand, averaging over a very short time (e.g., a minute or two) represents the peak concentration more conservatively; however, the validity of any comparison between the calculated "peak" concentration PAC value is questionable. It is therefore useful to calculate a time-weighted average (TWA) concentration at the receptor location for some period less than that implied by the PAC definition but long enough that the results can be viewed as having relevance to the criteria.

To address both concerns, TWA concentration at the receptor location is usually calculated for some period less than that implied by the PAC definition, but long enough that the results can be accepted as having some relevance to the criteria. For example, EPA 550-B-99-009, *EPA Risk Management Program Guidance for Offsite Consequence Analysis*, which specifies ERPG-2 values (one of the criteria for establishing the PAC-2) as primary toxic endpoints for their

evaluation, assumes a 10-minute release averaging time in its determination of distance to the endpoint for worst-case analyses of toxic gases even though the ERPG-2 values are based on 60 minutes.

The DOE PAC concentrations are based on different durations as defined by their concentration limit definitions from EPA or chemical industry. To standardize releases from gases, liquids, and particulates, the hazard evaluation and/or accident analysis may assume a peak 15-minute, TWA chemical concentration for comparison to the PAC values for SS control designation. There is no adjustment of the PAC value or the calculated concentration to account for differences between the recommended 15-minute exposure time and the exposure time implicit in the definition of the PACs.

If the toxic effects of a chemical are known to be dose-dependent (i.e., the toxic effects depend upon the total quantity of material taken up by the body) and not concentration-dependent, then for these chemicals only, the 1-hour average concentration may be used. For short-duration releases (e.g., less than 15 minutes), the concentration at the receptor may be calculated as the TWA over the release period, but for no less than 1 minute.

Some consequence assessment dispersion codes will calculate the desired maximum 15-minute average concentration directly by allowing the analyst to specify the averaging period. To determine the average concentration manually, the following formula may be used:

$$\mathrm{TWA} = \frac{C_1 T_1 + C_2 T_2 + C_n T_n}{T_1 + T_2 + T_n}$$

Where:

C = Concentration (ppm or mg/m^3)
T = Time period of exposure (min)

For release durations longer than 15 minutes, the peak 15-minute average concentration during the duration of the release is used for concentration dependent chemicals. For the peak 15-minute TWA, the 15-minute period of maximum exposure (concentration) is selected and input (as 15, one-minute segments) into the above formula. For exposure periods of less than 15 minutes, the product of $C_x T_x$ may equal zero during the exposure period. Individual time intervals less than one minute are not appropriate for use in the numerator of the above formula for calculating the TWA. This assumption is conservative for "instantaneous" types of releases (e.g., container puncture of powders, over-pressurization of container). However, the use of a shorter averaging duration than 15 minutes, such as the actual exposure period but not less than one minute, may be warranted depending on the acute toxicity of the chemical of interest and the peak concentration observed.

For chemical mixtures and concurrent releases of different substances, consequences are assessed using the Mixture Methodology "Hazard Index" approach recommended by the DOE Office of Emergency Management SCAPA Chemical Mixtures Working Group. A brief explanation of this approach and the published journal article are available on the SCAPA website, http://www.orau.gov/emi/scapa/index.htm, under Health Code Numbers. An Excel

workbook that automates the implementation of the approach and its user's guide are also available on the SCAPA website.

Concurrent releases are analyzed if a plausible scenario exists by which quantities of different substances could be released from the same location at the same time. Concurrent releases of dissimilar substances that, because of separation by distance or physical barriers, could result only from extreme malevolent acts or catastrophic events (such as major fires, airplane crashes, severe natural phenomena impacts, and building collapse) need not be analyzed.

A.3 Initial Conditions

Both hazard and accident analyses make use of initial conditions (ICs). ICs are specific assumptions regarding a facility and its operations that are used in defining accident scenarios. As discussed in Sections 3.2.2 and 3.2.3 of this Standard, facilities are analyzed as they exist (or are designed) when quantifying meaningful release mechanisms.

Specific examples of ICs include:

- A vault or building can withstand natural phenomena hazard (NPH) events according to its NPH Design Category;
- Facility geometry or layout affects accident progression or release;
- Solid transuranic waste is contained in a certified Department of Transportation (DOT) Type-A drum;
- A certain material is present only within a certified Type B shipping container;
- Facility and process inventories are limited to those identified; and
- A passive SSC prevents significant consequences.

It is important to define and document ICs carefully to ensure they are appropriately controlled, classified as SC or SS and preserved via TSR operating limits, design features or SACs as appropriate. As stated in Sections 3.2.2 and 3.2.1 for the unmitigated consequence and likelihood assessments, the initial conditions and assumptions for the analysis are required to be documented and evaluated to determine if controls need to be put in place to ensure the evaluation will remain valid. If the TSR control or safety classification is removed, the assumption may no longer be used in the unmitigated analysis as an initial condition.

Also, as stated in Section 3.2.2 on unmitigated analysis, it is not appropriate to credit administrative controls or safety management program controls as initial conditions. For example, it would not be acceptable to rely on a combustible loading limit in the unmitigated analysis to show that a full facility fire is not plausible. An exception is that MAR values may be considered initial conditions if addressed by a SAC.

A.4 Hazard Evaluation and Risk Ranking

As discussed in Section 3 of this Standard, the initial analytical effort for all facilities is a hazard analysis that systematically identifies and evaluates facility hazards and accident potentials. The hazard evaluation identifies the initiating event, scenario development, associated controls,

consequences, and likelihood. The latter two parameters are often used in both DOE and the commercial nuclear industry to specify risk ranking for a given event. Risk ranking in this context is a simple mechanism to summarize the event's significance in terms such as "low, moderate, and high" consequences and "anticipated, unlikely, extremely unlikely, and beyond extremely unlikely" likelihoods as described in Section 3.1.3.1 of this Standard. Risk rankings of unmitigated hazard scenarios allow selection of representative evaluation basis accidents (EBAs) as described in Section 3.2.1 of this Standard.

This Standard specifies consequence thresholds for safety SSCs and SAC designations. In this regard, and for other hazard evaluation and accident analysis purposes, quantification of accident likelihoods is useful to:

(1) Provide additional insight for the hazard evaluation or design basis accident (DBA)/EBA analysis for choosing among controls when multiple controls address the same events;
(2) Support event tree and fault tree analyses of complex nuclear operations for the hazard evaluation or DBA/EBA analysis;
(3) Identify higher-consequence accidents that may warrant more detailed consideration due to higher likelihood for selecting representative DBA/EBAs for accident analysis; and
(4) Identify operational accidents as not plausible for DBA/EBA selection based on a probabilistic risk assessment (PRA).

Beyond the qualitative application of consequences and likelihoods (or supplemented with quantitative perspectives) for the hazard evaluation, risk ranking serves the broader purpose of confirming for the DOE approval authority that the overall mitigated risk of facility operation is low. Risk ranking can also highlight a given scenario whose mitigated risk remains significant. Table A-1 gives an example risk-ranking table that combines likelihood and consequence.

Table A-1: Qualitative Risk Ranking Bins[1]

Consequence Level	Beyond Extremely Unlikely[2] Below 10^{-6}/yr	Extremely Unlikely 10^{-4} to 10^{-6}/yr	Unlikely 10^{-2} to 10^{-4}/yr	Anticipated Above 10^{-2}/yr
High Consequence	III	II	I	I
Moderate Consequence	IV	III	II	II
Low Consequence	IV	IV	III	III

I = Combination of conclusions from risk analysis that identify situations of major concern
II = Combination of conclusions from risk analysis that identify situations of concern
III = Combination of conclusions from risk analysis that identify situations of minor concern
IV = Combination of conclusions from risk analysis that identify situations of minimal concern

1. Industrial events that are not initiators or contributors to postulated events are addressed as standard industrial hazards in the hazard analysis.
2. For external events, likelihood below 10^{-6}/yr conservatively calculated is "Beyond Extremely Unlikely."

Risk ranking in DSAs does not constitute a PRA. Instead, it is a fundamentally qualitative or semi-quantitative exercise to gain perspective, not to quantify residual risk against formal criteria. Selected PRA-related tools such as fault and event trees may be used to the extent helpful in hazard evaluation or accident analysis. Further, risk ranking is not a means to disregard consequences ranked in excess of the safety SSC designation thresholds defined in Sections 3.3.1 and 3.3.2 of this Standard. Safety SSC and/or SAC designation is required for an

operational accident, NPH event, or external event that exceeds a consequence threshold, regardless of whether the unmitigated likelihood is ranked "anticipated," "unlikely," or "extremely unlikely." However, as discussed in Section 3.2.1, a quantitative analysis that is completed in accordance with DOE-STD-1628-2013, including the development of a PRA plan (approved by DOE), may be used to support decisions regarding the need for safety controls for operational events.

Although the exercise of determining accident likelihood is typically qualitative, analysts often develop a numerical basis for judgments to provide consistency. For example, a simple methodology for unmitigated likelihood assignment could be to assign a probability of "1" to non-independent events, "0.1" to human errors, and "0.01" to genuinely independent SSC failures that would be used to establish the initiating event likelihood[14] as described on Table 2 of Section 3.1.3.1. Again, for the unmitigated analysis, these human errors and equipment failures cannot represent the failure probability of a preventive control that would otherwise provide a SC or SS safety function. Another methodology for unmitigated initiating event likelihood classification would be to use a summary of historical data.

The mitigated frequency of occurrence when crediting preventive controls could also apply simple numerical estimates to assign a lower frequency bin. For example, a 0.01 failure probability could be assigned to a preventive engineered control or a SAC based on the technical justification in the DSA Chapter 4.

A.5 Criticality Safety

American National Standards Institute (ANSI)/American Nuclear Society (ANS) Standard 8-1, *Nuclear Criticality Safety* in *Operations with Fissionable Material Outside Reactors*, requires consideration of all credible initiating events. The criticality safety process is based on identifying multiple layers of defense with the objective that subcriticality is always ensured. Failure of any single control may diminish the overall effectiveness of the multilayered defense, but will not lead to an inadvertent criticality.

The ANSI/ANS-8 series of national standards also offer a variety of requirements and recommendations that result in an effective criticality safety program. These provisions cover such elements as training and qualification of criticality safety engineers and operators, control implementation verification, configuration management of controls, and periodic assessment and control implementation validation. DOE Order (O) 420.1C, *Facility Safety*, requires contractors to document how the requirements and recommendations of applicable ANSI/ANS-8 series national standards will be implemented. If they will not be implemented, the order requires a justification approved by DOE.

[14] To determine the likelihood of an accident scenario, only initiating events are expressed as rate of occurrence with the units of inverse time (i.e., per year), and other enabling events are expressed in terms of unitless failure probabilities.

A.6 Evaluation Basis Accidents

DBAs have traditionally been used in nuclear facility applications to inform facility design and explicitly identify the controls relied on to protect the public against significant releases of radioactive materials. A conceptually different approach is needed for existing facilities where DBAs are typically either non-existent or no longer valid for a variety of reasons, such as changes in the original mission or outdated design philosophies. For such facilities, the concept of the EBA was developed to identify the safety by analyzing the safety of the facility "as is." EBAs are derived from hazard scenarios identified during the hazard evaluation process. EBA analysis involves an evaluation of the adequacy of the existing controls protecting the public. This analysis may identify a need for corrective or compensatory measures in the form of SC or SS SSCs. EBAs may also be used to evaluate the need for SS controls to protect the co-located worker.

A.7 Dispersion Modeling Protocol

The modeling protocol needs to include sufficient information to allow for the establishment of the technical basis for the dispersion modeling result. By providing this level of information regarding the tools, methodologies, site characteristics, and data sources, the facility can ensure that any concerns regarding the final result are resolved early in the process. Basic background regarding the facility is necessary in demonstrating the appropriateness of the methods for assessing atmospheric dispersion. This background includes information regarding:

- Receptor locations – a facility map that highlights the release point and DOE site boundaries, local land use, significant building structures, and elevated terrain if those considerations are being used in the modeling process;
- Meteorological data – sufficient information regarding the projected sources of the data, the years covered, and the methodology used to process the raw data into a format appropriate for use in dispersion modeling, and the methods used to establish the averaging time, release height, calm wind handling, and the use of local surface roughness;
- Modeling tools – model choice for performing the dispersion analysis, if not established as part of the DOE Toolbox, along with proper documentation of the model's validity per DOE's requirements for software quality assurance; and
- Methodologies used to prepare modeling parameters and their validity – examples of these parameters include, but are not limited to, surface roughness, building wake, plume meander, averaging time, release characteristics, deposition velocity, and the appropriate dispersion coefficients.

A.8 Hierarchy of Controls

Preventive or mitigative controls are selected using a judgment-based process considering a hierarchy of control preferences. DOE has established a control selection strategy based on a hierarchy of controls for the design of new facilities and major modifications; see DOE O 420.1C, DOE-STD-1189-2008, and DOE G 420.1-1A for additional information. DOE O 420.1C, Attachment 2, Section 3(b)(4)(d) establishes the requirement for nuclear facilities to be designed to "provide controls consistent with the hierarchy described in DOE-STD-1189-2008."

DOE-STD-1189-2008 provides this hierarchy in the section entitled "Safety Design Guiding Principles" that states (note: clarifications to quoted text are included in brackets):

> *"Control selection strategy to address hazardous material release events is based on the following order of preference at all stages of design development.*
>
> - *Minimization of hazardous materials* [including radioactive and non-radioactive] *is the first priority.*
> - *Safety structures, systems, and components (SSCs) are preferred over* [Specific] *Administrative Controls* [and other administrative controls].
> - *Passive SSCs are preferred over active SSCs.*
> - *Preventative controls are preferred over mitigative controls.*
> - *Facility safety SSCs are preferred over personal protective equipment.*
> - *Controls closest to the hazard may provide protection to the largest population of potential receptors, including workers and the public.*
> - *Controls that are effective for multiple hazards can be resource-effective."*

Following efforts to minimize hazardous materials, this control selection strategy translates into the following hierarchy of controls, listed from most preferred to least preferred:

(1) SSCs that are preventive and passive;
(2) SSCs that are preventive and active;
(3) SSCs that are mitigative and passive;
(4) SSCs that are mitigative and active;
(5) ACs that are preventive; and
(6) ACs that are mitigative.

An exception to this hierarchy is for confinement of radioactive materials. In such cases, active confinement ventilation is preferred over passive confinement systems. The Order also states that *"Alternate confinement approaches may be acceptable if a technical evaluation demonstrates that the alternate confinement approach results in very high assurance of the confinement of radioactive materials"* and includes a footnote acknowledging that *"The safety classification (if any) of the ventilation system is determined by the facility documented safety analysis."*

It is not always possible to strictly follow the hierarchy of controls stated above. In those cases, Section 3.3 of this Standard requires that a technical basis be provided that supports the controls selected. In such cases, where no SSCs are selected as part of the credited control strategy, the technical basis typically addresses consideration of potential upgrades or modification of engineered features such that the final suite of controls does not rely entirely on ACs.

A.9 Defense-in-Depth

Defense-in-depth is a fundamental approach to hazard control for nuclear facilities that is based on several layers of protection to prevent the release of radioactive or other hazardous material to the environment. These protective layers are generally redundant and independent of each other to compensate for unavoidable human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon.

The layers of protection supporting defense-in-depth principles generally follow a progression from accident prevention to accident management (e.g., detection and isolation), and finally accident mitigation as a last line of defense.

LAYER I: Normal safe operation of nuclear facilities relies upon a high level of design quality so that passive SSCs such as sealed buildings will prevent the release of radioactive or other hazardous materials. Passive features are complemented by competent operating personnel well trained in operations, maintenance procedures, and management of off-normal situations. Personnel competence translates into fewer malfunctions, failures, or errors and thus minimizes challenges to any layer of defense.

LAYER II: If the intended design is compromised by either equipment or operator error and abnormal operations ensue, the next layer of defense-in-depth is relied on. This layer is focused on accident management and can consist of automatic systems, or operator actions to return the system or process to within normal operating parameters.

LAYER III: The next layer of defense-in-depth provides for mitigation of the consequences of accidents. When an abnormal operating situation progresses to a more serious accident, consequences may be mitigated by a combination of passive features, automatic systems, and emergency response actions such as evacuation of workers or the public. Emergency response actions represent a final measure of protection for releases that cannot be prevented. Emergency response actions are not relied on as a substitute for implementation of defense-in-depth features and procedures within a site or facility.

DOE O 420.1C identifies specific attributes of defense-in-depth to be applied in the design of new nuclear facilities and major modifications to existing nuclear facilities. Many of these same attributes are appropriate for application to the hazard control strategy for existing legacy DOE non-reactor nuclear facilities in a tailored fashion using a graded approach. For example, an existing legacy hazard category 2 facility with chemical processing operations might not be able to demonstrate conservative design margins or the quality assurance pedigree of a new facility. However, it would still be expected to have multiple barriers such as effective confinement, monitoring and automatic response systems, and mitigative features that would minimize consequences of chemical releases. These layers of protection would be expected to consist primarily of engineered features. On the other hand, a hazard category (HC) 2 facility with simple operations (i.e., low operational complexity such as waste storage) or a HC-3 facility, while still expected to incorporate multiple layers of protection, could rely to a greater degree on ACs.

Defense-in-depth is primarily focused on providing additional protection against radiological releases to the public; however, defense-in-depth may also be applied to provide additional protection against chemical exposures, and for worker safety.

A.10 Evaluation Guideline

The concept of an evaluation guideline (EG) was developed to help DOE determine the rigor of controls (including defense-in-depth) needed to avoid the potential dose from an accident, the level of planning necessary to respond to given accidents, or the training needed for individuals that may be placed in situations where such doses might occur.

The EG is established for the purpose of identifying and evaluating the effectiveness of needed SC SSCs. The 25 rem TED EG is not a safety standard because it does not define an acceptable or unacceptable dose from an accident. The 25 rem EG is a criterion used by DOE to help identify and define what measures and controls are necessary. It has been used for many years in a number of ways in emergency response and nuclear safety areas. Although the value exceeds the operational annual safety dose limits for protection of the workers and the public, it is deemed appropriate for use as a planning and evaluation tool for accident prevention and mitigation assessment. The value is a fraction of the dose necessary to cause a prompt radiation-induced fatality. A prompt fatality would not occur if the whole body absorbed dose (received over a few hours) is less than 100 rads, therefore, the selection of the 25 rem value from a 50-yr dose commitment provides protection from acute radiation risk.

To put the EG dose in perspective, it is based on a 50-yr dose commitment that is five times the annual occupational limit for normal operations, but is equal to the federal guideline for allowable dose for emergency response workers in the case of life-saving. A full body CT scan results in doses between 5 and 10 rads; the EG is approximately equal to, or might be exceeded by, three full body CT scans. A nuclear stress test can result in doses from a rem to a few rem. In the United States, the dose from natural background averages about 0.36 rem per year and about 25 rem in a lifetime. Background doses for portions of the U.S. and the world significantly exceed these levels. However, these comparisons are not actually relevant to the EG because it is not a dose that is expected to be received, nor is it permitted. It is used for identifying and evaluating the need for SC SSCs that will avert or mitigate the accident. A major value of the EG is that it guides the decision making process toward a level of uniformity that could not exist without some form of quantitative benchmark.

The concept of "challenging the EG" (doses between 5 and 25 rem) accounts for potential uncertainties in the accident analysis methodology. The rationale used in determining whether SC controls are designated may include considerations such as the level of uncertainly related to assumptions used in the accident analysis (e.g., MAR, initiating or enabling energy sources), and the level of conservatism related to accident analysis assumptions (e.g., damage ratios supported by hard data vs. engineering judgment).

A.11 Safety Management Programs

Sections 830.204(b)(5) and (b)(6) of 10 C.F.R. Part 830 require that the DSA define characteristics of safety management programs necessary to ensure the safe operation of the facility. Program commitments such as radiation protection, maintenance, and quality assurance encompass a large number of details that are more appropriately addressed in specific program documents such as plans and procedures. The cumulative effect of these details, however, is

recognized as being important to facility safety; this is the rationale for a top-level program commitment becoming part of the safety basis.

The importance of the program commitments, which may be incorporated in TSRs as ACs, cannot be overestimated. The safety basis, however, includes only the top-level summary of program elements, and the program key elements (see Chapter 7, Section 7.X.3, "Key Element"), not the details of the program or its governing documents. Discrepancies in a program would not constitute violation of the safety basis unless the discrepancies were so extensive as to render the premises of the summary invalid.

Where safety management programs or program elements are relied on to ensure a safety function required by the safety analysis, it is important to capture this information in the programmatic sections of the DSA and include it in the TSR document as appropriate. Additionally, some engineered features within a facility will be identified in the hazard evaluation table that provide a safety function, yet are not elevated to SC or SS classification, either because unmitigated consequences are not significant or because other SSCs are sufficiently classified for the hazard event. These engineered features are still subject to the provisions of SMPs and programmatic commitments stated in the TSR. For example, facility systems or equipment that provide a preventive and mitigative function as noted in the DSA hazard evaluation would be subject to provisions of the Initial Testing, In-Service Surveillance, and Maintenance program. Gross discrepancies in application SMPs could violate the safety basis documented in the DSA, even if the controls are not designated SC or SS.

At a minimum, all aspects of defense-in-depth identified are covered within the relevant safety management programs, such as maintenance, quality assurance, committed to in the DSA. The details of that coverage are developed in the safety management program, rather than in the DSA. Facility operators are expected to have noted the relative significance of these engineered features and have provided for them in programs, in keeping with standard industrial practice, based on the importance of the equipment. It is the fact of coverage that is relevant to the facility safety basis. The details of this programmatic coverage, for example, the exact type of maintenance items and associated periodicities, are not developed in or part of the DSA.

DOE facilities that use and rely on site-wide safety support services, organizations, and procedures may summarize the applicable site-wide documentation if its interface with the facility is made clear. The DSA then notes whether the reference applies to a specific commitment in a portion of the referenced documentation or is a global commitment to maintaining a program.

A.12 Specific Administrative Controls

SACs are ACs identified in the safety analysis as a control needed to prevent or mitigate an accident scenario, and has a safety function that would be SS or SC if the function were provided by an SSC. SACs have safety importance equivalent to engineered controls that would be classified as SC or SS if the engineered controls were available and selected. DOE-STD-1186-2004, *Specific Administrative Controls*, provides an acceptable methodology for development and use of SACs. In general, SSCs are preferable to ACs or SACs due to the inherent uncertainty of human performance. However, SACs may be used to help implement a specific aspect of a

programmatic AC that is credited in the safety analysis and therefore has a higher level of importance. In some cases, supporting SSCs (e.g., instrumentation, controls, and equipment) may need to be identified and credited in conjunction with the SAC (see Section 3.3. of DOE-STD-1186-2004).

Discussions in DOE-STD-1186-2004 (e.g., Sections 1.6.2, Derivation of Hazard Controls in the DSA; 1.6.3, The Role of ACs in TSRs; 1.6.4, Application of ACs and SACs; and 2.1, Identification of SACs) for designating a SAC address a variety of factors, including safety management program considerations. The specificity of ACs within the DSA/TSR will vary depending on the severity of hazards, the complexity of the facility, and the AC's overall contribution to controlling potential accident consequences (i.e., primary or supplemental control). Depending on the situation, some ACs that perform specific preventive or mitigative functions for accident scenarios may be identified in hazard or accident analyses. These are more specific functions than implied by general commitments to safety management programs, and they may need to be raised to a higher importance level.

The criteria for designating an AC as a SAC include two conditions that need to be met: (1) ACs are identified in the safety analysis as a control needed to prevent or mitigate an accident scenario and (2) ACs have a safety function that would be SS or SC if the function were provided by an SSC. These criteria include two "may" considerations: (1) ACs may protect initial conditions and (2) ACs may provide the main mechanism for hazard control. For example, an AC may serve as the most important control or only control, and may be selected where existing engineered controls are not feasible to designate as SS SSCs. Therefore, when ACs are selected over engineering controls, and the AC meets the criteria for an SAC, the AC is designated as a SAC. Controls identified as part of a safety management program may or may not be SACs, based on the designations derived from the hazards and accident analyses in the DSA. Programmatic ACs are not intended to be used to provide specific or mitigative functions for accident scenarios identified in DSAs where the safety function has importance similar to, or the same as, the safety function of SC or SS SSCs – the classification of SAC was specifically created for this safety function – this generally applies to the key element of the safety management program that provides the specific preventive or mitigative safety function. Designating the entire safety management program as a SAC is not appropriate since that does not provide the specific credited safety function.

A number of safety management programs are identified in Section 3 of this Standard as generically included in the TSR document for worker safety. Specific elements of some safety management programs support SSC operation or reliability and provide a framework from which SACs may be derived. DSA hazard analyses are required to be comprehensive and, as such, identify specific elements of safety management programs for a variety of routine exposure or material handling issues. It is inappropriate to credit these safety management provisions in lieu of SSCs (for example, substitution of respirators for an SSC ensuring a breathable atmosphere) or SACs. However, crediting program elements together with SSCs or SACs may be necessary in some cases.

APPENDIX B: ADDITIONAL GUIDANCE FOR NEW FACILITIES AND MAJOR MODIFICATIONS

This Appendix provides additional guidance on preparing a documented safety analysis (DSA) for facilities that have been designed under the requirements of DOE-STD-1189-2008. Guidance is also provided on updating DSAs for major modifications of existing facilities.

The "safety in design" process for new facilities designed under the requirements of DOE-STD-1189-2008 (or successor document) provides for DOE's review and approval of a conceptual safety design report, a preliminary safety design report, and a preliminary documented safety analysis (PDSA) prior to construction. The information found in a PDSA is based on the design development process using "safety in design" concepts in conformance with DOE-STD-1189-2008. The safety design basis documented in the PDSA is preserved and brought forward within the DSA. The DSA will include, however, any changes made to the safety design basis since the approval of the PDSA and will address additional requirements for the DSA (i.e., beyond those for a PDSA).

New projects exempted from DOE-STD-1189-2008 may follow the approach outlined in this appendix in transitioning from a PDSA to an operational DSA. However, the specifics of this transition need to be developed in accordance with existing contracts and guidance from the Safety Basis Approval Authority for the project.

B.1 Transitioning from a PDSA to a DSA for a New Facility

The following steps are typically followed in developing a DSA from a PDSA:

- Update DSA Chapter 3 to capture and analyze hazards associated with facility operations, identify new initiating events that may require updating the accident analysis, and identify the significance of the safety management programs;
- Update DSA Chapter 4 to reflect attributes of the final design's safety SSCs and SACs;
- Complete development of DSA Chapter 5, in accordance with this Standard (Note: The PDSA covers preliminary TSR derivation only.);
- Add the description of safety management programs in accordance with this Standard;
- Review project records for changes in design or completion of incomplete design information since the latest version of the PDSA;
- Incorporate any changes not included in the PDSA, including the supporting information and justification for the changes (Note: DOE-STD-1189-2008 addresses the transition from final design to readiness for operations in Chapter 3, Section 3.5, "Construction, Transition, and Closeout.");
- Address any conditions of approval on the PDSA, such as completing identified design or safety analysis tasks; and
- Address any final facility attributes, not addressed in the PDSA, such as:
  - Government-furnished equipment not addressed during facility design;
  - Late changes in design resulting from problems or circumstances discovered during construction or checkout and testing activities; and

- Changes resulting from implementation of Chapter 6, Section 6.4, "Change Control for Safety Reports as Affected by Safety-in-Design Activities," of DOE-STD-1189-2008.

B.2 Updating a DSA for a Major Modification

For a major modification of an existing facility, the safety design basis established in the PDSA for the modification is required to be incorporated into the facility's DSA. The following steps may be followed in such cases:

- Update Chapter 2 of the existing DSA to include the changed facility description;
- Update Chapter 3 to include the hazard analyses, accident analysis, safety system identifications, and safety classification determinations associated with the modification from the PDSA;
- Update Chapter 4 to include, for any safety structure, system, and component (SSC) involved with the modification (including interfaces with existing safety SSCs), the design and design adequacy information from the PDSA;
- Update Chapter 5 for any changed or new technical safety requirement (TSR) associated with the modification; and
- Review the safety management program descriptions and revise as necessary to reflect the modifications.

An alternative to updating existing DSA chapters is to provide a DSA addendum that addresses the major modification.