**NOT MEASUREMENT SENSITIVE**

**DOE-STD-3009-YR**

**DRAFT**

**DOE STANDARD**

CRITERIA AND GUIDANCE FOR PREPARATION OF U.S.

DEPARTMENT OF ENERGY NONREACTOR

NUCLEAR FACILITY DOCUMENTED

SAFETY ANALYSIS



**U.S. Department of Energy AREA SAFT**

**Washington, DC 20585**

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

This document has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from ES&H Technical Information Services, U.S. Department of Energy, (800) 473-4375, fax: (301) 903-9823.

**Foreword**

1. This Department of Energy (DOE) Standard (STD) has been approved for use by DOE, including the National Nuclear Security Administration, and its 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 (HS-30)

Office of 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*, imposes requirements for the documented safety analyses (DSA) for nuclear facilities. This Standard represents an acceptable methodology for meeting the 10 C.F.R. 830 requirements for the preparation of a DSA for nonreactor nuclear facilities.

4. Throughout this Standard, the word “shall” denotes actions that are required to comply with 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. All “shall” statements must be met to fully implement the DSA development methodology in accordance with 10 C.F.R. 830.204.

5. This Standard is a significant revision to DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*, and is intended to clearly identify those portions of the Standard that are required to meet 10 C.F.R. 830 requirements for DSA preparation methodology (unless DOE approval for an alternative methodology is granted). This Standard also updates some criteria to reflect lessons learned since its last revision.

6. With one exception, for existing facilities with approved DSAs there is no need to implement this revision of DOE-STD-3009 but Program Office may choose to do so for update of a facility (or site) DSA if desired. The exception is that Section 3.3.1, *Safety Class Controls,* shall be implemented for any facility for which safety class controls have not been implemented to prevent or mitigate postulated accident doses to below the public evaluation guideline.

7. If a Program Office chooses to use this DOE-STD-3009 revision for update of an existing DSA, then it should be implemented in a holistic fashion. The goal of this revised Standard is to provide clearer criteria and guidance to support more effective and consistent DSA development based upon lessons learned with implementing DOE-STD-3009. Any impact on the safety control set needs to be carefully examined to ensure safety margins are appropriately maintained.

Contents

[Definitions v](#_Toc343005610)

[Abbreviations and Acronyms x](#_Toc343005611)

[Section 1. Introduction 1](#_Toc343005612)

[1.1 PURPOSE 1](#_Toc343005613)

[1.2 APPLICABILITY 1](#_Toc343005614)

[1.3 COMPLIANCE WITH DSA PREPARATION METHODOLOGY 1](#_Toc343005615)

[1.4 OVERVIEW OF THE STANDARD 1](#_Toc343005616)

[Section 2. DSA Preparation Process and Application of the Graded Approach 2](#_Toc343005617)

[2.1 DSA PREPARATION PROCESS 2](#_Toc343005618)

[2.2 APPLICATION OF THE GRADED APPROACH 5](#_Toc343005620)

[Section 3. Hazard Analysis, Accident Analysis and Hazard Control Selection Criteria and Guidance……………………. 6](#_Toc343005621)

[3.1 HAZARD ANALYSIS 6](#_Toc343005622)

[3.1.1 Hazard Identification 6](#_Toc343005623)

[3.1.2 Hazard Categorization 7](#_Toc343005624)

[3.1.3 Hazard Evaluation 8](#_Toc343005625)

[3.2 ACCIDENT ANALYSIS 11](#_Toc343005626)

[3.2.1 Evaluation Basis Accident Selection 11](#_Toc343005627)

[3.2.2 Unmitigated Analysis 13](#_Toc343005628)

[3.2.3 Mitigated Analysis 14](#_Toc343005629)

[3.2.4 Accident Consequence Calculation Overview 14](#_Toc343005630)

[3.2.5 Source Term Analysis 15](#_Toc343005631)

[3.2.6 Dose Consequence Analysis 16](#_Toc343005632)

[3.3 HAZARD CONTROL IDENTIFICATION AND DESIGNATION 18](#_Toc343005633)

[3.3.1 Safety Class Controls 18](#_Toc343005634)

[3.3.2 Safety Significant Controls 19](#_Toc343005635)

[3.3.3 Other Hazard Controls 21](#_Toc343005636)

[3.4 Design of Hazard Controls 21](#_Toc343005637)

[3.5 Accident Frequency Calculation Overview 22](#_Toc343005638)

[3.6 Planned Design and Operational Safety Improvements 22](#_Toc343005639)

[3.7 References 23](#_Toc343005640)

[Section 4. DSA Format and Content 25](#_Toc343005641)

[DSA [EXECUTIVE SUMMARY] 25](#_Toc343005642)

[DSA [CHAPTER 1: SITE CHARACTERISTICS] 27](#_Toc343005643)

[DSA [CHAPTER 2: FACILITY DESCRIPTION] 30](#_Toc343005644)

[DSA [CHAPTER 3: HAZARD AND ACCIDENT ANALYSES AND CONTROL SELECTION] 32](#_Toc343005645)

[DSA [CHAPTER 4: SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS] 38](#_Toc343005646)

[DSA [CHAPTER 5: DERIVATION OF TECHNICAL SAFETY REQUIREMENTS] 45](#_Toc343005647)

[DSA [CHAPTER 6: PREVENTION OF INADVERTENT CRITICALITY] 48](#_Toc343005648)

[DSA [CHAPTER 7: SAFETY MANAGEMENT PROGRAMS] 50](#_Toc343005649)

[Appendix A: Technical Background of Key DSA Concepts 1](#_Toc343005650)

[Appendix B: DSA Development for a New Facility and for Major Modifications to Existing Facilities Designed Under DOE-STD-1189 1](#_Toc343005651)

# 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 for which there is a potential for a release of radioactive or other hazardous material and/or exposure to a predefined receptor.

**Accident analysis.** For the purposes of implementing this Standard, accident analysis is the process of deriving (and analyzing) a set of formalized evaluation basis accidents from the hazard analysis that is used to:

* Indicate the need for safety class control designation for public protection;
* Indicate the need for safety significant controls to support safety class controls for public protection, and, in some cases, for worker protection; and
* Select specific controls for designation as safety class or safety significant.

**Administrative controls (ACs).** Provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of a facility. [10 C.F.R. 830]

**Beyond design/evaluation basis accident.** An accident (e.g., fire, earthquake, spill, or explosion) 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, including surveillance and maintenance, decontamination, and dismantlement.

**Decontamination.** The removal or reduction of residual radioactive and other hazardous materials by mechanical, chemical, or other techniques to achieve a stated objective or end condition.

**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).** An accident explicitly considered as part of the facility design for a new facility. The facility with its collection of controls is specifically designed to prevent and/or mitigate all DBAs.

**Evaluation basis accidents (EBAs).** The representative and unique accidents evaluated in the accident analysis for the purposes of determining the need for safety class controls in an existing facility where DBAs were not utilized for this purpose.

**Evaluation guideline (EG).** The criterion for the dose of ionizing radiation (total effective dose equivalent) that the safety analysis evaluates against. The EG is established for the purpose of identifying the need for and evaluating safety class controls. A co-located worker threshold is also established that can be used to identify the need for and to evaluate safety significant 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.

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. However, specific operations and processes independent of buildings or other structures (e.g., waste retrieval and processing, waste burial, remediation, groundwater or soil decontamination, decommissioning) are also encompassed by this definition.

**Fissionable materials.** A nuclide capable of sustaining a neutron-induced chain reaction (e.g., uranium-233, uranium-235, plutonium-238, plutonium-239, plutonium-241, neptumium-237, americium-241, and curium-244). [10 C.F.R. 830]

**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 nonradiological hazards; and
* Any other relevant factor. [10 C.F.R. 830]

**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]

**Hazard analysis.** The determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by the assessment of hazardous situations associated with a process or activity. Largely qualitative techniques are used to pinpoint weaknesses in design or operation of the facility that could lead to accidents. The hazard analysis examines the complete spectrum of potential accidents that could expose members of the public, on-site workers, facility workers, and the environment to 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. 830.

**Hazard control**. 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]

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

**Hazardous material.** Any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health. Candidate hazards include radioactive materials, hazardous chemicals, and flammable liquids and gases as defined below:

* Occupational Safety and Health Administration in 29 C.F.R. 1910.1200, *Occupational Safety and Health Standards, Hazard Communication*, and 29 C.F.R. 1910.1450, *Occupational Safety and Health Standards, Occupational Exposure to Hazardous Chemicals in Laboratories*;
* Any material assigned a reportable quantity value in 40 C.F.R. 302, *Designation, Reportable Quantities and Notification*, Table 302.4;
* Level of concern quantities in Environmental Protection Agency’s *Technical Guidance for Hazards Analysis-Emergency Planning for Extremely Hazardous Substances*; or
* Materials rated as 3 or 4 by the National Fire Protection Association (NFPA) in NFPA704, *Standard System for the Identification of the Fire Hazards of Materials for Emergency Response*.

**Initiating event.** The first event (e.g., an earthquake or an incipient fire) in a sequence or chain of one or more events in an accident (or equivalently, hazard or accident 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]

**Limiting control settings (LCSs).** Settings on safety systems that control process variables to prevent exceeding a safety limit. [10 C.F.R. 830]

**Mitigative feature.** Any structure, system, or component that serves to mitigate the consequences of a release of hazardous materials in a hazard or accident scenario. [DOE-STD-1027, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*].

**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]

**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. 830. [10 C.F.R. 830]

**Preventive feature.** Any structure, system, or component that serves to prevent an accident scenario from occurring.

**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*.

**Programmatic.** A reference to facility-specific programs or site-wide programs necessary to ensure the safe operation of a facility. Radiation protection, hazardous material protection, quality assurance, training, document control, and emergency preparedness are examples of programs that provide programmatic controls to ensure safe operations.

**Public.** All individuals outside the DOE site boundary.

**Risk.** The quantitative or qualitative expression of possible loss that considers both the probability 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]

**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]

**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]

**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]

**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]

**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]

**Site boundary.** A well-marked boundary within which the owner and operator can exercise control without the aid of outside authorities. A public road or waterway traversing a DOE site is considered to be within the DOE site boundary if, when necessary DOE or the site contractor has the capability to control the road during accident or emergency conditions.

**Specific administrative control (SAC).** A formal, documented action or activity (hazard control) needed to prevent or mitigate an accident scenario that has a safety function that would be safety significant or safety class if the function were provided by a SSC.

**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]

# 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

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

G Guide

HAZOP Hazard and Operational Analysis

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 Off-site Individual

NRC Nuclear Regulatory Commission

OSHA Occupational Safety and Health Administration

PDSA Preliminary Documented Safety Analysis

PRA Probabilistic Risk Assessment

RF Respirable Fraction

SAC Specific Administrative Control

SC Safety Class

SL Safety Limit

SRID Standards and Requirements Identification Document

SS Safety Significant

SSC Structures, Systems, and Components

STD Standard

TEDE Total Effective Dose Equivalent

TEEL Temporary Emergency Exposure Limit

TPQ Threshold Planning Quantity

TQ Threshold Quantity

TSR Technical Safety Requirement

# Section 1. INtroduction

## 1.1 PURPOSE

This Department of Energy Standard (STD), DOE-STD-3009 describes a Documented Safety Analysis (DSA) preparation method 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. 830, *Nuclear Safety Management,* Subpart B, Appendix A, Table 2.

## 1.3 COMPLIANCE WITH DSA PREPARATION METHODOLOGY

Compliance with the DSA preparation methodology contained in this Standard is achieved by implementing all of the “shall” statements of this Standard.

This revision to DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*, is intended to clearly identify the requirements that must be met to comply with 10 C.F.R. 830.204 in the DSA preparation methodology identified in Table 2 of Appendix A of 10 C.F.R. 830 (unless DOE grants approval for an alternative methodology). It also updates some criteria to reflect lessons learned since the last revision of DOE-STD-3009.

With one exception, for existing facilities with approved DSAs there is no need to implement this revision of DOE-STD-3009 but Program Office may choose to do so for update of a facility (or site) DSA if desired. The exception is that Section 3.3.1, *Safety Class Controls,* shall be implemented for any facility for which safety class controls have not been implemented to prevent or mitigate postulated accident doses to below the public evaluation guideline (EG).

If a Program Office chooses to use this DOE-STD-3009 revision for update of an existing DSA then it should be implemented in a holistic fashion. The goal of this revised Standard is to provide clearer criteria and guidance to support more effective and consistent DSA development based upon lessons learned with implementing   
DOE-STD-3009. Any impact on the safety control set needs to be carefully examined to ensure safety margins are appropriately maintained.

## 1.4 OVERVIEW OF THE STANDARD

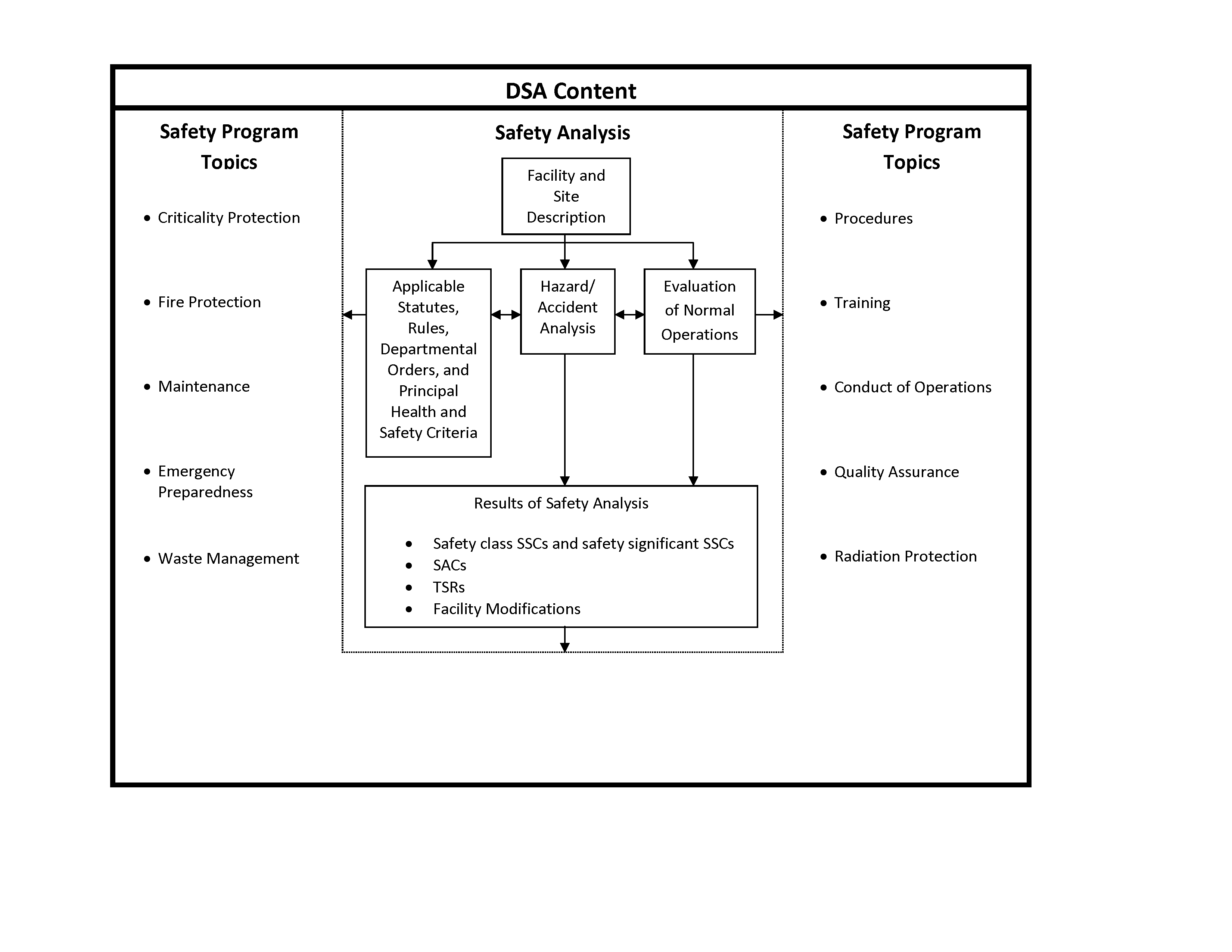
Section 2 discusses the overall DSA preparation process and application of the graded approach. Section 3 provides detailed criteria and guidance for implementing the fundamental tasks of hazard analysis, accident analysis, and hazard control selection. Section 4 outlines the products, content, and format of the DSA.

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

# Section 2. DSA Preparation Process and Application of the Graded Approach

## 2.1 DSA PREPARATION PROCESS

An overview of the content of a DSA in relation to the preparation process is shown in Figure 1. 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 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.



**Figure 1: DSA Scope and Integration**

The DSA preparation process is illustrated in Figure 2. 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 select an acceptable level of detail.

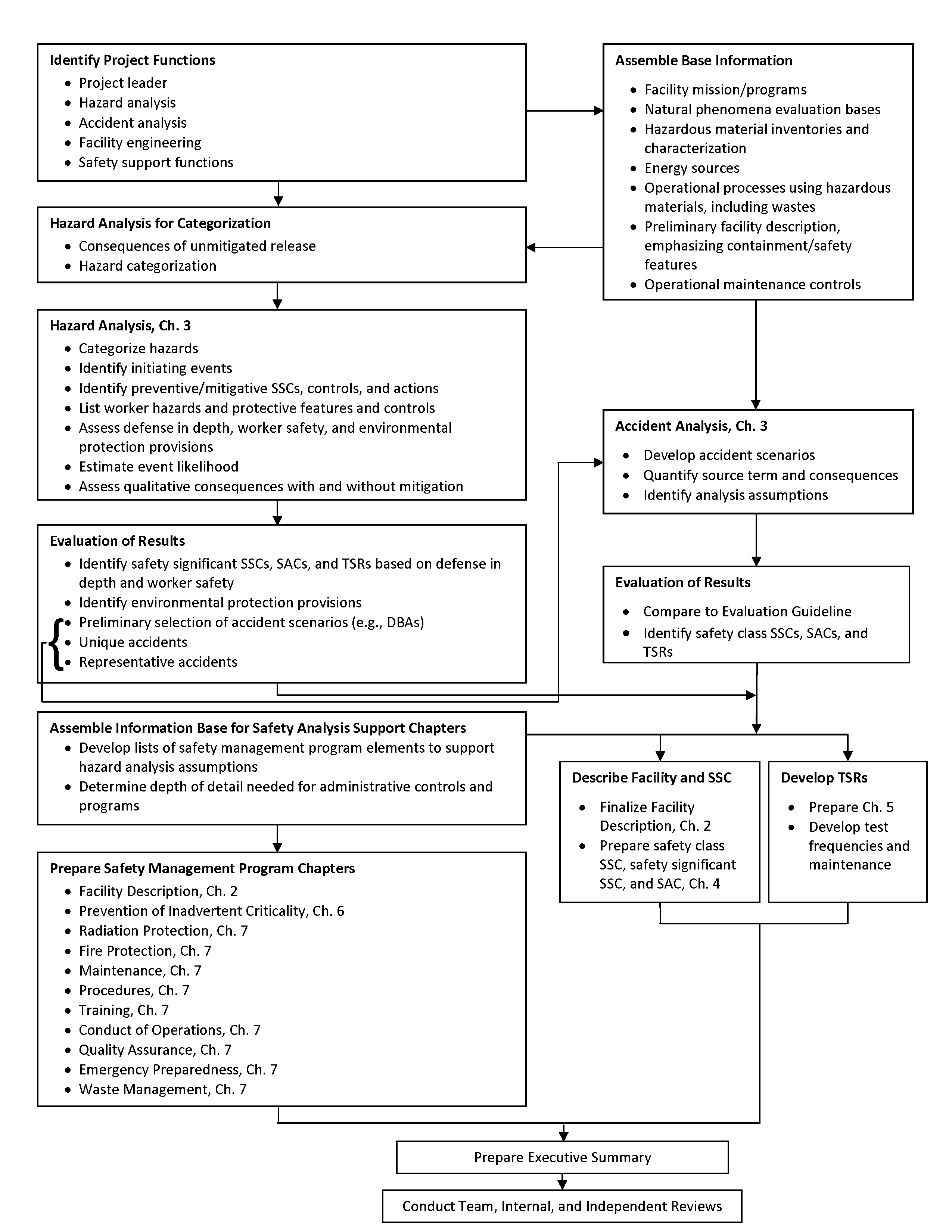
The foundation for effectively preparing a DSA is the assembly and integration of an experienced preparation team. The size and makeup of the team depend on the magnitude and type of facility hazards and the complexity of the processes that the DSA must address. In determining the makeup of the preparation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

In general, the safety analysis team should include, as a minimum, individuals experienced in process hazard and accident analyses, facility systems engineers, and process operators. Individuals with experience in specific subject matters, 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 ensured through integration of the required tasks.

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

* Identify site characteristics;
* Identify facility characteristics;
* Perform hazard analysis;
* Perform accident analysis;
* Identify and classify hazard controls;
* Describe the hazard controls;
* Derive technical safety requirements (TSRs);
* Summarize criticality safety; and
* Summarize safety management programs.



## Figure 2: DSA Preparation Process

## 2.2 APPLICATION OF THE GRADED APPROACH

10 C.F.R. 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 DSA preparation, as well as 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, 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 nonradiological hazards; and,
* Any other relevant factor.

10 C.F.R. 830 provides for exercising judgment in developing the DSA based on the nature of the facility in relation to these factors. For example, hazard category 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 hazard category 2 facility. In addition, facilities with short operational lives (or other compelling circumstances) should consider the appropriateness of using DOE-STD-3011, *Guidance for Preparation of Basis for Interim Operation (BIO) Documents*, to meet the requirements of 10 C.F.R. 830. On the opposite end of the spectrum, a complex hazard category 1 facility that is just going into operation requires extensive analysis and highly detailed documentation.

The application of the graded approach may allow for much simpler analysis and documentation for some facilities. For low-hazard hazard category 3 facilities, 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 a few specific administrative controls (SACs) or safety significant structures, systems, and components (SSCs). Consequently, not all facilities will need to address all of the topics for the DSA listed in this Standard, and if a facility has proper technical bases, it may be able to omit some topics or reduce the level of detail that would otherwise be required of hazard category 1 or 2 facilities.

Thus, application of the graded approach will generally lead to simpler analysis and documentation in DSAs for hazard category 3 facilities and facilities with short operational lives or one-of-a-kind experiments, including those conducted remotely or deep underground. 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. As a minimum, the scope of a DSA for a simple hazard category 3 facility could address the following three elements in a simplified fashion:

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

# Section 3. Hazard Analysis, Accident Analysis and Hazard Control Selection Criteria and Guidance

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 that are needed to provide protection for workers, the public, and the environment. This section provides detailed criteria and guidance for performing these three elements. An overview of these three elements is shown in Figure 3.

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 is included in Section 4.

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

## 3.1 HAZARD ANALYSIS

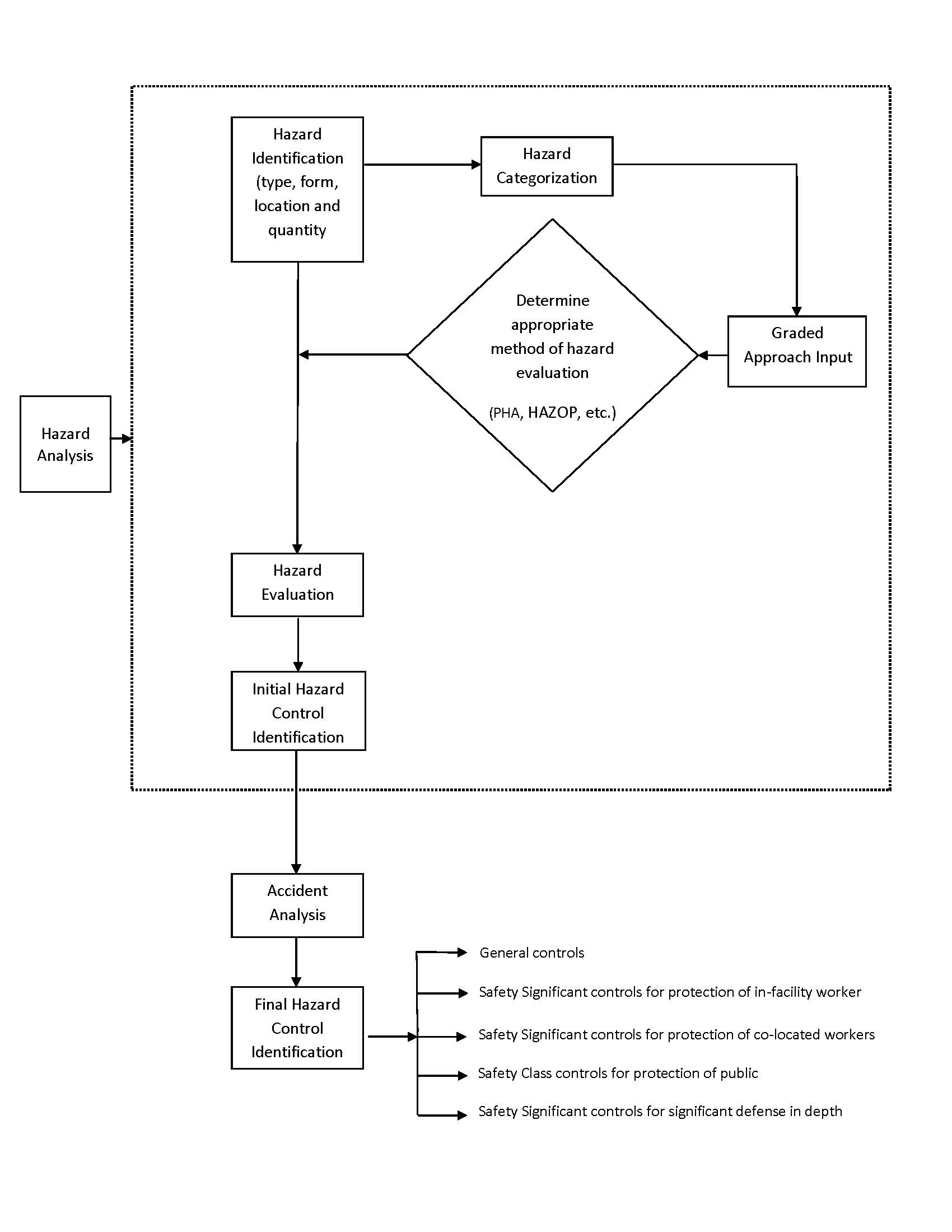
The initial analytical effort for all facilities is a hazard analysis that systematically identifies facility hazards, potential accidents, and controls through hazard identification and hazard evaluation. The hazard analysis focuses on thoroughness of evaluating the complete spectrum of hazards and 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 hazard identification methodology shall ensure the identification of all hazardous materials and energy sources associated with facility processes or associated operations (e.g., fissionable materials and waste handling) that could result in an accidental criticality, release of the material or exposure of personnel to the hazard. Standard industrial practices for hazard identification, such as that described in the Center for Chemical Process Safety’s *Guidelines for Hazard Evaluation Procedures* (Third Edition, American Institute of Chemical Engineers, 2008), may be used.

Bounding inventory values shall be utilized as obtained from flowsheet inventories, historical inventories, 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.

DSAs are not intended to analyze standard industrial hazards that make up a large portion of   
10 C.F.R. 851, *Worker Safety and Health Program*, unless these hazards are initiators to a release of hazardous material. That Rule, along with other national consensus codes and/or standards, regulates practices associated with these hazards. See Appendix A, Section A.1 of this Standard for further discussion.



**Figure 3: Methodology Overview**

### 3.1.2 Hazard Categorization

Hazard identification provides the basis for hazard categorization. The facility hazard category shall be consistent with DOE-STD-1027, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*.

### 3.1.3 Hazard Evaluation

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

#### **3.1.3.1 General**

The hazard evaluation shall be a systematic assessment of all of the facility hazards and the controls that can prevent or mitigate the hazards. The hazard evaluation shall evaluate all modes of operation, including startup, shutdown, and abnormal testing or maintenance configurations, and shall include the potential for both equipment failure and human error. 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 technique(s). 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 are appropriate for analyzing many hazard category 3 facilities, as well as simple hazard category 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 the Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures*.

As part of the hazard evaluation, an unmitigated scenario shall be evaluated for each initiating event assuming the absence of controls.[[1]](#footnote-1) The consequences and the frequency of the unmitigated scenario shall be estimated (utilizing qualitative and/or semi-quantitative techniques). Hazard scenario consequence estimates shall address potential impacts to facility workers, co-located workers, and the public. If it is clear from this analysis that the consequences will far exceed the public EG, the actual consequences need not be calculated because the need for SC controls has already been identified.

The controls (SSCs, administrative and/or programmatic) that can prevent or mitigate the hazard shall be clearly identified for each initiating event and the effectiveness of the controls (i.e., capability to prevent or mitigate the event) shall be evaluated. Hazard control identification is further discussed in Section 3.3 of this Standard.

The results of hazard evaluation should be provided in a table that presents:

* The hazard (initiating event and scenario);
* The potential consequences of the hazard; and,
* Preventative and mitigative controls.

Hazard ranking/binning may be used to support the hazard evaluation and hazard control identification process (See Appendix A, Section A.2 of for background information on hazard ranking/binning). If hazard ranking/binning is used, the following consequence and frequency thresholds are recommended.

Consequence Threshold

* Public consequence thresholds:
  + High: dose > 25 rem total effective dose equivalent (TEDE); exposure > acute exposure guideline level (AEGL)-2/emergency response planning guidelines (ERPG)-2/temporary emergency exposure limit (TEEL)-2
  + Moderate: 25 rem > dose >5 rem
  + Low: 5 rem > dose > 0.5 rem
* Co-located worker consequence thresholds[[2]](#footnote-2)):
* High: dose > 100 rem TEDE; exposure > AEGL-3/ERPG-3/TEEL-3
  + Moderate: 100 rem > dose > 25 rem
  + Low: 25 rem > dose >5 rem
  + Negligible: dose <5 rem
* Facility worker consequence thresholds (may be qualitatively estimated):
  + High: fatality
  + Moderate: serious injury, or significant radiological or chemical exposure Low: negligible impacts.

Note: both High and Moderate are considered to be significant as utilized for safety significant control classification purposes for facility workers.

Frequency thresholds (see Table 1)

**Table 1: Qualitative Likelihood Classification Table**

|  |  |  |
| --- | --- | --- |
| **Description** | **Frequency range (/year)** | **Definition** |
| Anticipated | 10-1>frequency>10-2 | Events that may occur several times during the lifetime of the facility (incidents that commonly occur). |
| Unlikely | 10-2>frequency>10-4 | Events that are not anticipated to occur during the lifetime of the facility. Natural phenomena of this probability class include: Uniform Building Code-level earthquake, 100-year flood, maximum wind gust, etc. |
| Extremely Unlikely | 10-4>frequency>10-6 | Events that will probably nor occur during the life cycle of the facility. |
| Beyond Extremely Unlikely | frequency<10-6 | All other accidents. |

Note that detailed probabilistic calculations are neither expected nor required. If probabilistic calculations are utilized the process for performing high quality quantitative risk assessments identified in the draft DOE Standard, *Development and Use of Probabilistic Risk Assessments in Department of Energy Nuclear Safety Applications,* issued in December 2010 for interim use and comment.

#### **3.1.3.2 Criticality Hazards**

Criticality safety controls are established as part of the hazard evaluation/Criticality Safety Evaluation process performed per ANS 8.1 and DOE Standard 3007. In addition, as part of the DSA development process, criticality hazards shall be screened for inclusion into the DSA.  Situations for when a particular scenario and associated control(s) should be explicitly documented in the DSA hazard evaluation include:

* Events where consequences (from the criticality itself or subsequent impact to hazardous material) to a co-located worker exceed 100 rem or consequences to the public exceed the EG; and
* Processes that do not incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible;
* Processes in which an active engineered control(s) are required by the NCS analysis to ensure subcriticality.

Other controls that have significant safety importance as determined by the NCS analysis process (e.g., controls that have broad applicability across multiple fissionable material operations with the potential of defeating NCS defense in depth, or the use of a Criticality Accident Alarm System) should also be documented in the DSA hazard evaluation.

For criticality hazard scenarios screened for inclusion, the DSA shall include simple summaries of the scenarios and identify the preventive and mitigative features that were identified though the Criticality Safety Evaluation process. If such scenarios are included in the hazard tables, no frequency estimates are required because of the differences in hazard evaluation technique.

In addition to the screening, a summary describing the criticality hazards and the associated controlled parameters shall be presented in Chapter 6 of the DSA. This summary may group common controls and state control limits in such a way to reduce the need for frequent DSA updates.

The DSA hazard evaluation shall present the unmitigated dose consequence resulting from a criticality accident unless it has been determined that criticality is not credible.

#### 3.1.3.3 Chemical Hazards

As part of the hazard evaluation process, chemical hazards shall be evaluated. The first step of the chemical hazard evaluation process should be a screening of standard industrial hazards and low hazard chemicals. Appendices B and C of DOE-STD-1189 provide an acceptable approach for screening and evaluating consequences associated with hazardous chemicals. Evaluation of the facility worker impacts should only be performed in a qualitative manner. Chemicals that are not excluded by the screening process shall be evaluated utilizing the general method described in Section 3.1.3.1. See Appendix A, Section A.4 for further discussion of chemical hazards.

## 3.2 ACCIDENT ANALYSIS

Accident analysis entails the formal characterization of a limited subset of accidents referred to as Evaluation Basis Accidents (EBAs)[[3]](#footnote-3) and the calculation of the approximate and reasonably conservative consequences of these events. Appendix A, Section A.5 discusses the concept of EBAs.

For SC classification purposes, these consequences shall be compared to the 25 rem TEDE EG. If the EG is exceeded, safety class controls shall be identified to prevent or mitigate the event (see Section 3.3.1 for those rare instances where no viable control strategy can prevent doses in one or more EBAs from exceeding the public EG). If the EG is challenged (i.e., calculated doses exceed 5 rem), then consistent with the approach adopted in Appendix A, Section A.2.1, of DOE-STD-1189, safety class controls should be considered. The EG is discussed further in Appendix A, Section A.6.

For SS classification purposes, an evaluation of co-located worker consequences is also required and may be performed as part of either the hazard or accident analysis. This analysis is performed consistent with that for offsite receptors except for atmospheric dispersion analysis. Section 3.3.2 addresses dose consequence analysis for co-located workers primarily relating to atmospheric dispersion and receptor location (which is based upon DOE-STD-1189, Appendix A).

The effectiveness of mitigative safety class controls is determined by performing a *mitigated* dose calculation. The assumptions and process for calculating mitigated and unmitigated dose are described in the following sections.

### 3.2.1 Evaluation Basis Accident Selection

EBAs are selected from:

* Operational accidents which are caused by initiators internal to the facility;
* Natural events such as earthquakes, floods, tornadoes, etc.; and,
* Man-made external events such as an aircraft crash.

EBAs are derived from the spectrum of hazard scenarios developed in the hazard analysis. Two types of EBAs shall be defined for further analysis: (1) representative and (2) unique. EBAs only need to be developed for consequences that have the potential to challenge the EG.

Representative EBAs bound a number of accidents with a similar control set (e.g., the worst fire, or fires, or a number of fires). At least one bounding accident from each of the major types determined from the hazard analysis (fire, explosion, spill, etc.) shall be selected. The word “bounding” is intended to refer to the physical parameters of the accident scenarios, such as the material at risk (MAR), the combustible loading limits, and the maximum explosion pressure.

Unique EBAs are those events that may be bounded by other events but have their own unique control set. For example, suppose that four explosions that may exceed the EG in unmitigated release can occur in a facility. Three explosions are functionally identical and have the same control set. For accident analysis, it is acceptable to select the bounding representative EBA for those three scenarios. Suppose, however, that the fourth explosion, though slightly smaller in consequence, is unrelated to the other three and has its own unique control set. To neglect that explosion for the representative case previously discussed could result in a failure to identify SC controls. The fourth explosion is, therefore, a unique EBA that should also be selected for accident analysis.

Representative EBAs shall be defined such that:

* The MAR assumed in the unique EBAs reflects the maximum MAR available to the represented hazard scenarios;
* The control(s) applicable to the EBA are similar in kind and will perform the same as the control sets of the represented hazard scenarios; and,
* The accident environments derived for the EBA controls reflect the accident environments of the represented hazard scenarios.

The only events that can be excluded from accident analysis are: (1) operational events that are not physically possible in an unmitigated evaluation; (2) natural phenomena initiators of greater magnitude than those required by DOE O 420.1C (and its associated natural phenomena hazard implementation standards); and (3) external man-made accidents or natural phenomena initiators with a cutoff frequency of 10-6 per year, conservatively calculated.

### 3.2.2 Unmitigated Analysis

An unmitigated consequence analysis shall be performed that considers material quantity, form, location, disperability, and interaction with available energy sources. The analysis shall not assume the availability of safety features (e.g., ventilation systems, fire suppression), except for passive SSCs that are accessed to survive the accident conditions. The initial conditions and all assumptions for the analysis shall be documented and evaluated to determine if controls[[4]](#footnote-4) need to be put in place to ensure the evaluation will remain valid for the lifetime of the facility. Section 11 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 scenario, and they may also affect the magnitude of the resultant consequences. These assumptions, however, shall be protected at a level commensurate with their importance (e.g., 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 criteria shall be followed:

* Take no credit for active safety controls, such as ventilation filtration systems in the case of a spill or fire suppression in the case of a fire;
* Take credit for passive safety controls only if assessed to survive accident conditions in order to define a physically meaningful scenario. 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 not be assumed that the contents have dropped in an uncontained manner. Similarly, if the facility has permanently-installed resilient flooring that prevents an undesired consequence of such a drop, an assessment of the drop against some other non-resilient surface is not meaningful. However, it is important to note that such defining assumptions will warrant some level of safety SSC designation to ensure that the assumptions remain valid in the future. In the above examples, the container and the flooring warrant designation as SS or SC design features depending upon whether the container design and construction is critical to the validity of the assumption and consequences of the design feature not performing as assumed;
* Take no credit for passive safety controls that produce a leakpath reduction in source term, such as building filtration;
* Assume the availability of passive safety controls that are not affected by the accident scenario. 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,
* Evaluate facility-wide, secondary, and common cause events that are directly caused by natural events, such as earthquake-induced fires and explosions;
* Do not credit operator intervention actions that may abort the progression of the event, that is, assume the event occurs with no intervention.
* Take no credit for administrative controls, SACs, or safety management programs in the unmitigated analysis. MAR values may be considered initial conditions (see Appendix A.11)

The unmitigated consequence calculation determines the need for SS and SC-designated controls and provides the framework for designating these controls. If the unmitigated consequences of a release scenario exceed the public EG value, SC controls shall be identified as specified in Section 3.3.1.

### 3.2.3 Mitigated Analysis

A mitigated analysis shall be performed to determine the effectiveness of SS and SC controls for co-located workers and the public identified to mitigate the consequences of the EBA (see Section 3.3 for a discussion of the SC selection process). This analysis should be the same as the unmitigated analysis except for the fact that consequences are estimated with SC controls in place (for consequences to the public) and with SC and SS controls in place (for consequences to workers).

The SC mitigative SSC(s) shall reduce the unmitigated consequences below the EG. Section 3.3.1 discusses a process that shall be followed in rare cases that this cannot be achieved. Further, it is DOE’s goal that the combined effectiveness of the suite of controls for a given accident will be mitigated such that the resulting public consequences would be well below of the EG[[5]](#footnote-5). The information shall be presented in Section 3.4.4.X.5 of a DSA where the effect of hazard controls is shown.

As with the unmitigated case, the analysis recognizes the physical design of facility SSCs. Facilities should be analyzed as they exist when quantifying meaningful release mechanisms. For example, if liquid hazardous material is brought into a facility in steel piping and stored in steel tanks, it is not meaningful to disregard the existence of these physical features in analysis. Disregarding the physical reality of design in an effort to insert conservatism can result in expending resources on what are essentially fictitious scenarios and is, therefore, counterproductive.

### 3.2.4 Accident Consequence Calculation Overview

Accident 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 determined. As with every phase of the analysis, the effort expended is a function of the estimated consequence.

Calculations shall be made such that input parameters are technically justified (i.e., as described in Section 3.2.5 and 3.2.6), and underlying assumptions and the methodology used in their selection do not result in unrealistic accident scenarios.

All assumptions made in the accident analysis shall be well-founded, defendable, and protected at a level commensurate with their importance (e.g., TSR provisions or safety basis documentation). The DSA shall present information at a level sufficient for review and approval. Referencing an auditable trail of information as part of the controlled supporting documentation is acceptable if the reference is configuration-controlled with respect to the DSA.

The two main steps in the accident dose calculation are: (1) the determination of the *source term* (the amount of radioactive or other hazardous material that is released from the facility); and, (2) the *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 conversion factors, or toxicity of other hazardous materials). These two steps are described in Sections 3.2.5 and 3.2.6.

### 3.2.5 Source Term Analysis

The radioactive airborne source term is typically estimated 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). These parameters are discussed in detail in DOE-HDBK-3010, *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*.

**Material at Risk**

The MAR is the bounding quantity of hazardous material that is available to be acted on by a postulated accident. The MAR may range from the total inventory in a facility or a subset 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. While DOE-STD-1027 excludes material in qualified containers from consideration for the purposes of hazard classification, the existence of such material shall be acknowledged in the DSA and excluded from the source term for a particular event scenario only if the containers can be shown to perform their safety functions under the 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 a standard or technical basis for a different value. For example, DOE-STD-5506, *Preparation of Safety Basis Documents for Transuranic (TRU) Waste Facilities*, contains specific recommendations for DRs to be used in existing transuranic waste operations.

**Airborne Release Fraction and Respirable Fraction**

Bounding estimates for radionuclide ARFs and RFs for a wide variety of MAR and release phenomena are presented in DOE-HDBK-3010 and shall be used unless there is a standard or technical basis for a different value. In cases where direct shine may contribute significantly to dose, that contribution should be evaluated without the use of the RF.

ARFs and RFs shall be selected based on physical conditions and stresses anticipated during accidents. DOE-HDBK-3010 defines bounding ARFs and RF mechanisms 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 passing from a glovebox, the fraction passing from a room, or the fraction passing through filtration vis-à-vis door leakage. 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 conservative parameters, such that the overall LPF would be conservative.

### 3.2.6 Dose Consequence Analysis

The dose estimate is that received during a 2-hour exposure to the plume. The assumed length of exposure may be extended to 8 hours for source term release durations that exceed 2 hours. The exposure period begins when the plume reaches the Maximally-exposed Off-site Individual (MOI). The dose pathways to be considered are inhalation, direct shine, and ground shine. 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 radioactivity in liquid form to water pathways, should be considered. In this case, real potential uptake locations should be the evaluation points.

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 waste storage, the surface and groundwater pathways may be more important. However, in these cases, the accident releases usually would be expected to develop more slowly than the airborne releases, and more time would be available for implementing preventive and mitigative measures. Therefore, the emphasis on SC controls, in terms of immediate availability and operation, is not generally applicable to these pathways.

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

**Receptor Location**

For the purposes of comparison to the public EG, the comparison point shall be the location of a theoretical MOI. This location is typically at the site boundary location with the highest directionally dependent dose based on a ground release, but it could be beyond the DOE site boundary if an elevated plume is not at ground level at the site boundary. In such cases, the point of maximum exposure is typically where the plume reaches ground level. An assessment of any changes in the site boundary and their potential effects on the safety SSC designation should be performed in association with the required update of the DSA for a facility. Privatization and site turnover initiatives may affect these determinations. The directional dependence of the distance for the receptors can 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 minimum distance to the site boundary within a 45-degree sector centered on the compass direction of interest. For elevated plumes that reach ground level beyond the site boundary, the directionally dependent distance should be the distance to the point where the plume reaches ground level (maximum value).

**Atmospheric Dispersion**

Accident phenomenology may be modeled assuming straight-line Gaussian dispersion characteristics, applying meteorological data representing a one-hour average for the duration of the accident. The Nuclear Regulatory Commission’s (NRC) Regulatory Guide 1.23, *Meteorological Monitoring Programs for Nuclear Power Plants*, describes acceptable means of generating the meteorological data upon which dispersion is based. More guidance on appropriately defining stability classes can be found in the Environmental Protection Agency’s (EPA) EPA-454/R-99-005, *Meteorological Monitoring Guidance for Regulatory Modeling Applications*. These two guidance documents should be evaluated for their appropriateness. Dispersion models based on straight-line Gaussian dispersion are appropriate for this calculation. Factors such as localized surface roughness and dry deposition, can be considered.

Accident duration is defined in terms of plume passage at the location of the dose calculation, for a period not to exceed eight hours. The accident progression should not be defined using only input variables that maximize dispersion and minimize exposure (i.e., using a release rate that is specifically intended to expose the MOI to only a small fraction of the total material released, or defining the time and wind speed so that the plume does not reach the MOI).

The χ/Q values for each hour of meteorological data should be determined using the directionally dependent distance to the receptor for the corresponding wind direction. (The parameter χ/Q represents the dilution of the radioactive plume via dispersion and deposition as it travels from the facility during an accident.) A χ/Q value that is exceeded no more than five percent of the total number of hours in the data set shall be the comparison point for assessment against the EG. To ensure a representative distribution of directional dependence, five years of on-site meteorological data should be used. The 95th percentile dose should be calculated for each year, and the resulting highest year’s value should be used to determine the maximum impact. If the analysis does not assume directional dependence (i.e., if it uses the minimum distance for any sector for all wind directions), one year of on-site meteorological data is sufficient.

Accidents with unique dispersion characteristics, such as fires and explosions, may be modeled using phenomenon-specific codes that more accurately represent the release conditions. The appropriateness of the model to the specific situation should be discussed. For accident phenomena defined by weather extremes, actual meteorological conditions associated with the phenomena may be used for comparison to the EG.

Computer codes are typically used to support the dispersion calculation, for example the MACCS2 code has been utilized in many cases and DOE has established code guidance supporting its use. The following provides some appropriate considerations for ensuring conservative calculation of doses when using the MACCS2 code:

* A deposition velocity of 0.1 cm/sec for unfiltered release of particles or calculated site specific value;
* A surface roughness of 3 cm or calculated site specific value;
* Plume centerline concentrations for calculation of dose consequences;
* Plume meander not used in the consequences analysis; and,
* Wake effect of nearby obstacles ignored in the plume dispersion.

**Dose Conversion Factors**

Dose conversion factors consistent withInternational 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*, shall be used. However, there is no need to update existing dose calculations in approved DSAs that use older values.

## 3.3 HAZARD CONTROL IDENTIFICATION AND DESIGNATION

If the need for a safety class or safety significant control designation is determined, all preventive and mitigative features associated with the sequence of failures that result in a given release scenario are candidates for consideration. Designation of one or more of these controls shall adhere to a hierarchy that gives preference to passive engineered safety features over active ones; engineered safety features over ACs or SACs; and preventive over mitigative controls. Consistent with the requirements of DOE Order 420.1C, preference shall be given to active over passive confinement systems. The overall concept of control hierarchy is further discussed in Appendix A, Section A.12.

Hazard controls shall incorporate a defense in depth approach that builds in layers of defense against release of hazardous materials so that no one layer by itself, no matter how robust, is completely relied upon. The overall approach to defense-in-depth is further discussed in Appendix A, Section A.8. Section 3.3.2 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 hazardous material (see Chapter 4, Section [3.3.2.4] of this Standard for further discussion).

### 3.3.1 Safety Class Controls

If the unmitigated release consequence for an EBA/DBA exceeds the public EG, SC controls shall be applied to prevent the accident or mitigate the consequences to below the EG. It is expected that new nuclear facilities will reflect through their design, construction and operation a very low probability for accidents that could result in the release of any significant amount of radioactive material. Design basis accidents for all 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 controls will be such that accident consequences would be well below the EG[[6]](#footnote-6)..

If the need for SC control designation is determined, all preventive and mitigative features 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 many factors, such as: (1) the control’s effectiveness; (2) a general preference for preventive over mitigative controls and passive over active controls; and (3) relative reliability.

For existing facilities, an extremely unusual situation could occur where no viable control strategy exists that could either prevent or mitigate the dose in one or more of the accident scenarios from exceeding the EG. In such an event, a discussion of potential corrective and compensatory measures shall be included in the DSA. If this case occurs the control strategy and the basis for its adequacy shall be formally documented in an attachment to the DSA. The attachment shall:

* Identify the accidents that cannot be mitigated or prevented, including the likelihood of the event(s) and the mitigated consequences associated with the event(s).
* Provide a detailed analysis of the expected frequency and consequence of the associated accident. The detailed analysis should address the significant contributors to uncertainties in both the frequency and consequence evaluations.
* Discuss the available controls that could reduce the likelihood and/or consequences of an accident, including their potential failure modes and reasons why they are not sufficient to meet the EG.
* Discuss the overall strategy along with timeframe and decision milestones, including planned operational improvements, potential facility modifications and/or additional compensatory measures to reduce the likelihood and/or mitigate consequences of an accident. DOE will independently verify the proposed compensatory measures prior to their implementation.
* Present the rationale for the decision to continue operation of the facility to justify the conclusion that the facility provides a level of protection that would not result in undue risk to the public, taking into account the work to be performed, associated hazards, and existing control strategy.
* Address interactions with all necessary levels of contractor and DOE site and Headquarters line management and oversight organizations to assure that appropriate efforts are taken to rectify the situation.
* Specify a senior level of DOE approval authority for these circumstances, including a Program Secretarial Officer or higher (when appropriate) in consultation with its Central Technical Authority and the Office of Health, Safety, and Security.

### 3.3.2 Safety Significant Controls

As described in the following sections, SS control designation shall be made on the basis of the control’s contribution to: (1) defense-in-depth for the protection of public from release of radiological materials; (2) protection of the public from release of hazardous chemicals; (3) protection of co-located workers from release of hazardous chemicals or release or exposure to (e.g., criticality events) radiological materials and (4) protection of facility workers from release of or exposure to hazardous chemicals or radiological material. The applicable quantitative and qualitative criteria for these receptors are defined below.

**Safety Signification Controls Providing Defense-in-Depth for Protection of the Public**

SSCs that provide a significant contribution to defense-in-depth against radiological material releases requiring SC controls shall be designated as safety significant. A situation where a SSC should be identified as providing a significant contribution to defense-in-depth is one where only one SC control is relied on to prevent or mitigate an accident and one or more SSC is available (for existing facilities) or can be designed (for new facilities) to prevent or mitigate the accident. Examples of SSCs that could provide a significant contribution to defense-in-depth in these situations include (1) a facility-level ventilation system with high efficiency particulate air (HEPA) filtration which provide mitigation for a situation where a SC preventative control is utilized, (2) a glove box ventilation system provides a second mitigative SSC to back up a facility level ventilation system, or (3) a fire protection system provides a second means to mitigate an accident in addition to a facility level ventilation system.

The SS controls used for defense-in-depth should be independent from each other and from the related SC controls. In other words, it should be qualitatively shown that multiple SS and SC SSC failures would not occur from the same accident scenario. Note also that SC controls are not assigned for chemical hazards; therefore, this concept of defense-in-depth SS controls does not apply to chemical hazards. For chemical hazards, SS controls are identified in accordance with the criteria provided below.

**Safety Signification Controls Providing Protection to Public from Chemicals**

SS designation of controls for protection of the public from chemical releases shall be performed in a manner consistent with DOE-STD-1189. A general threshold for consideration of the need for SS SSCs is a peak air concentration at the receptor location that exceeds AEGL-2, ERPG-2, and/or TEEL-2. Note, however, that the TEEL table includes many more chemicals than the industrial safety standards of AEGL-2 and ERPG-2. Analysis is not expected for all the chemicals on the TEEL list, when it is apparent that due to releasability or dispersability considerations, there would be limited, if any, concern for downwind release and exposure. Therefore, care should be taken to not extend the resources for SS designation on TEEL-list chemicals that are generally considered to pose limited risk.

**Safety Signification Controls Providing for Co-located Worker Safety**

SS designation for protection of co-located workers from radiological releases shall be performed in a manner consistent with DOE-STD-1189. A conservatively calculated unmitigated dose of 100 rem TEDE is the threshold for designation of safety SSCs as SS for new facilities. The methodology used to generate the source term should be consistent with that used in accident analysis for the unmitigated scenario. The dispersion methodology should be consistent with Appendix A of DOE-STD-1189.

SS designation for protection of co-located workers from chemical releases shall be performed in a manner consistent with DOE-STD-1189. A general threshold for consideration of the need for SS SSCs is a peak calculated unmitigated exposure of AEGL-3/ERPG-3/TEEL-3.

**Safety Signification Controls Providing for Facility Worker Safety**

Safety management programs provide the foundation for protecting facility workers. Select hazards, however, may be qualitatively evaluated as meriting SS SSC or SAC designation. SS control designation should be considered for cases where a fatality, serious injury, or significant radiological or chemical exposure may occur. Consistent with Appendix C of DOE-STD-1189, the following circumstances are examples that warrant consideration of SS designation:

* Energetic releases of high concentrations of radiological or toxic chemical materials where the facility worker would normally be immediately present and may be unable to take self-protective actions;
* Deflagrations or explosions within process equipment or confinement and containment structures or vessels where serious injury or death to a facility worker may result from the fragmentation of the process equipment failing or the confinement (or containment) with the facility worker close by;
* Chemical or thermal burns to a facility worker that could reasonably cover a significant portion of the facility worker body where self-protective actions are not reasonably available due to the speed of the event or where there may be no reasonable warning to the facility worker of the hazardous condition; and,
* Leaks from process systems where asphyxiation of a facility worker normally present may result.

Safety significant SSCs are considered for cases involving significant exposure of the facility worker to radiological or other hazardous materials. This determination should be based on qualitative engineering judgment and historical experience. This approach is used because of the inherent large variability in quantitative consequence estimates resulting from small differences in assumptions regarding facility worker position or circumstance. This emphasis on qualitative estimation is intended to preserve good judgment where meaningful analysis is limited.

The criticality safety hazard evaluation process uses the ANSI/ANS-8.1, *Nuclear Criticality Safety in Operations With* *Fissionable Material Outside Reactors,* for identifying controls. DOE-STD-3007 provides additional guidance*.* Section 3.1.3 of this Standard provides criteria for determining whether a particular scenario and associated control(s) should be explicitly analyzed in the DSA hazard evaluation. Criticality safety controls that are explicitly analyzed in the DSA hazard evaluation shall be evaluated for SS designation using the basis for facility worker safety described above.

### 3.3.3 Other Hazard Controls

The hazard evaluation process may identify controls that do not rise to the level of SC and/or SS but still enhance the safety of the facility. These controls may be identified in the hazard evaluation table and should be controlled via safety management programs.

## 3.4 Design of Hazard Controls

For new facilities, the design requirements for SC and SS controls are specified in DOE O 420.1C which includes specific requirements for use of industry codes and standards as well as DOE standards such as DOE-STD-1020, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities*.

For existing facilities, an engineering evaluation shall be conducted that evaluates the performance capabilities of safety SSC(s) and demonstrates that the safety SSC(s) can adequately and reliably perform its designated safety functional requirements under the postulated accident conditions (i.e., are safety SSC(s) design attributes such as pressure and temperature operating ranges sufficient in light of expected accident conditions). This evaluation shall be supported either by:

* comparing the safety SSC design attributes to DOE O 420.1C design requirements, and associated codes and standards that are applicable, and demonstrating compliance[[7]](#footnote-7); or
* demonstrating that the existing SSCs satisfy equivalent requirements of current design codes and standards; or
* a technical basis that includes calculations, performance tests, or reliability evidence from operating history or industry databases.

The evaluation of SC and SS SSC adequacy shall be documented in the DSA (see Chapter 4 Sections [4.3.X.4] and [4.4.X.4] of this Standard for further discussion).

## 3.5 Accident Frequency Calculation Overview

Accident frequency calculations may be performed to provide supporting information for the analytical and decision-making processes. For each initiating event, a reasonably conservative and approximate frequency estimate of the initiating event is combined with estimates of probabilities of subsequent events that must occur to result in the release of or exposure to hazardous material for a predefined receptor (such as the public). This estimate (the hazardous material leaving the facility and outside the facility boundary) is used to calculate the dose to the MOI and does not account for the probability that an individual will be under the plume centerline and remain there for the required duration of time.

Calculation of accident frequencies may be used to:

* Guide decisions on reasonable levels of conservatism to be employed in various portions of accident analysis;
* Exclude certain events or event combinations from further analysis, such as external events with associated release frequencies below 1E-6 /yr;
* Assist in selecting representative EBAs for accident analysis[[8]](#footnote-8); and,
* Bin hazard scenarios.

The frequencies and consequences of each bin entry are based on the combinations of successes and failures of all controls, such as SSCs, and the various states of physical phenomena (e.g., the presence and amounts of MAR in a location, or whether an explosion will occur as a result of dropping a piece of explosive).

## 3.6 Planned Design and Operational Safety Improvements

As part of the hazard and accident analyses, the need for additional design and/or operational safety improvements may be identified. Due to capital costs, the need for further study (e.g., technical issues, cost-benefit), procurement lead times, or other complications, it may not be feasible to implement such design or operational improvements before the DSA is submitted. DOE does not wish to unduly delay DSA completion for such reasons, and numerous safety precedents acknowledge accepting work in progress. Accordingly, the facility operator may choose to commit to implementing an improvement that is not reflected in the current design or facility operations.

## 3.7 References

* 10 C.F.R. 50.34, *Contents of Applications, Technical Information*
* 10 C.F.R. 851, *Worker Safety and Health Program.*
* 29 C.F.R. 1910.119, *Process Safety Management of Highly Hazardous Chemicals*.
* 29 C.F.R. 1910.1200, *Occupational safety and Health Standards, Hazard Communications.*
* 29 C.F.R. 1910.1450, *Occupational Exposure to Hazardous Chemicals in Laboratories.*
* 40 C.F.R 302.4, *Designation, Reportable Quantities and Notification.*
* 40 C.F.R. 355 Appendix A, *The List of Extremely Hazardous Substances and Their Threshold Planning Quantities.*
* 40 C.F.R. 68.130, *List of Substances*. (Regulated toxic and flammable substances under Section 112(r) of the Clean Air Act).
* ANSI/ANS-8 *Nuclear Criticality Safety* in *Operations with* *Fissionable Material Outside Reactors.*
* Center for Chemical Process Safety*, Guidelines for Hazard Evaluation Procedures,* American Institute of Chemical Engineers, 2008.
* DOE O 414.1D, *Quality Assurance,* April 2011.
* DOE O 420.1B, *Facility Safety,* 2012.
* DOE O 440.1B, *Worker Protection Program for DOE (Including the National Nuclear Security Administration) Federal Employees,* May 2007.
* DOE G 424.1-1B, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements,* April 2010*.*
* DOE-HDBK-3010-94 (Chg 1), *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*, March 2000.
* DOE-STD-1020-94, *Natural Phenomena Hazards Analysis and Design Criteria for DOE*.
* 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.
* DOE-STD-1104, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents,* May 2009.
* DOE-STD-1186-2004, *Specific Administrative Controls,* August 2004.
* DOE-STD-1189-2008, *Integration of Safety into the Design Process*, March 2008.
* DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*, February 2007.
* DOE-STD-3011-2002, *Guidance for Preparation of Basis for Interim Operation (BIO) Documents*, December 2002.
* DOE-STD-5506-2007, *Preparation of Safety Basis Documents for Transuranic (TRU) Waste Facilities*, April 2007.
* Draft DOE Standard, *Development and Use of Probabilistic Risk Assessments in Department of Energy Nuclear Safety Applications*, for interim use, December 2011.
* EPA-454/R-99-005, *Meteorological Monitoring Guidance for Regulatory Modeling Applications,* Environmental Protection Agency*,* February 2000.
* Environmental Protection Agency/Federal Emergency Management Agency/U.S. Department of Transportation, *Technical Guidance for Hazards Analysis-Emergency Planning for Extremely Hazardous Substances*, 1987.
* ICRP Publication 68, *Dose Coefficients for Intakes of Radionuclides by Workers*, International Commission on Radiological Protection, 1994.
* ICRP Publication 72, *Age-Dependent Doses to members of the Public from Intake of Radionuclides*, International Commission on Radiological Protection, 1995.
* NFPA 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response*, National Fire Protection Association, 2012.
* NRC Regulatory Guide 1.23, *Meteorological Monitoring Programs for Nuclear Power Plants*, Nuclear Regulatory Commission, March 2007.
* NUREG-1140, *A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees,* January 1, 1988.

# Section 4. DSA Format and Content

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 sections described here are numbered in a manner that could be utilized 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. However, all 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. Expected products of this summary, as applicable based on the graded approach, include:

* A summary of the facility background and mission;
* An overview of the facility, including location and boundaries;
* A description of the facility hazard category;
* A summary of the results of the facility safety analysis, including hazards analyzed and TSR controls;
* A summary of the acceptability of the facility safety basis; and.
* A guide to the structure and content of the DSA (i.e., the “road map”).

The Executive Summary is prepared after all the other DSA chapters have been completed, since it draws primarily upon the information in those chapters. The information provided in the Executive Summary should be at a high-level and should not reproduce the details documented in subsequent chapters.

**ORGANIZATION AND CONTENT GUIDANCE FOR THE DSA [EXECUTIVE SUMMARY]**

The following presents criteria and guidance related to the content of a DSA Executive Summary.

**[E.1] Facility Background and Mission**

This section identifies the facility for which the DSA has been prepared and presents general information on the background of the facility as it relates to the stage of the facility life-cycle. Clearly present the current mission statement for which the DSA documents the safety basis (i.e., the purpose for which authorization is sought).

Present any relevant information (e.g., short facility life-cycle, anticipated future change in facility mission, approved DOE exemptions) that affect the extent of the safety analysis documented in the DSA and briefly explain its impact in terms of application of the graded approach.

**[E.2] Facility Overview**

This section provides an overview of the facility, including the facility location, physical and institutional boundaries, relationships and interfaces with nearby facilities, facility layout, and significant external interfaces (e.g., utilities, fire support, and medical support).

**[E.3] Facility Hazard Categorization**

This section provides a statement of the facility hazard category as determined in accordance with DOE-STD-1027. If determination of the hazard category relied upon segmentation of facility hazards, briefly explain the technical basis for such segmentation.

**[E.4] Safety Analysis Overview**

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

* A description of the facility operations analyzed in the DSA;
* A summary of the significant hazards associated with the facility processes including design basis accidents (DBAs)[[9]](#footnote-9); and,
* A summary of the TSR controls relied upon in the facility safety basis.

**[E.5] Organizations**

This section identifies the prime contractors responsible for facility design and construction (e.g., an architect-engineer), facility maintenance and operation, and any consultants, oversight groups, and outside service organizations with significant safety functions. This section should also identify groups, including consultants that participated in the DSA development process.

**[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 provides a description of site characteristics sufficient for understanding the aspects of the facility environs that are important to the safety basis. This chapter provides information to support and clarify assumptions used in the hazard and accident analyses related to identification and analysis of potential external and natural event accident initiators and accident consequences external to the facility.

The description of site characteristics, as a minimum, shall locate the facility on the overall site, show the facility boundaries, and shall identify any other facilities that can significantly impact the facility being examined.

For hazard category 3 facilities, on-site meteorological conditions, hydrology, and off-site accident pathways do not typically need to be addressed, since consequences are limited to the facility itself. However, if significant chemical hazards are present in a hazard category 3 facility that has the potential to cause significant off-site consequences, more information shall be provided concerning those items.

For hazard category 2 facilities, the site characteristics description is focused within the site boundaries, unless hazards have the potential to cause off-site consequences of concern. For hazard category 2 facilities with the potential for an accident resulting in consequences of concern at the site boundary, information on site characteristics shall be extended beyond the site boundary.

Supporting documentation shall be referenced. Brief abstracts of referenced documentation should be included, with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

**ORGANIZATION AND CONTENT GUIDANCE FOR DSA [CHAPTER 1]**

The following presents criteria and guidance related to the content of DSA Chapter 1. The information in this chapter is numbered in a manner that could be utilized in a DSA (e.g., “1.1, Introduction” and “1.2, Requirements”).

**[1.1] Introduction**

This section provides an introduction to the contents of this chapter, including objectives and scope specific to the chapter, as developed**.**

**[1.2] Requirements**

This section shall list the design codes, standards, regulations, and DOE Orders that are required for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific to this chapter and pertinent to the safety analysis, not a comprehensive listing of all industrial standards or codes or criteria. Standards and requirements identification documents (SRIDs) may be referenced as appropriate.

**[1.3] Site Description**

This section shall describe the site boundary and facility area boundary.

It shall provide 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 where the EG is applied; and,
* Additional detail maps, as needed, to present near-plant detail, such as orientation of buildings, traffic routes, transmission lines, and neighboring structures.

**[1.3.1] Demography**

Population information, based on recent census data, shall be included 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 off-site consequences. The minimum area addressed is defined by the area significantly affected by the accidents analyzed in DSA Chapter 3, “Hazard and Accident Analyses and Control Selection.”

**[1.4] Environmental Description**

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

**[1.4.1] Meteorology**

This section shall provide the meteorological information necessary to understand the regional weather phenomena of concern for facility operations and to understand any dispersion analyses performed.

**[1.4.2] Hydrology**

This section shall provide the hydrological information necessary to understand any regional hydrological phenomena of concern for facility operations, as well as to understand any dispersion analyses performed.

Include information on groundwater aquifers, drainage plots, soil porosity, and other aspects of the hydrological character of the site. Discuss or reference, to the degree necessary, the average and extreme conditions as determined by historical data to meet the intent of this section.

**[1.4.3] Geology**

This section shall provide the geological information necessary to understand any regional geological phenomena of concern for facility operations. Describe the nature of investigations performed and provide the results of the investigations. Include geologic history, soil structures, and other aspects of the geologic character of the site.

**[1.5] Natural Event Accident Initiators**

This section shall identify specific natural events, such as design basis earthquakes, that are considered to be potential accident initiators. Summarize the assumptions supporting the analysis in DSA Chapter 3.

**[1.6] Man-made External Accident Initiators**

This section shall identify specific man-made external events associated with the site – such as explosions from natural gas lines or accidents from nearby transportation activities – that are considered to be potential accident initiators, exclusive of sabotage and terrorism. Summarize the assumptions supporting the analysis in DSA Chapter 3.

**[1.7] Nearby Facilities**

This section shall identify any nearby facilities that could be affected by accidents within the facility being evaluated. Conversely, this section also identifies any hazardous operations or facilities on or off site that could adversely impact the facility being evaluated. Summarize the assumptions supporting the analysis in DSA Chapter 3.

**[1.8] Validity of Existing Environmental Analyses**

This section shall assess the validity of site characteristic assumptions for existing environmental analyses and impact statements based on the more recent DSA effort. Simply state that no significant discrepancies exist or indicate the need to revise and update assumptions used in facility environmental statements through brief discussions summarizing major discrepancies.

## DSA [CHAPTER 2: FACILITY DESCRIPTION]

This chapter provides descriptions of the facility and processes to support assumptions used in the hazard and accident analyses. These descriptions focus on all major facility features necessary to understand the hazard analysis and accident analysis, not just safety SSCs. Note that safety SSCs are described in detail in DSA Chapter 4, “Safety Structures, Systems, and Components”, but other SSCs are not.

The development of this chapter for hazard category 2 and 3 facilities should be an iterative process dependent on the development of the hazard and accident analyses. The facility description 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 significance of the identified preventive and mitigative features and the degree of facility context necessary to understand the analyses. For a hazard category 3 facility, only a brief description of the facility, processes, and major SSCs should be necessary. Graded information will be provided, based predominantly on complexity. This chapter does not include information at the level of functional requirements and performance criteria; rather, that information is provided for safety SSCs only in DSA Chapter 4. In the basic description of safety SSCs in DSA Chapter 2, their categorization as SC or SS SSCs may simply be noted.

Supporting documentation shall be referenced. Brief abstracts of referenced documentation should be included, with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

**ORGANIZATION AND CONTENT GUIDANCE FOR DSA [CHAPTER 2]**

The following presents criteria and guidance related to the content of DSA Chapter 2. The information in this section is numbered in a manner that could be utilized in a DSA (e.g., “2.1, Introduction” and “2.2, Requirements”).

**[2.1] Introduction**

This section provides an introduction to the contents of this chapter including objectives and scope specific to the chapter, as developed.

**[2.2] Requirements**

This section shall list the design codes, standards, regulations, and DOE Orders that are required for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific to this chapter and pertinent to the safety analysis, not a comprehensive listing of all industrial standards or codes or criteria.

**[2.3] Facility Overview**

This section shall include 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 shall provide an overview of the basic facility buildings and structures, including construction details such as basic floor plans, equipment layout, construction materials, dimensions, and dimensions significant to the hazard and accident analysis activity. Provide sufficient information to support an overall understanding of the facility structure and the general arrangement of the facility as it pertains to hazard and accident analysis.

**[2.5] Process Description**

This section shall describe the individual processes within the facility. Include details on basic process parameters, including: (1) a summary of types and quantities of hazardous materials; (2) process equipment; (3) instrumentation and control systems and equipment; (4) basic flow diagrams; and, (5) operational considerations associated with individual processes or the entire system, including major interfaces and relationships between SSCs. The intent is to provide sufficient information to support an understanding of the assessment of potential accidents under normal and abnormal operating conditions, the safety analysis, and its conclusions.

**[2.6] Confinement Systems**

This section shall identify and describe the set of SSCs that perform confinement functions, such as process vessels, gloveboxes, ventilation systems, and facility walls.

**[2.7] Safety Support Systems**

This section shall identify and describe the principal systems that perform safety support functions (i.e., safety functions that are not part of specific processes). State the purpose of each system and provide an overview of each system, including principal components, operations, and control function. Examples of systems under this heading might include fire protection, criticality monitoring, radiological monitoring (e.g., air monitoring, contamination prevention), chemical monitoring (e.g., hydrogen concentration monitoring), and effluent monitoring.

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 summary shall specify whether the reference applies to a specific commitment in a portion of the referenced documentation, or whether it is a global commitment to maintain a program for which a number of details may vary without affecting the global commitment.

This section is designed to organize the presentation of information, and not to designate any special class of equipment.

**[2.8] Utility Distribution Systems**

This section shall provide a schematic outline of the basic utility distribution systems, including a description of the off-site power supplies and on-site components of the system. Details of systems are given, to the level necessary, for understanding the utility distribution philosophy and facility operations.

**[2.9] Auxiliary Systems and Support Facilities**

This section shall provide information on the remaining portions of that facility that have not been covered by the preceding sections and that are necessary to create a conceptual model of the facility as it pertains to the hazard and accident analyses.

## DSA [CHAPTER 3: HAZARD AND ACCIDENT ANALYSES AND CONTROL SELECTION]

This chapter of the DSA provides information documenting how the requirements of 10 C.F.R. 830 were met to evaluate normal, abnormal, and accident conditions and the results of the evaluation.

This chapter describes the process used to systematically identify and assess hazards to evaluate the potential internal, man-made external, and natural events that could cause the identified hazards and events to develop into accidents. Subsequent accident analysis evaluates the potential for public consequences from these accidents. This chapter covers the topics of hazard identification, facility hazard categorization, hazard evaluation, and accident analysis.

Supporting documentation shall be referenced. Brief abstracts of referenced documentation should be included, with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

**ORGANIZATION AND CONTENT GUIDANCE FOR DSA [CHAPTER 3]**

The following presents criteria and guidance related to the content of DSA Chapter 3. The information in this section is numbered in a manner that could be utilized in a DSA (e.g., “3.1, Introduction” and “3.2, Requirements”).

**[3.1] Introduction**

This section provides an introduction to the contents of this chapter, including objectives and scope specific to the chapter, as developed.

**[3.2] Requirements**

This section shall list the design codes, standards, regulations, and DOE Orders that are required for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific to this chapter and pertinent to the safety analysis, not a comprehensive listing of all industrial standards or codes or criteria.

**[3.3] Hazard Analysis**

This section shall describe the hazard identification and evaluation performed for the facility.

**[3.3.1] Methodology**

This section presents the methodology used to identify hazards and to perform a systematic evaluation of hazards.

**[3.3.1.1] Hazard Identification**

This section shall identify the method used to identify and inventory the hazardous materials and energy sources (in terms of quantity, form, and location) associated with the facility processes or associated operations (e.g., waste handling).

This section shall also indicate the 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 shall be provided.

The basis for removing standard industrial hazards or insignificant hazards from further consideration shall be provided, and the corresponding interfaces with other programs (e.g., OSHA) shall be identified.

**[3.3.1.2] Hazard Evaluation**

This section shall present:

* 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). This rationale should focus on the selection of a technique for given processes, such as HAZOP;
* In summary fashion, the basic approach and guidance used in generating the largely qualitative consequence and likelihood estimates in the hazard evaluation; and,
* The process used to identify the need for, and adequacy of, identified controls associated with each hazard scenario. Reference any detailed guidance as necessary.

**[3.3.2] Hazard Analysis Results**

**[3.3.2.1] Hazard Identification**

This section shall present the results of the hazard identification activity, either by direct inclusion of, or by reference to, the hazard identification data sheets. As a minimum, a summary table identifying hazards by form, type, location, and total quantity shall be provided. The basic set of hazards identified shall include radionuclides, 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”) as long as the assessment in the hazard analysis addresses the hazards that are likely in facility operations.

The major accidents or hazardous situations (e.g., fires, explosions, loss of confinement) that have occurred in the facility’s operating history shall be summarized in this subsection. 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 section shall present the results of the final hazard categorization activity specified in   
DOE-STD-1027, including the facility hazard categorization, where segmentation has been employed, the segment boundaries and individual segment classifications.

Any segmentation shall be justified in terms of independence. Where facility segmentation is used, provide the hazard breakdown by segment in a summary table.

MAR that was excluded for any reason (e.g., sealed sources, qualified containers) from the hazard categorization process shall be identified.

**[3.3.2.3] Hazard Evaluation**

This section shall present the results of the hazard evaluation activity, either by direct inclusion, or inclusion by reference, to the hazard evaluation data sheets.

For each hazard scenario, document the following:

* The key unmitigated hazard scenario assumptions, such as the quantity of hazardous material involved, energy sources, release pathways, affected receptors, and any key physical limiting issues;
* Unmitigated and mitigated consequences for the facility worker (qualitative or semi-quantitative), the co-located worker (qualitative or semi-quantitative), and the public; and,
* The controls assumed to function for the mitigated scenario.

Detailed bases of engineering judgments are not required to be formally documented in the DSA, however brief summaries of the underlying rationale should be provided. Pertinent documentation shall be referenced as necessary. Additionally, if risk-binning is performed, the results should also be documented.

**[3.3.2.4] Defense-in-Depth**

This section shall provide the narrative evaluation of the facility’s approach to defense-in-depth for protection of workers and the public from the release of hazardous material. A summary listing of defense-in-depth features shall be provided in this section of the DSA. For those features that are hardware-oriented, the DSA shall describe the programmatic requirements that maintain their configuration and operability. See Appendix A, Section A.8 of this Standard and the defense-in-depth design requirements of DOE O 420.1C for a discussion of defense-in-depth.

**[3.3.2.5] Worker Safety**

This section shall provide the narrative evaluation of the facility’s approach to worker safety, exclusive of standard industrial hazards. This section shall include a list of any SS controls (SSCs or SACs) and safety management programs assigned for worker safety and their bases. Any safety designations of controls for co-located worker protection shall be consistent with the applicable criteria used in the hazard or accident analyses.

**[3.3.2.6] Environmental Protection**

This section shall provide the narrative evaluation of the facility’s approach to environmental protection. This section should focus on unique issues not covered elsewhere. SC and SS SSCs are not designated solely for environmental protection.

**[3.4] Accident Analysis**

This section shall describe the accident selection, DBA/EBA development, designation of SS and SC controls, and the results of the mitigated accident analysis. Also included shall be an analysis of any beyond DBAs/EBAs performed for the facility.

**[3.4.1] Methodology**

This section summarizes the methods used to derive the DBA/EBAs from the hazard analysis, quantifies their consequences, designates SC controls, and evaluates the effectiveness of safety controls in preventing or mitigating these postulated DBA/EBAs.

For the analytical tools that were used:

* Identify and describe any computer models used;
* Include in the description its validation for the specific application, including the type and range of data; and,
* Briefly summarize and reference detailed information on algorithms, computational and analytical bases, and software quality assurance measures. Computer models shall meet the quality assurance program requirements of DOE O 414.1D, *Quality Assurance*, as applicable.

Documentation of methodology should include the following:

* Methods used to estimate source terms for DBA/EBAs, including:
* The basic approach for estimating physical facility damage from DBA/EBAs;
* 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, including assumptions about such variables as meteorological conditions, time-dependent characteristics, activity, 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 shall identify the set of facility DBA/EBAs in terms of:

* The categories of operational accidents, natural events, and man-made external events;
* The DBA/EBA type (fire, explosion, spill, earthquake, tornado, etc.); and
* Whether the EBA is representative or unique. In the case of representative accidents, the hazard scenarios that they bound, shall be identified.

**[3.4.3] Design Basis/Evaluation Basis Accidents**

This section shall analyze the DBA/EBAs identified in Section 3.4.2, “Accident Selection” to quantify their approximate and reasonably conservative frequencies and consequences, and to compare their consequences to the EG.

For each DBA/EBA, both the unmitigated scenario and mitigated DBA/EBA should be sufficiently documented to explain the thought process that went into analysis, the selection of SC SSCs, and the evaluation of the level of protection provided by the identified SSCs controls.

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

**[3.4.3.X] Applicable DBA/EBA**

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

**[3.4.3.X.1] Scenario Development**

This section describes the progression of the accident, linking initiating events with preventive and mitigative controls and other contributing phenomena to formally define the accidents identified in Section 3.4.2, “Accident Selection.” Note: each response, action, or indication required to initiate action, is relevant to the scenario progression.

When summarizing the initiating event for a given natural-event DBA/EBA, identify the load factors, return periods, amplification factors for the facility, and similar variables that characterize the phenomenon. For operational DBA/EBAs, these may include the magnitude of the energy release or physical conditions relevant to accident progression, such as temperature or pressures.

Summarize the facility and equipment response to the loads or environmental conditions postulated to be present at the time of the given natural event or accident. Reference the analysis or facility documentation of this evaluation and summarize the relevant assumptions. Discuss the degree of conservatism of the evaluation.

Because external-event DBA/EBAs are developed using frequency criteria, reference the analysis that substantiates the external event frequency.

**[3.4.3.X.2] Source Term Analysis**

This section identifies the material and energy released through the pathways of concern during the accident. Define all parameters and phenomenological models used to derive the source term, including the characteristics of the release (e.g., an energy release as it relates to the source term determination). As a minimum, this definition includes the MAR (as derived from the hazard identification), the bounding release fraction or rate that determines the initial source term, and the overall facility LPFs that determine the final source term released external to the facility. Detailed quantification of uncertainty is not required.

**[3.4.3.X.3] Consequence Analysis**

This section identifies the receptor doses associated with the relevant pathways in accordance with the guidance provided in Section 3.2.6 (Dose Consequence Analysis) of this Standard. Provide, as a minimum, the unmitigated doses for the relevant DBA/EBAs and the mitigated doses assuming the functioning of the credited preventive and mitigative controls.

Compare: (1) the information related to protection of the public (derived from the hazard and accident analyses) and the potential insights gained for environmental contamination issues; and, (2) the facility’s National Environmental Policy Act documentation. There should be no significant discrepancies between the DSA and that documentation.

**[3.4.3.X.4] Comparison to Consequence Thresholds**

This section compares the unmitigated consequences to the EG and co-located worker thresholds described in Section 3.3.2.

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

This section lists the SC and SS SSCs, SACs, and safety management programs that are identified to function to prevent the scenario and/or to reduce public dose below the EG, provide defense-in-depth, or to provide worker safety. The DSA shall provide a technical basis for the establishment of controls, whenever engineering controls are not available to meet the hierarchy in accordance with Section 3.3, *Hazard Control Identification and Designation*.

**[3.5] Beyond Design Basis Accidents (BDBAs)**

This section shall document the analysis of any BDBA defined for the facility. The DSA should document the scope and method for analyzing BDBAs, the results of a realistic analysis of the impact of failure of hazard controls, the results of analysis of all analyzed Natural Phenomena Hazards (NPH) and any additional opportunities to prevent or to mitigate BDBAs. These analyses of NPH BDBEs provide valuable insights and can serve as bases for cost-benefit considerations for improvements, either for facility modifications or for enhanced emergency management capabilities. It may also be appropriate to include some of these BDBA considerations in the emergency plans of the DOE and non-DOE organizations that could be called upon to respond to a BDBA.

BDBAs need not be analyzed to the same degree of detail as DBAs/EBAs, and do not serve as a basis for designating safety SSCs.

**[3.6] Planned Design and Operational Safety Improvements**

This section shall present any commitments to future design and operational safety improvements. For each commitment, provide the following:

* 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 proposed until the improvement is implemented.

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

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

This chapter provides details on the facility SSCs that are necessary for the facility to protect the public, provide defense-in-depth, or contribute to worker safety. Similarly, this chapter provides details of SACs that are significant for reducing the risk of specific accidents. It also describes the attributes (i.e., 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.

Supporting documentation shall be referenced. Maximum advantage should be taken of pertinent existing safety analyses and design information (i.e., requirements and their bases) that are immediately available or can be retrieved through reasonable efforts. A brief summary should be included for each such reference, explaining its relevance to this chapter and providing an introductory understanding of the reference.

**ORGANIZATION AND CONTENT GUIDANCE FOR DSA [CHAPTER 4]**

The following presents criteria and guidance related to the content of DSA Chapter 4.

The information in this section is numbered in a manner that could be utilized in a DSA (e.g., “4.1, Introduction” and “4.2, Requirements”).

**[4.1] Introduction**

This section provides an introduction to the contents of this chapter based on the graded approach and includes objectives and scope specific to the chapter, as developed.

**[4.2] Requirements**

This section shall list the design codes, standards, regulations, and DOE Orders that are required for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific to this chapter and pertinent to the safety analysis, not a comprehensive listing of all industrial standards or codes or criteria.

**[4.3] Safety Class Structures, Systems, and Components**

Relevant information shall be provided, in the following SC SSC-specific subsections, with sufficiently detailed descriptions to provide an understanding of the safety function of each SC SSC. Descriptions of each SC SSC shall be complete enough to indicate the suitability of the safety analysis inputs and assumptions.

A summary list of SC SSCs shall be provided. This summary list should identify, in tabular form, 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. The remaining subsections provide details that correlate to the summary list.

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

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

Identify the SC SSC.

**[4.3.X.1] Safety Function**

This section shall state the reason for designating the SSC as an SC SSC, followed by specific identification of its preventive or mitigative safety function(s) as determined in the hazard and accident analysis. Do not discuss non-safety functions.

Safety functions are top-level statements that express 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.” The specific accidents associated with the safety function should be identified.

The specific accident(s) or general rationale associated with the safety function should be 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 section shall provide a description of the SC SSC and the basic principles by which it performs its safety function (e.g., the sensor and interlock for hydrogen detector discussed in Section 4.3.X.1, “Safety Function”). This section shall also describe its boundaries and interface points with other SSCs relevant to the safety function. Focus on providing information required to support the system evaluation in Section 4.4.X.4, “System Evaluation”.

SSCs whose failure would result in an SC SSC losing the ability to perform its required safety function shall be identified. These SSCs shall also be considered SC SSCs for the specific accident conditions for which the SC designation was made originally.

When describing the SSC, provide a basic summary of the physical information known about the SSC, including process and instrumentation drawings or a simplified system drawing with reference to process and instrumentation drawings. Summarize and refer to pertinent aspects of the manufacturer’s specifications if known. Pertinent aspects are considered to be those that directly relate to the safety function (e.g., diesel generator load capacity, time to load if critical), rather than general industrial equipment specifications that derive from these capabilities (e.g., starting torque, motor insulation, number and type of windings). Such lower-tier details should be implicitly included only by reference to the overall specifications.

**[4.3.X.3] Functional Requirements**

This section shall identify the functional requirements that are specifically needed to fulfill safety functions. Such requirements shall be specified for both the SC SSC and any needed support for the SC SSCs.

Designate as functional requirements only those requirements necessary for the safety function being credited. Functional requirements are provided for SC SSCs for the specific accident(s) where the SC SSC must function (e.g., if that accident is not initiated by an earthquake, the functional requirement does not involve seismic parameters).

Functional requirements shall 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, one obvious parameter would be keeping the hydrogen concentration below the explosive limit. If the offgas temperature was significantly above ambient temperatures, operation at that temperature would be a functional requirement as well.

**[4.3.X.4] System Evaluation**

**Identifying Performance Criteria**

This section shall provide 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 in addition to important parameters that are identified by applicable codes and standards related to their performance and reliability to perform when called upon (e.g., a certain gpm flow rate for the fire suppression system to comply with NFPA requirements).

In determining performance criteria for SC SSCs, design criteria established in DOE O 420.1C associated with SC designation, such as single-point failure criteria, shall be used.

**Evaluating Against Performance Criteria**

The ability of the SC SSC to meet performance criteria under EBA conditions shall be evaluated in accordance with the requirements in Section 3.4. The intent is that the SC control meets, or exceeds, the performance criteria. If the control cannot meet the performance criteria, identify the vulnerability and any compensatory measures necessary to support the general safety function of the SSC. These compensatory measures may have to be identified as additional TSR controls and may have to be designated as SC themselves.

When design information does not exist for an SSC to support a comparison to relevant design criteria, an engineering evaluation shall be used to support an understanding of the SSC’s performance and capabilities. This evaluation must be supported by a technical basis that includes calculations, performance tests, or reliability evidence from operating history or industry databases.

**[4.3.X.5] Controls (TSRs)**

This section shall list all SC controls that require TSRs. In addition, it shall identify design features and parameters related to the facility and processes that require TSRs to ensure assumptions and inputs to the accident analysis are maintained valid.

**[4.4] Safety Significant Structures, Systems, and Components**

Relevant information shall be provided, in the following SS SSC-specific subsections, with sufficiently detailed descriptions to provide an understanding of the safety function of each SS SSC. Descriptions of each SS SSC shall be complete enough to allow the accuracy of the safety analysis inputs and assumptions to be verified.

A summary list of SS SSCs shall be provided. This summary list should identify, in tabular form, the SS SSCs, the rationale (from DSA Chapter 3) underlying the SS designation, safety functions, functional requirements, and performance criteria judged to require TSR coverage. The remaining subsections provide details that correlate to the summary list.

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

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

Identify the SS SSC.

**[4.4.X.1] Safety Function**

This section shall state the reason for designating the SSC as an SS SSC, followed by specific identification of its preventive or mitigative safety function(s) as determined in the hazard and accident analysis. Do not discuss non-safety functions.

Safety functions are top-level statements that express 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.”

The specific accident(s) or general rationale associated with the safety function should be 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 section shall provide a description of the SS SSC and the basic principles by which it performs its safety function (e.g., the sensor and interlock for hydrogen detector discussed in Section 4.4.X.1, “Safety Function”). This section shall also describe its boundaries and interface points with other SSCs relevant to the safety function.

SSCs whose failure would result in an SS SSC losing the ability to perform its required safety function shall be identified. These SSCs shall also be designated as SS SSCs for the specific accident conditions or general rationale for which the SS designation was made originally.

When describing the SSC, provide a basic summary of the physical information known about the SSC, including simplified system drawings. If deemed pertinent, aspects of the manufacturer’s specifications shall be provided if known. Pertinent aspects are considered to be those that directly relate to the safety function (e.g., diesel generator load capacity, time to load if critical), rather than general industrial equipment specifications that derive from these capabilities (e.g., starting torque, motor insulation, number and type of windings). Such lower-tier details should be implicitly included only by reference to the overall specifications.

**[4.4.X.3] Functional Requirements**

This section shall identify the functional requirements that are specifically needed to fulfill safety functions. Such requirements shall be specified for both the SS SSC and any supporting SS SSCs.

Designate as functional requirements only those requirements necessary for the safety function. Functional requirements shall be provided for SS SSCs for the specific accident(s) or general rationales for which the SS SSC is needed (e.g., if that accident is not initiated by an earthquake, the functional requirement does not involve seismic parameters).

Functional requirements specifically address the pertinent response parameters or nonambient environmental stresses related to an accident for which the safety function is relied on. In the hydrogen detector example, one obvious parameter would be keeping the hydrogen concentration below the explosive limit. If the offgas temperature is 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 shall provide 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 in addition to important parameters that are identified by applicable codes and standards related to their performance and reliability to perform when called upon (e.g., a certain gpm flow rate for the fire suppression system to comply with NFPA requirements). In determining performance criteria for SS SSCs, design criteria established in DOE O 420.1C associated with SS designation shall be used.

When design information does not exist for an SSC to support a comparison to relevant design criteria, an engineering evaluation shall be used to support an understanding of the SSC’s performance and capabilities. This evaluation must be supported by a technical basis that includes calculations, performance tests, or reliability evidence from operating history or industry databases.

**Performance Evaluation**

The ability of the SS SSC to meet performance criteria shall be evaluated in accordance with requirements in Section 3.4 of this Standard. The intent is that the SS control meets, or exceeds, the performance criteria. If the control cannot meet the performance criteria, identify the vulnerability and any compensatory measures necessary to support the general safety function of the SSC. These compensatory measures may have to be identified as additional TSR controls and may have to be designated as SS themselves.

**[4.4.X.5] Controls (TSRs)**

This section shall list all SS controls that require TSRs. In addition it shall identify design features and parameters related to the facility and processes that require TSRs to ensure assumptions and inputs to the accident analysis are maintained valid.

**[4.5] Specific Administrative Controls**

Relevant information shall be provided, in the following SAC-specific subsections, with sufficiently detailed descriptions to provide an understanding of the safety function of the SAC. Descriptions of each SAC shall be complete enough to indicate the suitability of the safety analysis inputs and assumptions (see DOE-STD-1186, and Appendix A, Section A.9 of this Standard).

A summary list of SACs shall be provided. This summary list should identify, in tabular form, 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. The remaining subsections provide details that correlate to the summary list.

Note: The following format is repeated sequentially for each (“X”) SAC. The examples provided are for illustration purposes only and should not be construed as a requirement to designate such ACs as SACs.

**[4.5.X] Applicable Specific Administrative Control**

Identify the SAC.

**[4.5.X.1] Safety Function**

This section shall state the reason for designating an AC as an SAC, followed by specific identification of its preventive or mitigative safety function(s) as determined in the Chapter 3 hazard and accident analysis. Do not discuss non-safety functions.

Safety functions are top-level statements that express 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.” The specific accident(s) or general rationale associated with the safety function should be identified.

**[4.5.X.2] SAC Description**

This section shall provide a description of the SAC and the basic principles by which it performs its safety function (e.g., nuclear material control procedure for the MAR limit discussed in Section 4.5.X.1). Its boundaries and interface points with any SSCs relevant to the safety function, such as procedural actions interfacing with sensors/instrumentation and equipment shall be described.

If an SAC is utilized in lieu of the identification of safety SSCs, the rationale for this decision shall be clearly identified and discussed. Engineering controls are preferable to ACs and SACs, and emphasis should be placed on identifying safety SSCs. A discussion of why SSC(s) are not plausible or practical for accomplishing the safety function should be included.

SSCs whose failure would result in losing the ability to complete the action required by the SAC shall be identified. These SSCs shall be designated as SC or SS based on the significance of the SAC safety function.

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 section shall identify the functional requirements that are specifically needed to fulfill safety functions. Such requirements shall be specified for both the SAC and any needed supporting SSCs.

Designate as functional requirements only those requirements necessary for the SAC safety function. Functional requirements shall be provided for SACs for the specific accident(s) or general rationales for which the SAC is needed.

For SACs, functional requirements may involve unimpeded access to specific rooms or areas, use of certain instrumentation, written procedures or checklists, and special tooling. The description of the functional requirement shall fully address all aspects important for ensuring the SAC can be accomplished.

**[4.5.X.4] SAC Evaluation**

**Performance Criteria**

This section shall provide performance criteria imposed on the SAC so it can meet functional requirements(s) and, thereby, satisfy its safety function. Performance criteria characterize the specific operational responses and capabilities necessary to meet functional requirements.

**Performance Evaluation**

The formulation of SACs should include a process to validate that plant operators can perform the task(s) called for in an SAC within the timeframes assumed in the safety basis. If SACs require operator action and perform a function similar to a safety SSC, assurance should be provided that the operators can adequately perform their required tasks by analyzing the following human performance factors (at a minimum):

* 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 levels induced by the external environment (e.g., noise, heat, light, and protective clothing).

Formal engineering calculations may be necessary to ensure that plant operators have the appropriate time and resources to carry out the required tasks. For example, if it is assumed that operators will take action to detect and isolate a leak, flow rate calculations will need to be performed to substantiate the time interval needed to accomplish the task. Consequences of incorrect implementation of the control should be evaluated, and measures to prevent control failure should be factored into the control formulation.

**[4.5.X.5] Controls (TSRs)**

This section shall identify the assumptions that require TSRs to ensure performance of the safety function. SACs are generally implemented in TSRs in one of two forms:

* Limiting Condition of Operation (LCO)/Surveillance Requirement – SACs can often be written in the format of an LCO.
* Specific “Directed Action” AC – A Specific “Directed Action” AC TSR can be in the Administrative Controls section of the TSR.

Section 4 of DOE-STD-1186 discusses the treatment of SACs in TSRs.

## 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 hazard controls in 10 C.F.R. 830.

This chapter builds upon the control functions determined to be essential in DSA Chapter 3 and DSA Chapter 4 to derive TSRs. This chapter is meant to support and provide the information necessary for the separate TSR document required by 10 C.F.R. 830.205.

Supporting documentation shall be referenced. Brief abstracts of referenced documentation should be included, with enough essential facts to provide an understanding of the referenced documentation and its relation to this chapter.

**ORGANIZATION AND CONTENT GUIDANCE FOR DSA [CHAPTER 5]**

The following presents criteria and guidance related to the content of DSA Chapter 5. The information in this section is numbered in a manner that could be utilized in a DSA (e.g., “5.1, Introduction” and “5.2, Requirements”).

**[5.1] Introduction**

This section provides an introduction to the contents of this chapter including objectives and scope specific to the chapter, as developed.

**[5.2] Requirements**

This section shall list the design codes, standards, regulations, and DOE Orders that are required for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific to this chapter and pertinent to the safety analysis, and not a comprehensive listing of all industrial standards or codes or criteria. SRIDs may be referenced as appropriate.

**[5.3] TSR Coverage**

This section shall provide assurances that TSR coverage for the facility is complete. The section shall list the features identified in DSA Chapters 3 and 4 that are needed to:

* Provide significant defense-in-depth. These features are SS SSCs or SACs noted in DSA Section 3.3.2.3 and their associated assumptions requiring TSR coverage identified in DSA Section 4.4.X.5 or 4.5.X.5, and any other TSR assumptions;
* Provide for significant worker safety. These features are SS SSCs and SACs. Associated assumptions requiring TSR coverage as SS SSCs or SACs are identified in DSA Section 4.4.X.5 or 4.5.X.5, and any programs or program elements identified as needing coverage in TSR ACs are identified in DSA Section 3.3.2.3; and,
* Provide for significant public safety in accordance with implementation of the EG. These features are SC SSCs or SACs, and their associated assumptions requiring TSR coverage that are identified in the DSA.

The information should be organized in a table format that identifies the relevant hazard and the major features relied on for protection against that hazard. This presentation forms the basis for organization of the remainder of the chapter. Associated TSR safety limits (SLs), limiting control settings (LCSs), limiting condition for operations (LCOs), surveillance requirements, ACs, and design features identified throughout the remainder of the chapter should be included in this presentation for overall clarity.

This section shall specifically note the listed safety SSCs, if any, that will not be provided with TSR coverage, and shall provide an accompanying explanation.

**[5.4] Derivation of Facility Modes**

This section shall discuss the derivation of the basic operational modes (e.g., 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 DSA Chapter 3 regarding operational conditions associated with accidents.

**[5.5] TSR Derivation**

This information can be organized by the hazard protected against, the specific features, or even the actual TSRs, if desired. The method of organization is left to the discretion of the DSA preparer. The following format is repeated sequentially for each TSR (“X”).

**[5.5.X] Applicable Hazard/Feature/TSR “X”**

This section shall identify the specific feature(s) listed in DSA Section 5.3 and the relevant modes of operation.

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

This section shall provide the basis for, and identify, information sufficient to derive SLs, LCSs, and LCOs to support the facility TSR documentation required by 10 C.F.R. 830.205. SLs, if used, are reserved for a small set of extremely significant features that prevent potentially major off-site impacts. LCSs are developed for any SL that is protected by an automatic device with setpoints. LCSs/LCOs act to keep normal operating conditions below the SLs and are developed for each identified SL, thereby providing a margin of safety. Most LCOs are assigned without an accompanying SL.

Generally, SLs are applicable only for the protection of passive barriers, as close to the accident source as possible, whose failure during a specific event will result in exceeding the EG. 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 off-site radiological dose below the EG during an accident is mitigative and is more appropriately covered by an LCO. Temporary loss of this ventilation system’s function during normal operations does not initiate a significant 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, consider a tank that acts as a barrier preventing an uncontrolled release of hazardous material that could exceed the EG without ventilation mitigation. If that tank could experience a hydrogen explosion and rupture, the tank hydrogen concentration may warrant coverage by an SL.

**[5.5.X.2] Surveillance Requirements**

This section shall provide the basis for and identify information necessary to derive surveillance requirements that address testing, calibration, or inspection requirements to maintain operation of the facility within SLs, LCSs, and LCOs.

**[5.5.X.3] Administrative Controls**

This section shall provide the basis for and identify information necessary to derive TSR ACs. This section is the only applicable section for the features that are listed in DSA Section 5.3, “TSR Coverage,” and that are provided with only TSR ACs. The rationale for assigning TSR ACs shall be clearly and briefly stated.

A special type of TSR AC is one that covers a safety management program. The “Administrative Controls” section of the TSR document shall contain commitments to establish, maintain, and implement these programs at the facility and, as appropriate, facility staffing requirements.

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

**[5.6] Design Features**

This section identifies and briefly describes the passive design features that, if altered or modified, would have a significant effect on safe operation. Simply reference DSA Chapter 2, “Facility Description,” for the descriptions if that chapter contains all the desired information.

**[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.

## DSA [CHAPTER 6: PREVENTION OF INADVERTENT CRITICALITY]

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 requirements, it can be included by reference and summarized in this chapter.

Supporting documentation shall be referenced. A brief abstract of referenced documentation shall be included, with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

This section of the DSA shall summarize the key attributes of the CSP and include, by reference, additional elements of the CSP required by DOE O 420.1C and DOE-STD-3007-2007.

**ORGANIZATION AND CONTENT GUIDANCE FOR [CHAPTER 6]**

**[6.1] Introduction**

This section provides an introduction to the contents of this chapter based on the graded approach and includes objectives and scope specific to the chapter as developed.

**[6.2] Criticality Safety Program**

A DOE-approved CSP description document is required by DOE O 420.1C. Reference to this CSP description document should be made.

This section shall also list the applicable nuclear criticality safety standards that are required for ensuring the subcriticality of fissionable material operations in the facility. The intent is to provide only the requirements that are specific and pertinent to the safety analysis, not a comprehensive listing of all industrial standards or codes or criteria. Some or all pertinent requirements may be incorporated via reference to a separate CSP description document.

Additional information for this section shall include: (1) a general discussion of the criticality control strategy and criticality safety design strategy, its basis, and any design criteria used to ensure subcritical configurations under all normal, credible abnormal, and accident conditions (i.e., ensure that criticality limits are not exceeded); (2) the parameters used for the prevention and control of criticality; and, (3) a description of the basis and analytical approach the facility uses for deriving operational criticality limits.

**[6.3] Criticality Safety Program Elements**

This section shall describe the elements of the CSP that are to perform or maintain a safety function, when relied on, or credited in DSA Chapter 3. The description should include detail regarding how the program element will meet that safety function. It is recommended that a unique identifier be applied to each program element.

A summary table should be generated from the essential program elements discussed above. Such a table summarizes the programmatic elements and provides a link to the safety functions these elements perform or maintain, and a reference to the hazards or accidents requiring those functions.

**[6.4] Supporting Programs and Program Elements**

Typically, a group of programs or processes work together to support the CSP (e.g., configuration management, conduct of operations, training, and work control). In this section, identify the programs and processes that provide key support to the CSP and summarize generally how these programs ensure that a criticality will not occur and provide for appropriate criticality alarm systems when required by the ANS/ANSI standards and DOE-STD-3007.

## DSA [CHAPTER 7: SAFETY MANAGEMENT PROGRAMS]

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 shall be referenced. A brief abstract of referenced documentation shall be included, with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter. See Appendix A, Section A.10 of this Standard for further discussion of safety management programs.

Historically, DSAs have provided individual chapters numbered 7-17 for the following subjects: radiation protection; hazardous material protection; radioactive and hazardous waste management; initial testing, in-service and surveillance, and maintenance; operational safety, comprised of conduct of operations and fire protection; procedures and training; human factors; quality assurance; emergency preparedness; provisions for decontamination and decommissioning; and, management, organization, and institutional safety provisions. The level of detail associated with these chapters was very prescriptive, even though the DSA development guidance stated that the individual chapters were not intended to be the vehicle for review and approval of the associated programs. Therefore, the effort expended in developing and reviewing such chapters is not judged to have yielded commensurate safety benefits.

This revision to DOE-STD-3009 allows these subjects to be treated in one consolidated chapter that is shorter and less prescriptive in content. 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.

**ORGANIZATION AND CONTENT GUIDANCE FOR [CHAPTER 7]**

10 C.F.R. 830.204(b) (5) identifies ninesafety management programs that must be addressed. 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. These programs should be addressed in additional subsections appended sequentially 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 large chemical hazards. Neither of these topics is expected for facilities with small amounts of explosive or chemical hazards that are primarily of concern to facility workers.

The format for these subsections shall be as follows:

**[7.X] Name of Program**

This section describes the program in a few sentences.

**[7.X.1] Governing Documents**

If the program is individually implemented at the facility, the governing facility documents shall be 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 shall be identified, with a summary explanation of their relationship to the safety of the facility. If the program is implemented jointly, both sources shall be identified.

This identification should be restricted to the 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.

**[7.X.2] Program Description**

This section provides a one-paragraph to one-page description of the major elements comprising the program and their role in facility safety.

**[7.X.3] Key Elements**

This section shall provide a summary description of 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 analysis, but not at a level that requires designation as an SAC; or, (2) are not specifically assumed to function for mitigated scenarios, but are recognized by facility management as an important capability that warrants special emphasis. The basis for selection as a key element shall be specified.

This basis should include detail regarding how the program element functions to: (1) manage or control a hazard or hazardous condition evaluated in the hazard analysis; (2) impact or interrupt accident progression as analyzed in the accident analysis; and, (3) provide a broad-based capability relevant to multiple scenarios.

# Appendix A: Technical Background of Key DSA Concepts

This Appendix provides background information, much of which is historical information and philosophy that was used in the development of the original Department of Energy (DOE) Standard (STD) 3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, for documented safety analysis (DSA) development and remains pertinent to the revision, DOE-STD-3009-2012, Criteria and Guidance for Preparation of U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis. The information in this Appendix is intended to provide perspective and technical basis for key elements of the development of a DSA.

**A.1 Standard Industrial Hazards**

Standard industrial hazards are hazards that are routinely encountered in general industry and construction, and for which national consensus codes and/or standards – such as Occupation Safety and Health Administration (OSHA) standards, 10 C.F.R. 851, *Worker Safety and Health Program*, and transportation safety – exist to guide safe design and operation without the need for special analysis for safe designs and/or operational parameters. DSAs do not define safety controls for these hazards. Standard industrial hazards are evaluated in the DSA only to the extent that they act as initiators and contributors to accidents that cause the release of hazardous materials that could seriously injure a worker or the public or could compromise the function of credited safety systems.

Standard industrial hazards specifically include:

* Normal facility or construction hazards, such as hot objects, electrocution, and falling objects;
* Hazards addressed in a national consensus code and/or standard (and whose manner of use is covered by the code or standard);
* Chemical quantities consistent with the scale of laboratory use of chemicals per the Code of Federal Regulations (C.F.R.) in 29 C.F.R. 1910.1450, *Occupational Exposure to Hazardous Chemicals in Laboratories*;
* Materials used in the same form, quantity, and concentration as a product packaged for distribution and use by the general public; and
* General asphyxiation hazards (e.g., confined space entry procedures, dewars, gas piping, and inerting systems in gloveboxes normally operating at less than atmospheric pressure). The potential exceptions, based on situation-specific judgment, would be large sources of cryogenic fluids or pressurized gas held inside a building where an extremely rapid release could occur.

DSAs are not intended to cover safety as it relates to the standard industrial hazards that make up a large portion of 10 C.F.R. 851 compliance, because national consensus codes and/or standards already regulate these practices without the need for special analysis. For example, worker electrocution from electrical wiring faults is not a DSA issue. However, the existence of 440 Volt AC cabling in a glovebox could be identified as an accident initiator of a fire involving hazardous materials.

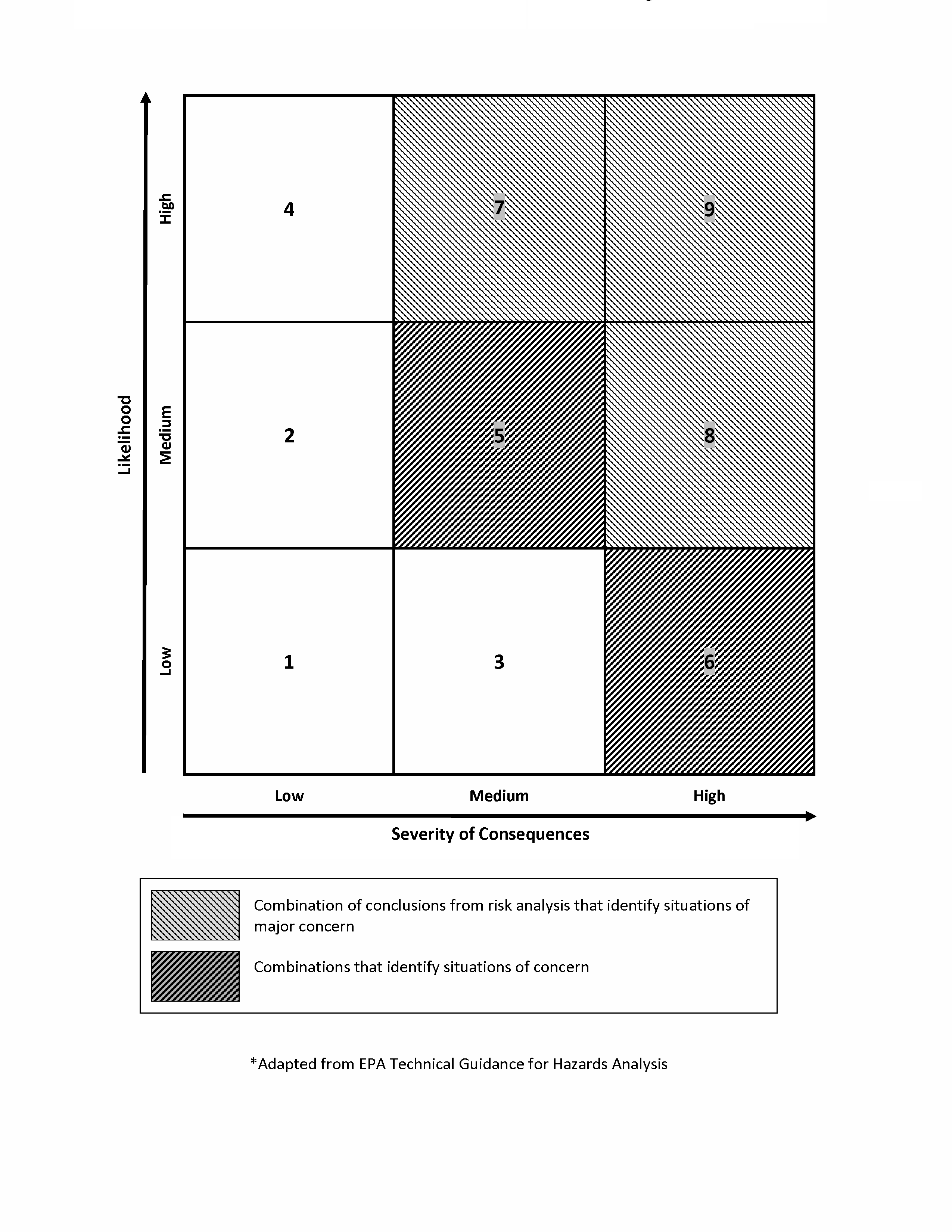
**A.2 Hazard Analysis and Risk Ranking**

As discussed in Section 3 of DOE-STD-3009, the initial analytical effort for all facilities is a hazard analysis that systematically identifies facility hazards and accident potentials through hazard identification and hazard evaluation. The hazard evaluation is required to identify the initiating event, scenario development, associated controls, consequence, and frequency. The latter two parameters are often used in both DOE and industry to specify risk ranking for a given event as well. Risk ranking in this context is a simple mechanism to summarize the event’s significance in terms such as “low, moderate, and high.”

DOE-STD-3009 specifies consequence thresholds for safety structures, systems, and components (SSC) and administrative control (AC) designations. In this regard, frequency estimation is useful to: (1) indicate that an unmitigated event is “beyond extremely unlikely”[[10]](#footnote-10) and, thus, does not require safety SSC designation; (2) provide additional insight for choosing among controls when the same controls address multiple events; and, (3) identify higher-consequence accidents that may warrant more detailed consideration due to higher likelihood. Beyond that, risk ranking serves a broader purpose of confirming for the DOE approver that the overall mitigated risk of facility operation is low. Conversely, it can highlight a given sequence whose mitigated risk remains significant. Risk ranking in DSAs is, therefore, provided primarily for overall perspective. Figure A-1 gives an example risk ranking table that combines frequency and consequence.

Risk ranking in DSAs does not constitute a probabilistic risk assessment (PRA). Instead, it is a fundamentally qualitative or semi-quantitative exercise to gain perspective, not to make a significant and definitive effort to identify residual risk against formal criteria. Selected   
PRA-related tools (e.g., fault and event trees) may be used to the extent they are deemed useful in hazard or accident analysis. Further, risk ranking is not a means to disregard consequences ranked in excess of the safety SSC designation thresholds defined in Chapter 3. Safety SSC and/or AC designation is required for an operational event that exceeds a consequence threshold, regardless of whether the unmitigated frequency is ranked “unlikely” or “extremely unlikely”. However, an unmitigated frequency ranking of “beyond extremely unlikely” is an acceptable way to identify a scenario that is not deemed plausible. Such scenarios do not require safety SSC and/or AC designation.

Although the exercise of binning is essentially qualitative, analysts often use a simple numerical basis for judgments to provide consistency. For example, a simple methodology for frequency binning would be to assign a probability of “1” to non-independent events, “0.1” to human errors, and “0.01” to genuinely independent failures. Safety System failures could be assigned lower probabilities around 0.001. [Note: To determine the frequency of an accident scenario, only initiating events are expressed as frequencies with the units of inverse time, and other events are expressed in terms of unitless probabililities.] Another methodology would be to use a summary of historical data.



**Figure A-1: A Three-by-Three Risk Ranking Matrix for Hazard Evaluation**

**A.3 Criticality Safety**

Criticality represents a special case for hazard evaluation. The criticality safety program controls 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 evaluation demonstrating that all fissionable material operations will be maintained subcritical under both normal and credible abnormal conditions. The standards require consideration of all credible initiating events (e.g., operator errors and natural phenomena hazard events). All necessary controls are identified in criticality safety evaluations that meet the requirements of ANSI/ANS-8.1, *Nuclear Criticality Safety* in *Operations with* *Fissionable Material Outside Reactors,* and DOE-STD-3007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*, and are not selected based on an evaluation of likelihood or consequence. 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 a criticality accident. In addition to hazard evaluation and control identification, the ANSI/ANS-8 criticality safety standards identify numerous requirements and recommendations that result in a robust criticality safety program. These include 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 all the requirements and recommendations of applicable ANSI/ANS-8 series national standards will be implemented (or provide justification for why they will not be implemented) in a criticality safety program description document and submit it for DOE approval.

**A.4 Chemical Hazards**

The DSA identifies chemicals that may present a significant exposure hazard or that could initiate or worsen a radiological release. The DSA is not intended to expend significant analytical resources evaluating chemicals that can be safely handled by implementation of a hazardous material protection program. Therefore, a hazardous chemical material screening process is established to select for DSA evaluation only those chemicals of concern (type and quantity) that are in the facility/activity and present hazard potentials outside the routine scope of the hazardous material protection program.

Hazardous chemicals of concern are those identified with: (a) a threshold quantity value (TQ) in 29 C.F.R. 1910.119, *Process Safety Management of Highly Hazardous Chemicals* (or state-specific equivalent); (b) a TQ in 40 C.F.R. 68.130, *List of Substances*; or (c) a Threshold Planning Quantity (TPQ) in 40 C.F.R. 355, *Emergency Planning and Notification*, Appendix A, *The List of Extremely Hazardous Substances and Their Threshold Planning Quantities*. It is recognized that some DOE sites may handle classified (information not available to the public) substances not on such lists, and such substances should be individually assessed for DSA inclusion. However, the lists cited cumulatively identify the primary chemicals of analytical concern in industry. Further, the DSA should not dismiss these chemicals simply because they are present in quantities less than a TQ or TPQ value. Such chemicals that are maintained in quantities well in excess of laboratory quantities, and that present hazard potentials outside the routine scope of the hazardous material protection program, should be evaluated.

Chemicals that are specifically not required to receive individual analysis in DSAs include:

* Chemicals with no known or suspected toxic properties;
* Materials that have a health hazard rating of 0, 1, or 2, based on National Fire Protection Association (NFPA) 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response*;
* Materials used in the same form, quantity, and concentration as a product packaged for distribution and use by the general public;
* Chemicals in a quantity that can be “easily and safely manipulated by one person,” as determined in accordance with the provisions of 29 C.F.R. 1910.1450(b) (i.e., “laboratory quantities of chemicals”);
* Any solid or liquid materials, even those deemed hazardous, that, because of their physical form or other factors (e.g., plausible dispersal mechanisms, low vapor pressure), do not present an airborne exposure hazard; and,
* Chemicals that can be defined as standard industrial hazards for which national consensus codes and standards provide for safe design and operation. The consensus code or standard needs to be identified and must be applicable to the use of the chemical in the facility that is to be screened from further evaluation.

The basic toxicity of smoke plumes from fires is recognized as inherently dangerous and is not specifically evaluated in a DSA. These are standard industrial hazards that are covered under the fire protection program.

With respect to process systems where asphyxiation of a facility worker could result in accident conditions, the intent is not to address routine asphyxiation hazards. (These are identified as standard industrial hazards in Section A.1.) The intent is to consider safety significant (SS) classification only when: (1) significant quantities of cryogenic material or compressed gases exist in distribution systems within a facility, and (2) failure of the system could result in extremely rapid dispersal and cause an immediately life-threatening condition in the entire room (i.e., there is no opportunity for evacuation). Excluded are refrigerated liquid gas storage pads external to a facility, which are considered to be standard industrial hazards and are of interest only to the extent that release of the liquid gas can realistically create conditions (e.g., in controls room or at nearby nuclear facilities) capable of initiating an accident that releases radioactive or hazardous material.

**A.5 Evaluation Basis Accidents**

Design basis accidents (DBAs) have traditionally been used in nuclear facility applications to inform facility design and explicitly identify the controls that are relied on to protect the public against significant radiological releases. A conceptually different approach is needed for existing facilities, where DBAs are typically either non-existent or irrelevant for a variety of reasons, such as changes in the original mission or early design philosophies. For existing facilities, the concept of the evaluation basis accident (EBA) was developed to identify the controls that protect the public through an analysis of the safety of the facility “as is.” The EBAs are derived from the hazard scenarios identified during the hazard analysis process, and EBA analysis involves an evaluation of the adequacy of the existing controls protecting the public, and the possible need for corrective or compensatory measures.

**A.6 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 needed safety-class (SC) SSCs. The 25 rem TEDE EG is not a safety standard because it does not define an acceptable or unacceptable dose from an accident. DOE does not find any accident acceptable and requires appropriate measures be taken to avert and mitigate all accidents.

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 the 25 rem value provides a significant margin of safety for acute radiation risk.

Although a 25 rem dose is known to increase the risk of cancer, the risk is low, particularly as applied in DOE-STD-3009. An actual 25 rem dose would hypothetically increase an individual’s risk of cancer by 1.5%, assuming a risk of fatal radiation-induced cancer of 6x10-4 per rem (15 cases per per 1000 exposures). However, given the fact that the accidents being evaluated and compared to the EG are high consequence but low frequency (not likely to occur) and because the 25 rem criterion is applied at the boundary, there is ample assurance that the DOE’s Nuclear Safety Goal (DOE Policy 420.1) will be satisfied by the use of the EG consistent with DOE-STD-3009.

To put the EG dose in perspective, it 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.

Requirements for commercial nuclear power plants include the 25 rem siting criterion. Note 7 of 10 C.F.R. 50.34, *Contents of Applications, Technical Information*, specifically states that “*its use is not intended to imply that this number constitutes an acceptable limit for an emergency dose to the public under accident conditions.*” Rather, it states that “*this dose value has been set forth…as a reference value, which can be used in the evaluation of plant design features with respect to postulated reactor accidents in order to assure that such designs provide assurance of low risk of public exposure to radiation, in the event of such accidents*.”

**A.7 Worker Safety**

Workers, typically those in close proximity to operations, are the population principally at risk from potential consequences associated with hazard category 2 and 3 facilities. The DOE recognizes, via 10 C.F.R. 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 DOE-STD-3009 requires answering the fundamental question of how worker safety is most appropriately addressed in the DSA.

OSHA has published 29 C.F.R. 1910.119, *Process Safety Management of Highly Hazardous Chemicals*, which applies to some DOE facilities. The requirements in this OSHA standard are intended to eliminate or mitigate the consequences of releases of such materials as certain hazardous chemicals and flammable liquids and gases. Many of the topics requiring coverage in the OSHA standard, such as design codes, standards, process hazard analysis, human factors, and operator training, are parallel to the requirements in 10 C.F.R. 830.

10 C.F.R. 851, DOE O 440.1B, *Worker Protection Program for DOE (Including the National Nuclear Security Administration) Federal Employees,* and the OSHA rule address the issue of worker safety with respect to process accidents by requiring the performance of hazards analyses for processes (exclusive of standard industrial hazards) in conjunction with basic safety programs that discipline operations and ensure judgments made in hazard analyses are supported by actual operating conditions. These requirements effectively integrate programs and analyses into an overall safety management structure without requiring quantitative risk assessment. This integration and the basic concepts of process safety management described by OSHA regulations and the manuals and codes of practice described in DOE Order 440.1B are philosophically accepted as appropriate for DSAs. DOE-STD-3009 effectively merges process safety management principles with traditional DSA precepts. Section A.4 of the Appendix provides a discussion of the approach to addressing chemical hazards.

**A.8 Defense-in-Depth**

Defense in depth is a fundamental approach to hazard control for nuclear facilities that is based on several layers of protection with successive barriers to prevent the release of hazardous material to the environment. This concept is based on creating multiple independent and redundant layers of defense to compensate for potential 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. Normal safe operation of nuclear facilities relies upon a high level of design quality so that robust, reliable, passive SSCs will prevent the release of hazardous materials and perform their required functions with high reliability and high tolerance against degradation. This safe practice is complemented by reliance on competent operating personnel who are well trained in operations and maintenance procedures. Personnel competence translates into fewer malfunctions, failures, or errors and thus minimizes challenges to the next layer of defense.

If the intended design is compromised by either equipment malfunction (from whatever cause) or operator error and there is a progression from the normal to an abnormal range of operation, the next layer of defense-in-depth is relied on. This layer is focused on accident management and can consist of: (1) automatic systems, or (2) a means to alert the operator to take action or manually activate systems that correct the abnormal situation and halt the progression of events toward a serious accident.

The next layer of defense-in-depth provides for mitigation of the consequences of accidents. Passive and automatically or manually activated features (e.g., containment or confinement system, deluge systems, filtered exhaust), and/or certain safety management programs (e.g., emergency response) minimize consequences in the event that all other layers have been breached. Emergency response actions represent a final measure of protection for releases that cannot be prevented and should not be relied on as a substitute for implementation of defense-in-depth principles.

DOE O 420.1C describes attributes of defense-in-depth that must be included in the design for new nuclear facilities. Many of these same attributes should be applied to the hazard control strategy for existing DOE non-reactor nuclear facilities to a degree they can be achieved and as tailored based on the provisions of a graded approach. For example, an existing legacy Hazard Category 2 facility with chemical processing operations might not be able to demonstrate that it was designed with conservative design margins or the quality assurance pedigree of a new facility. However, it would still be expected to have multiple barriers such as robust confinement, equipment that monitors facility conditions and responds to upset conditions to disrupt accident progression, and mitigative controls that minimize consequences of radiological releases. These layers of protection would be expected to rely primarily on engineered features. On the other hand, a Hazard Category 2 facility with simple operations or a Hazard Category 3 facility, while still expected to incorporate multiple layers of protection, could have a comparatively higher occurrence of equipment in combination with administrative controls.

**A.9 Specific Administrative Controls and Safety Management Programs**

SC and SS controls were historically understood to be SSCs. Important controls may also include specific administrative controls (SACs), which are ACs that 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-3009, along with DOE-STD-1186, *Specific Administrative Controls,* provides guidance applicable to these types of controls. In general, SSCs are preferable to ACs or SACs due to the inherent uncertainty of human performance. SACs may be used to help implement a specific aspect of a program AC that is credited in the safety analysis and therefore has a higher level of importance.

A number of safety management programs are identified in Chapter 3 of DOE-STD-3009 as generically included in the TSR document for worker safety. Specific elements of safety management programs are sometimes designated as well, usually in concert with SSCs or SACs.

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 (e.g., requiring respirator use routinely for normal operations rather than crediting an available SSC) or SACs. However, crediting program elements together with SSCs or SACs can be necessary to acknowledge control provisions that prevent generalized insults. .

**A.10 Safety Management Programs**

10 C.F.R. 830.204(b)(5) and 830.204(b)(6) require that the DSA define the characteristics of the safety management programs necessary to ensure the safe operation of the facility. Program commitments (e.g., radiation protection, maintenance, and quality assurance) encompass a large number of details that are more appropriately covered in specific program documents (e.g., plans and procedures) external to the DSA. 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 can 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”, as described in Section 4 of DOE-STD-3009), 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 gross as to render the premises of the summary invalid.

By virtue of the application of the graded approach, most of the engineered features in a facility will not be identified in the categories of SC or SS SSCs even though they may perform some safety functions. However, such controls noted as a barrier or a preventive or mitigative feature in the hazard and accident analyses must not be ignored in managing operations. For example, the commitment to a maintenance program means that the preventive and mitigative equipment identified as such in the DSA hazard analysis is included in the facility maintenance program, and the facility operating contractor must manage these controls in accordance with safety management programs. Where safety management programs or program elements are relied on to perform a safety function required by the safety analysis, it is important to capture this information in the programmatic sections of the DSA and include them in the TSR document as appropriate. As a minimum, all aspects of defense-in-depth identified must be covered within the relevant safety management programs (e.g., maintenance, quality assurance) committed to in the DSA. The details of that coverage are developed in the maintenance 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 (i.e., 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 for which a number of details may vary without affecting the global commitment.

**A.11 Initial Conditions**

Both hazard and accident analysis utilize initial conditions (ICs). ICs are specific assumptions regarding a facility and its operations that are included in an unmitigated or mitigated evaluation to facilitate manageable scenario definition. As discussed in Sections 3.2.2 and 3.2.3 of DOE-STD-3009, facilities should be analyzed as they exist (or are designed) when quantifying meaningful release mechanisms.

Specific examples of ICs include:

* A vault/building can withstand natural phenomenon hazard (NPH) events that it is designed to based on its NPH Design Category (e.g., NDC-2, NDC-3);
* Solid transuranic waste is contained in a certified 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.

It is important to define ICs carefully and to document them to ensure they are appropriately controlled.

**A.12 Hierarchy of Controls**

DOE O 420.1C and DOE-STD-1189 require that new facilities establish a control selection strategy based on a hierarchy of controls that addresses potential hazardous material release events, throughout all stages of DOE hazard category 1, 2, and 3 nuclear facility design, construction, operation, and decommissioning. This hierarchy is based on the following order of preference:

* Minimization of hazardous materials;
* Engineered safety structures, systems, and components (SSCs) are preferred over Specific Administrative Controls (SACs);
* Passive SSCs are preferred over active SSCs;
* Preventive controls are preferred over mitigative controls; and
* Facility safety SSCs are preferred over personal protective equipment (PPE).

When controls are being considered, controls closest to the hazard are preferred since they will provide protection to the largest population of potential receptors, including facility workers and the public. Controls should also be sought that are effective in the case of multiple hazards to ensure the most effective utilization of resources.

For new hazard category 1, 2, and 3 nuclear facilities constructed utilizing DOE-STD-1189, passive engineered SSCs are required to be an integral part of the design with additional mitigative features providing for layers of protection within the philosophy of defense-in-depth.

For existing DOE hazard category 1, 2, and 3 nuclear facilities, it is not always possible to strictly follow the explicit hierarchy of controls. In those cases, Section 3.3 of this Standard establishes the need for the DSA to provide a technical basis for the established controls. In these cases, consideration should still be given to potential upgrades or modification of engineered features such that the final suite of controls does not have sole reliance on administrative controls.

# Appendix B: DSA Development for a New Facility and for Major Modifications to Existing Facilities Designed Under DOE-STD-1189

**B.1 Introduction**

This Appendix to Department of Energy (DOE) Standard (STD) 3009 provides guidance on preparing an initial documented safety analysis (DSA) for facilities that have been designed under the requirements of DOE-STD-1189, *Integration of Safety into the Design Process*. Guidance is also provided for updating DSAs for major modifications of existing facilities.

The main body of DOE-STD-3009 focuses primarily on existing hazard category 2 and hazard category 3 facilities designed prior to the issuance of DOE-STD-1189 and under different safety design requirements. The implementation of these requirements in facility design and associated safety analysis was usually less formally documented than under the DOE-STD-1189 process. DOE-STD-3009 was developed to support the establishment and documentation of the safety of existing facilities to meet updated safety basis requirements.

The “safety in design” process for new facilities designed under the requirements of DOE-STD-1189 provides for the adequacy and acceptance by DOE of the safety design basis through reviews and approvals 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 that incorporated “safety in design” concepts and the requirements of DOE-STD-1189. Consequently, the review and approval of the DSA is expected to focus on changes since the approval of the PDSA and on the coverage of contents not addressed in the PDSA.

The safety design basis documented in the PDSA should be preserved within the DSA. The DSA should include any changes made to the safety basis since the approval of the PDSA and should address additional requirements for the DSA (i.e., beyond those for a PDSA).

New projects exempted from DOE-STD-1189 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 applied in accordance with existing contracts and guidance from the Safety Basis Approval Authority for the project.

**B.2 Relationship of a DSA with a PDSA Developed Under DOE-STD-1189 Guidance**

DOE-STD-1189, Appendix I (Preliminary and Final Design Stage Safety Documentation) contains format and content guidance for a PDSA. This guidance is based on the outline of DOE-STD-3009 for DSA Chapters 1 though 6. This similarity is intentional, in order to facilitate the transition from a PDSA to a DSA, consistent with the general guidance of DOE-STD-3009.

DOE-STD-1189, Appendix I calls for more specific and detailed information than what the main body of DOE-STD-3009 specifies for a DSA. This is especially true for PDSA Chapter 3, “Hazard Analysis, Accident Analysis, and Control Selection,” and PDSA Chapter 4, “Safety Structures, Systems and Components (SSCs) for Preliminary Design,” which use the safety classification criteria and guidance in DOE-STD-1189, Appendices A through D (which are more specific for seismic design classification and safety significant (SS) classification than those in DOE-STD-3009). The 25 rem evaluation guideline and dose comparison calculation guidance of Section A.3 of Appendix A of DOE-STD-3009-94 were adopted by DOE-STD-1189 for new and major modifications to DOE nuclear facilities. The information on SSCs to be presented in PDSA Chapter 4 results from the “safety in design” activities under DOE-STD-1189, and is more detailed and complete than expected in Chapter 4 of DOE-STD-3009 for an older facility, where a compromise between available information and complete design reconstitution is necessary.

Finally, a new appendix for a PDSA (see Appendix I of DOE-STD-1189) is specified that includes a system-level crosswalk between the safety design requirements and guidance of DOE Order (O) 420.1C, *Facility Safety* (under which it was designed) and its associated guides and standards, and the design approach used for selected safety SSCs. The information in this Appendix should be incorporated in Chapter 4 of the operational DSA and checked for consistency and completeness.

This enhanced level of safety design basis information should be preserved in the operational DSA for a new facility and should serve as the baseline of information for its safety basis. It will also facilitate any needed unreviewed safety question screening and determinations.

**B.3 Tasks to be Accomplished in Transitioning from a PDSA to a DSA for a New Facility**

The following steps must be accomplished in developing a DSA:

* Update Chapter 4 to reflect attributes of the final design safety SSCs and specific administrative controls.
* Complete development of Chapter 5, “Derivation of Technical Safety Requirements (TSRs).” according to the guidance in the main body of DOE-STD-3009. (Note that the PDSA covers preliminary TSR derivation only.)
* Add the description of safety management programs according to the guidance of DOE-STD-3009.
* 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. DOE-STD-1189 addresses the transition from final design to readiness for operations in Chapter 3, Section 3.5, “Construction, Transition, and Closeout.” The PDSA approval may be conditional on completing some design or safety analysis tasks. In addition, the final facility might include:
  + Government-furnished equipment that was not addressed during facility design;
  + Late changes in design resulting from problems or circumstances discovered during construction or checkout and testing activities; and,
  + Any 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, addressing configuration management of the PDSA relating to the topics discussed in Section 3.5 of DOE-STD-1189. (It also describes criteria for determining when the PDSA needs to be updated via a revision.)
* Initiate development of a facility-specific unreviewed safety question procedure.

**B.4 Incorporation of Information from a PDSA into a DSA for a Major Modification**

The safety design basis for a major modification of an existing facility, which is established in the PDSA for the modification, must be incorporated into the facility’s DSA.

Section A.3 of DOE-STD-1189, Appendix A provides the seismic design classification and co-located worker SS criteria (for a major modification of an existing facility not designed under the guidance of that standard) that should be used, with the following caveats:

* Backfit analyses should examine the need to upgrade interfacing SSCs in accordance with these criteria; and,
* Relief may be requested from the design requirements implied by application of these criteria in design. These considerations should be documented in the PDSA if relief is requested.

If the major modification is a completely new building segment with new safety SSCs, the safety classification criteria and guidance of DOE-STD-1189, Appendices A, B, and C, would normally be expected to be applied during design and carried into the DSA for that segment. For major modifications that are integral to an existing facility (e.g., a change to a process line in the facility), the backfit analyses described in DOE-STD-1189, Appendix A, Section A.3 might be expected to be invoked in some cases.

In either case, Chapter 2 of the existing DSA must be updated to include the changed facility description. Chapter 3 must include the hazard analyses, safety system identifications, and safety classification determinations associated with the modification from the PDSA. Chapter 4 must include, for any safety SSC involved with the modification (including interface with existing safety SSCs), the design and design adequacy information from the PDSA, and a summary of any backfit analyses that were performed if the safety SSCs were not classified in accordance with the criteria of DOE-STD-1189. Chapter 5 will need to be updated for any changed or new TSR bases associated with the modification. The safety management program descriptions should be reviewed and revised as necessary to reflect the modifications.

1. The intent is to identify the maximum, physically possible consequence (i.e., no specific controls are assumed to function). Section 3.2 provides the methodology for unmitigated consequence determination in accident analysis. This discussion is applicable to hazard analysis as well.

   The frequency of the unmitigated scenario in the hazard analysis is simply an order-of-magnitude frequency category in the absence of SSC intervention. It is based on the initiating event frequency, modified to consider the physical likelihood of achieving the end state associated with the unmitigated consequence. [↑](#footnote-ref-1)
2. For new facilities and major modification, this DOE Standard dictates the quantitative evaluation of co-located worker dose utilizing a generic χ/q. For existing facilities that may be performing a re-evaluation of co-located worker impact, this approach is also recommended. [↑](#footnote-ref-2)
3. For facilities designed in accordance with DOE-STD-1189, the set of accidents is called the design basis accidents. Appendix B of this Standard discusses the development of the DSA based upon a PDSA developed in accordance with DOE-STD-1189. [↑](#footnote-ref-3)
4. For example, if the presence of an assumed passive SSC prevents significant consequences, it should be classified as wither SS or SC. [↑](#footnote-ref-4)
5. This goal is not associated with a particular value, and therefore is not an explicit requirement. [↑](#footnote-ref-5)
6. This goal is not associated with a particular value, and therefore is not an explicit requirement. [↑](#footnote-ref-6)
7. Comparisons to design codes and standards, as well as nuclear safety design criteria of DOE O 420.1C, help to demonstrate adequacy of safety SSC(s). [↑](#footnote-ref-7)
8. Physically possible operational events resulting in high offsite radiological consequences must be moved forward into accident analysis for determination of safety classification of controls, without consideration of frequency. [↑](#footnote-ref-8)
9. As discussed in Section 3.2 and in Appendix A, Section A.5, for existing facilities the term Evaluation Basis Accident can be used in place of DBAs. [↑](#footnote-ref-9)
10. Note again, that these are qualitative determinations in hazard analysis. In this context, Beyond Extremely Unlikely means that the aggregate physical events needed to reach the hazardous condition of concern become unreasonable to postulate. A determination that an event is not plausible does not factor in failure frequencies for controls; it may only consider generic physical capabilities (i.e., any steel pipe will have a leak frequency less than “X”), physical geometry, and egregious levels of human error. [↑](#footnote-ref-10)