TS

NOT MEASUREMENT SENSITIVE

DOE-STD-3009-94
July 1994

CHANGE NOTICE NO.1
January 2000

CHANGE NOTICE NO. 2
April 2002

CHANGE NOTICE NO. 3
March 2006

DOE STANDARD

PREPARATION GUIDE FOR U.S DEPARTMENT OF ENERGY NONREACTOR NUCLEAR FACILITY DOCUMENTED SAFETY ANALYSES

U.S. Department of Energy
Washington, DC 20585

AREA SAFT

Change Notice No. 3 DOE-STD-3009-94
March 2006

Preparation Guide for U.S. Department of Energy
Nonreactor Nuclear Facility Documented Safety Analyses

Table of Changes

Section	Change
Foreword	Updated contact information
Guiding Principles	Added paragraph on Specific Administrative Controls
Definitions	Added SAC definition
Abbreviations and Acronyms	Added SAC acronym
Introduction	Revised to include SAC information, including Figures I-1 and I-2
Chapter 3: Purpose	Purpose of Chapter 3 - Added "SACs" to the second item under the fourth bullet
Chapter 3 section 3.3	Revised Figure 3-1 to include SAC in process
Chapter 3 section 3.3.2.3	Revised Figure 3-2 to include SAC in worker safety evaluation
Chapter 3 section 3.3.2.3.2	Added "SACs" Added new last paragraph in this section.
Chapter 3 section 3.3.2.3.3	Added "and SACs" in bullet statement on top of the page. Second paragraph, changed "two" to "three" Added second bullet statement "specific administrative controls" Added new fifth paragraph in this section on SACs ("Identify specific administrative controls . . .")
Chapter 3 section 3.4	Added "SACs" in third paragraph Revised Figure 3-4 to include SAC
Chapter 3 section 3.4.2.X.5	Added "SACs" to title of this section, and inserted "(or equivalent SAC)" in the first sentence of this section.
Chapter 4 Introduction	Revised to include SAC information.
Chapter 4 section 4.5	Added new section 4.5 Specific Administrative Controls
Chapter 5 Purpose	Added "(SACs)"
Chapter 5 Application of the Graded Approach	Added last paragraph to address SACs.
Chapter 5 section 5.3	Added "or SACs" in three places.
Chapter 5 section 5.5.X.3	Added last sentence in the section regarding SACs

Change Notice No. 2 DOE-STD-3009-94
April 2002

Preparation Guide for U.S. Department of Energy
Nonreactor Nuclear Facility Documented Safety Analyses

Table of Changes

Section	Change
Whole document	Requirements from DOE Order 5480.23 were replaced by those from 10 CFR 830.
Whole document	Terminology was made consistent with 10 CFR 830.
Whole document	References to DOE Orders 5480.21, 5480.22, and 5480.23 were replaced by references to 10 CFR 830.
Whole document	References to specific revision numbers of documents were deleted since most recent edition of the document applies.
Whole document	References to other documents were updated.
Whole document	The term “Evaluation Guidelines” was changed to “Evaluation Guideline”.
Foreword	National Nuclear Security Administration was added as an applicable organization.
Foreword	Address for beneficial comments was changed.
13 / Table I-1	Table I-1 was deleted because it refers to the 5480.23 Order, rather than the 10 CFR 830 rule.

Change Notice No. 1 DOE-STD-3009-94 January 2000

Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports

Section	Change
Table of Contents	Appendix A information inserted.
Definitions	Appendix A referenced under **Evaluation guidelines.**
Introduction	Appendix A referenced under **Accident Analysis.**
Introduction	Appendix A referenced at the end of **Safety-class structures, systems, and components.**
Chapter 3	Appendix A referenced in 3.3.2.3.5 **Accident Selection,** relating to **Figure 3-4, Flowchart for performing an accident analysis.**
p. A-1 / Appendix A	Insert Appendix A in back of document

Foreword

1. This Department of Energy (DOE) Standard (STD) has been approved for use by the Department of Energy, including the National Nuclear Security Administration (NNSA), and its contractors. Any reference to a document (e.g., DOE standards, orders, and guides) refers to the most current version.)
2. Beneficial comments (recommendations, additions, and deletions) and any pertinent data that may be of use in improving this document should be addressed to either one or both of the following:

Richard Englehart
Office of Nuclear and Facility Safety Policy
EH22, 270 CC
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874
Phone: (301) 903-3718
Facsimile: (301) 903-6172
Email: Richard.Englehart@eh.doe.gov

Richard Black
Office of Nuclear and Facility Safety Policy
EH-22, 270 CC
U. S. Department of Energy
19901 Germantown Road
Germantown, MD 20874
Phone: (301) 903-0078
Facsimile: (301) 903-6172
Email: Richard.Black@eh.doe.gov

3. The 10 CFR Part 830 Rule imposes requirements for nuclear facility documented safety analyses (DSAs). The Department of Energy recognizes a benefit from guidance on the interpretation and implementation of this Order to provide safety assurance for all relevant facilities. This Standard represents a "safe harbor" for the preparation of a DSA.

   The Department of Energy safety management approach is built on a hierarchy of documents. At the top are safety policies. Next come safety requirements (Orders and Rules). Below these are safety guides that clarify the requirements. Technical standards, such as this document, support the guides by providing additional guidance into how the requirements should be met.

   DOE-STD-3009, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses," was prepared to be consistent with the Rule requirements. To ensure that DSA developments will be used in compliance with the Rule, it is advised that this Standard be used in conjunction with the Rule.

Guiding Principles

This Standard incorporates and integrates many different approaches regarding DSA format and content. To ensure a consistent application of this Standard among users, the following guiding principles are provided.

- The focus of this Standard is primarily on Hazard Category 2 and Hazard Category 3 facilities.
- Hazard analysis and accident analysis are merged into one chapter (Chapter 3) to ensure that the proper emphasis is placed on identification and analysis of hazards. The hazard analysis distinguishes when accident analysis is required as a function of potential offsite consequence. Guidance for hazard and accident analysis is not based on probabilistic risk assessment (PRA).
- Defense in depth, worker safety, and environmental issues are identified
- Defense in depth as discussed in this Standard, consists of two components:
  - Equipment and administrative features providing preventive or mitigative functions so that multiple features are relied on for prevention or mitigation to a degree proportional to the hazard potential.
  - Integrated safety management programs that control and discipline operation.
- Guidance is provided for evaluating the safety of a facility for which documentable, deterministic design basis accidents (DBAs) do not exist in order to establish bounding accidents (derivative design basis accidents) that envelope the safety of existing facilities. Guidance is also provided on the treatment of beyond design basis accidents.
- Distinction is made between "safety-class (SC) structures, systems, and components (SSCs)," and "safety-significant (SS) structures, systems, and components," and the balance of facility structures, systems, and components. Safety-class structures, systems, and components are related to public protection and are defined by comparison with the numerical Evaluation Guideline (EG). (See Appendix A of this Standard for additional guidance.) Safety-significant structures, systems, and components are identified for specific aspects of defense in depth and worker safety as determined by the hazard analysis. Specific definitions are provided for these two terms.
- Guidance is provided identifying Administrative Controls that are major contributors to defense in depth, which are designated as Specific Administrative Controls (SAC). This Standard, along with DOE-STD-1186 *Specific Administrative Controls*, provides guidance applicable to these types of controls. SACs provide preventive and/or mitigative functions for specific potential accident scenarios, which also have safety importance equivalent to engineered controls that would be classified as safety-class or safety-

significant if the engineered controls were available and selected.

- Consequences from normal operations are addressed in the Radiation Protection, Hazardous Material Protection, and Waste Management chapters.
- Guidance is provided in each chapter on the application of the graded approach.
- A common DSA format (chapter, title, and organization) for all nonreactor nuclear facilities is desirable but not essential. A table is to be provided by the preparer that indicates where the DSA requirements of 10 CFR 830 are addressed. Content needs to be flexible to allow for different facility types, hazard categories, and other grading factors.
- Facility descriptive material is intentionally split to emphasize structures, systems, and components of major significance:
  - Chapter 2, "Facility Description," provides a brief, integrated overview of the facility structures, systems, and components.
  - Chapter 4, "Safety Structures, Systems, and Components," provides detailed information *only* for those structures, systems, and components that are safety class and safety significant. This application of the graded approach will provide for a significant reduction of DSA volume, while maintaining a focus on *safety.*
- The programmatic chapters, including Chapter 6-17 provide a summary description of the key features of the various safety programs as they related to the facility being analyzed. These chapters are not meant to be used as the vehicle for the determination of adequacy of these programs.

Contents

Introduction to DOE-STD-3009

DSA Preparation Guidance

Executive Summary

Content Guidance

CHAPTER ONE

Site Characteristics

Content Guidance

CHAPTER TWO

Facility Description

Content Guidance

CHAPTER THREE

Hazard and Accident Analyses

Content Guidance

CHAPTER FOUR

Safety Structures, Systems, and Components

Content Guidance

CHAPTER FIVE

Derivation of Technical Safety Requirements

Content Guidance

CHAPTER SIX

Prevention of Inadvertent Criticality

Content Guidance

CHAPTER SEVEN

Radiation Protection

CHAPTER EIGHT

Hazardous Material Protection

CHAPTER NINE

Radioactive and Hazardous Waste Management

CHAPTER TEN

Initial Testing, In-Service Surveillance, and Maintenance

CHAPTER ELEVEN

Occupational Safety

CHAPTER TWELVE

Procedures and Training

CHAPTER THIRTEEN

Human Factors

CHAPTER FOURTEEN

Quality Assurance

CHAPTER FIFTEEN

Emergency Preparedness Program

Content Guidance

CHAPTER SIXTEEN

Provisions for Decontamination and Decommissioning

Content Guidance

CHAPTER SEVENTEEN

Management, Organization, & Industrial Safety Provisions

Appendix A, Evaluation Guideline

List of Figures

List of Tables

Definitions

Notes: Origins of the definitions are indicated by references shown in "[ ]" (brackets). If no reference is listed, the definition originates in this Preparation Guide and is unique to its application.

Accident. An unplanned sequence of events that results in undesirable consequences.

Accident analysis. Accident analysis has historically consisted of the formal development of numerical estimates of the expected consequence and probability of potential accidents associated with a facility. For the purposes of implementing this Standard, accident analysis is a follow-on effort to the hazard analysis, not a fundamentally new examination requiring extensive original work. As such, it requires documentation of the basis for assignment to a given likelihood of occurrence range in hazard analysis and performance of a formally documented consequence analysis. Consequences are compared with the Evaluation Guideline to identify safety-class structures, systems, and components.

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

Organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility consistent with the technical safety requirement. In general, the administrative controls section addresses (1) the requirements associated with administrative controls, (including those for reporting violations of the technical safety requirement); (2) the staffing requirements for facility positions important to safe conduct of the facility; and (3) the commitments to the safety management programs identified in the documented safety analysis as necessary components of the safety basis for the facility. [10 CFR 830 Appendix A]

Beyond design basis accident. An accident of the same type as a design basis accident (e.g., fire, earthquake, spill, explosion, etc.) but defined by parameters that exceed in severity the parameters defined for the design basis accident. The same correlation applies to beyond derivative design basis accidents with regard to derivative design basis accidents.

Decommissioning. Those actions taking place after deactivation of a nuclear facility to retire it from service and includes surveillance and maintenance, decontamination, and dismantlement. [10 CFR 830]

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. [10 CFR 830]

Design basis. The set of requirements that bound the design of systems, structures, and components within the facility. These design requirements include consideration of safety, plant availability, efficiency, reliability, and maintainability. Some aspects of the design basis are important to safety, although others are not.

Evaluation Guideline (EG). The radioactive material dose value that the safety analysis evaluates against. The Evaluation Guideline is established for the purpose of identifying and evaluating safety-class structures, systems, and components. On-site Evaluation Guidelines are not required for adequate documentation of a safety basis utilizing the overall process of this Standard. The Evaluation Guideline is discussed separately in Appendix A.

Facility. Any equipment, structure, system, process, or activity that fulfills a specific purpose. Examples include accelerators, storage areas, fusion research devices, nuclear reactors, production or processing plants, coal conversion plants, magnetohydrodynamics experiments, windmills, radioactive waste disposal systems and burial grounds, environmental restoration activities, testing laboratories, research laboratories, transportation activities and accommodations for analytical examinations of irradiated and nonirradiated 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. The flexibility in the definition does not extend to subdivision of physically concurrent operations having potential energy sources that can seriously affect one another or which use common systems fundamental to the operation (e.g., a common glovebox ventilation exhaust header).

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 CFR 830]

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

(1) The relative importance to safety, safeguards, and security;
(2) The magnitude of any hazards involved;
(3) The life cycle stage of a facility;
(4) The programmatic mission of a facility;
(5) The particular characteristics of a facility;
(6) The relative importance of radiological and nonradiological hazards; and
(7) Any other relevant factor. [10 CFR 830]

Hazard. A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to an operation or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation). [10 CFR 830]

DSAs specifically examine those hazards inherent in processes and related operations that can result in uncontrolled release of hazardous material (i.e., chemical or radiological) or process-unique energy sources (e.g., high pressure autoclave). Standard industrial hazards do not require DSA coverage. Standard industrial hazards such as burns from hot objects, electrocution, falling objects, etc., are of concern only to the

degree that they can be a contributor to a significant uncontrolled release of hazardous material (e.g., 115-volt wiring as initiator of a fire) or major energy sources such as explosive energy.

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 hazards analysis examines the complete spectrum of potential accidents that could expose members of the public, onsite workers, facility workers, and the environment to hazardous materials.

Hazard categorization. Evaluation of the consequences of unmitigated releases to categorize facilities or operations into the following hazard categories:

1. Hazard Category 1: The hazard analysis shows the potential for significant offsite consequences.
2. Hazard Category 2: The hazard analysis shows the potential for significant onsite consequences.
3. Hazard Category 3: The hazard analysis shows the potential for only significant localized consequences. [10 CFR 830]

DOE-STD-1027 provides guidance and radiological threshold values for determining the hazard category of a facility. DOE-STD-1027 interprets Hazard Category 1 facilities as Category A reactors and other facilities designated as such by the Program Secretarial Officer.

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 as defined by OSHA in 29 CFR 1910.1200 and 29 CFR 1910.1450; any material assigned a reportable quantity value in 40 CFR 302, Table 302.4; threshold planning quantities in 40 CFR 355 Appendix A; threshold planning quantities in 29 CFR 1910.119; level of concern quantities in EPA's "Technical Guidance for Hazard Analysis—Emergency Planning for Extremely Hazardous Substances"; or materials rated as 3 or 4 in National Fire Protection Association 704 "Identification of the Fire Hazards of Materials."

Limiting conditions for operation (LCO). The limits that represent the lowest functional capability or performance level of safety-related structures, systems, and components required for safe operations. [10 CFR 830]

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

Mitigative feature. Any structure, system, or component that serves to mitigate the consequences of a release of hazardous materials in an accident scenario. [DOE-STD-1027]

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 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 CFR 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 CFR 830. [10 CFR 830]

Process Safety Management (PSM). A process or activity involving the application of management principles as defined in 29 CFR 1910.119, "Process Safety Management of High Hazardous Chemicals."

Programmatic. 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.

Preventive feature. Any structure, system, or component that serves to prevent the release of hazardous material in an accident scenario. [DOE-STD-1027]

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: (1) to provide systematic identification of hazards within a given DOE operation; (2) to describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and (3) to analyze and evaluate potential accidents and their associated risks.

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 CFR 830]

Safety-class structures, systems, and components (SC SSCs). Structures, systems, or components including portions of process systems, whose preventive and mitigative function is necessary to limit radioactive hazardous material exposure to the public, as determined from the safety analyses. [10 CFR 830]

Safety limits (SLs). Limits on process variables associated with those safety-class physical barriers, generally passive, that are necessary for the intended facility functions and which are required to guard against the uncontrolled release of radioactive materials. [10 CFR 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 CFR 830]

As a general rule of thumb, safety-significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in a prompt worker fatality or serious injuries or significant radiological or chemical exposures to workers. The term, serious injuries, as used in this definition,

refers to medical treatment for immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb).

The general rule of thumb cited above is neither an evaluation guideline nor a quantitative criterion. It represents a lower threshold of concern for which safety-significant SSC designation may be warranted. Estimates of worker consequences for the purpose of safety-significant SSC designation are not intended to require detailed analytical modeling. Considerations should be based on engineering judgment of possible effects and the potential added value of safety-significant SSC designation. [DOE G 420.1-1]

[Note: Safety-significant SSC as used in this Standard distinguishes a specific category of SSCs other than safety-class SSCs. It should not be confused with the generic modifier "safety significant" used in DOE orders.]

Safety structures, systems, and components (safety SSCs). The set of safety-class structures, systems, and components, and safety-significant structures, systems, and components for a given facility. [10 CFR 830]

Site boundary. A well-marked boundary of the property over which the owner and operator can exercise control without the aid of outside authorities.

For the purpose of implementing this Standard, the DOE site boundary is a geographic boundary within which public access is controlled and activities are governed by DOE and its contractors, and not by local authorities. A public road 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.

Standard industrial hazards. Hazards that are routinely encountered in general industry and construction, and for which national consensus codes and/or standards (e.g., OSHA, transportation safety) exist to guide safe design and operation without the need for special analysis to design safe design and/or operational parameters.

Specific administrative control (SAC). An administrative control is designated as a SAC if (1) it is identified in the documented safety analysis as a control needed to prevent or mitigate an accident scenario, and (2) it has a safety function that would be safety-significant or safety-class if the function were provided by an SSC.

Technical safety requirements (TSRs). 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 documented safety analysis 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 CFR 830]

To satisfy the intent of this Standard, he administrative equivalent of TSRs should also be assigned for the conditions, the safe boundaries, and the management of administrative controls necessary to ensure the safe operation of the facility and to reduce the potential risk to the public and facility workers from uncontrolled releases of nonradiological hazardous material or energy. Such equivalents designated for control of nonradiological hazards are considered as important to safety as radiological TSRs, and are needed to satisfy the overall process outlined in this Standard for controlling the broad spectrum of hazards in accordance with the requirements of 10 CFR 830. Distinguishing between the

radiological TSRs and their nonradiological equivalents may be necessary due to the potentially different regulatory enforcement structures associated with each. However, such distinction is beyond the scope of this Standard as the DSA only provides information to derive these controls, not formally define them. Accordingly, for the purposes of this Standard, no distinction is made between radiological TSRs and their nonradiological equivalents, and the term TSRs refers to both. TSRs for radiological hazards are formally defined in the separate TSR document required by 10 CFR 830.

Abbreviations and Acronyms

AC	Administrative Controls
ALARA	As Low as Reasonably Achievable
ARF	Airborne Release Fraction
ARR	Airborne Release Rate
CFR	Code of Federal Regulations
CSE	Criticality Safety Evaluation
D&D	Decontamination and Decommissioning
DBA	Design Basis Accidents
DOE	U.S. Department of Energy
DOE-STD	DOE Standard
DR	Damage Ratio
DSA	Documented Safety Analysis
EG	Evaluation Guideline
EH	Office of Environment, Safety and Health
EIS	Environmental Impact Statement
EM	Office of Environmental Management
EPA	Environmental Protection Agency
EPP	Emergency Preparedness Plan
ERPG	Emergency Response Planning Guideline
ES&H	Environment, Safety, and Health
FHA	Fire Hazards Analysis
FMEA	Failure Modes and Effects Analysis
G	Guide
HASP	Health and Safety Plan
HAZOP	Hazard and Operational Analysis
HDBK	Handbook
HEPA	High Efficiency Particulate Air
LCO	Limiting Conditions for Operation
LCS	Limiting Control Setting
LPF	Leakpath Factor
MAR	Material at Risk
MOI	Maximally-exposed Offsite Individual

NEPA	National Environmental Policy Act
NFPA	National Fire Protection Association
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
OSHA	Occupational Safety and Health Administration
OSR	Operational Safety Requirement
P&ID	Process and Instrument Drawing
PDSA	Preliminary Documented Safety Analysis
PHA	Preliminary Hazard Analysis
PRA	Probabilistic Risk Assessment
PrHA	Process Hazards Analysis PSM Process Safety Management
QAP	Quality Assurance Program
RF	Respirable Fraction
SAC	Specific Administrative Control
SC	Safety Class
SL	Safety Limit
SR	Surveillance Requirement
SRID	Standards and Requirements Identification Documents
SS	Safety Significant
SSC	Structures, Systems, and Components
STD	Standard
TEDE	Total Effective Dose Equivalent
TSR	Technical Safety Requirements
USQ	Unreviewed Safety Question

Introduction

This introduction addresses the following major topics related to implementing the requirements of 10 CFR 830.

- **Purpose of DOE-STD-3009**—Indicates scope and general applicability of this Standard.
- **DSA Preparation Conceptual Basis and Process –** Ensures consistent and appropriate treatment of all DSA requirements for the variety of DOE nonreactor nuclear facilities.
- **Hazard Analysis**—Provides final facility hazard categorization and considers and incorporates into programmatic requirements measures to protect workers, the public, and the environment from hazardous and accident conditions. Technical Safety Requirements and safety-significant structures, systems, and components, that are major contributors to worker safety and defense in depth, are identified in the hazard analysis.
- **Accident Analysis**—Designates safety-class structures, systems, and components and safety controls (i.e., TSRs) as a function of the Evaluation Guideline (see Appendix A).
- **Application of the Graded Approach**—Provides a consistent and measured treatment of this concept, including guidance on the minimum acceptable DSA content.

PURPOSE OF DOE-STD-3009

This Standard describes a DSA preparation method that is acceptable to the DOE as delineated for those specific facilities listed in Table 2 of Appendix A, "General Statement of Safety Basis Policy", to Subpart B, "Safety Basis Requirements", of 10 CFR 830. It was developed to assist Hazard Category 2 and 3 facilities in preparing SARs that will satisfy the requirements of 10 CFR 830. Hazard Category 1 facilities are typically expected to be Category A reactors for which extensive precedents for SARs already exist.

Guidance provided by this Standard is generally applicable to any facility required to document its safety basis in accordance with 10 CFR 830. For new facilities in which conceptual design or construction activities are in progress [i.e., Preliminary Documented Safety Analysis (PDSAs)] elements of this guidance may be more appropriately handled as an integral part of the overall design requirements process (e.g., preliminary design to design criteria). The methodology provided by this Standard focuses more on characterizing facility safety (i.e., back-end approach) with or without well-documented information than on the determination of facility design (i.e., front end approach). Accordingly, contractors for facilities that are documenting conceptual designs for PDSAs should apply the process and format of this Standard to the extent it is judged to be of

benefit.

Beyond conceptual design and construction, the methodology in this Standard is applicable to the spectrum of missions expected to occur over the lifetime of a facility (e.g., production, shutdown/standby, decontamination and decommissioning). As the phases of facility life change, suitable methodology is provided for use in updating an existing DSA and in developing a new DSA if the new mission is no longer adequately encompassed by the existing DSA (e.g., a change from production operations to decontamination and decommissioning). This integration of the DSA with changes in facility mission and associated updates should be controlled as part of an overall safety management plan.

A unique element of DSA documentation is the required provisions for decontamination and decommissioning (D&D) as discussed in Chapter 16 of this Standard. This forward looking aspect of facility operations is independent of facility mission and is intended to be a means of ensuring that current facility operations take into account D&D operations that will occur in the future.

For facilities transitioning into D&D, the safety basis of the D&D operations is documented throughout a DSA. This DSA, of which the principal emphasis is on the D&D operations themselves, provides the necessary analysis and supporting information to describe the facilities as they undergo shutdown, deactivation, decontamination, and decommissioning or dismantlement. The facility consists of the physical building, its constituent components, and the actual processes of D&D being performed. Physical buildings and constituent components targeted for D&D are briefly described in Chapter 2, "Facility Description." Detailed descriptions are reserved for the actual D&D processes, which are the focus of evaluation in Chapter 3, "Hazard and Accident Analysis," and Chapter 4, "Safety Structures, Systems, and Components," for each stage of major configuration change. Also included are the temporary engineering and administrative controls used to maintain the safety basis. This description and evaluation would envelop major configurations during the D&D operations for which the authorization basis is sought. This is consistent with the intent of DSAs for operating facilities where all operations conducted are not detailed in the DSA. DSAs for D&D describe in Chapter 16, "Provisions for Decontamination and Decommissioning," assurances that the D&D operations for which approval is being sought are effectively planned and will not result in future, unnecessary D&D activities (e.g., inadequate labeling of characterized hazardous material).

DSA PREPARATION CONCEPTUAL BASIS AND PROCESS

The safety management programmatic requirements identified in 10 CFR 830, and illustrated in Figure I-1, form the boundaries within which the safety analysis is performed and represent the means of assuring safe operation of the facility. 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 grading the level of detail and control needed in specific programs. The result is documentation of the safety basis that emphasizes the controls needed to maintain safe operation of a facility.

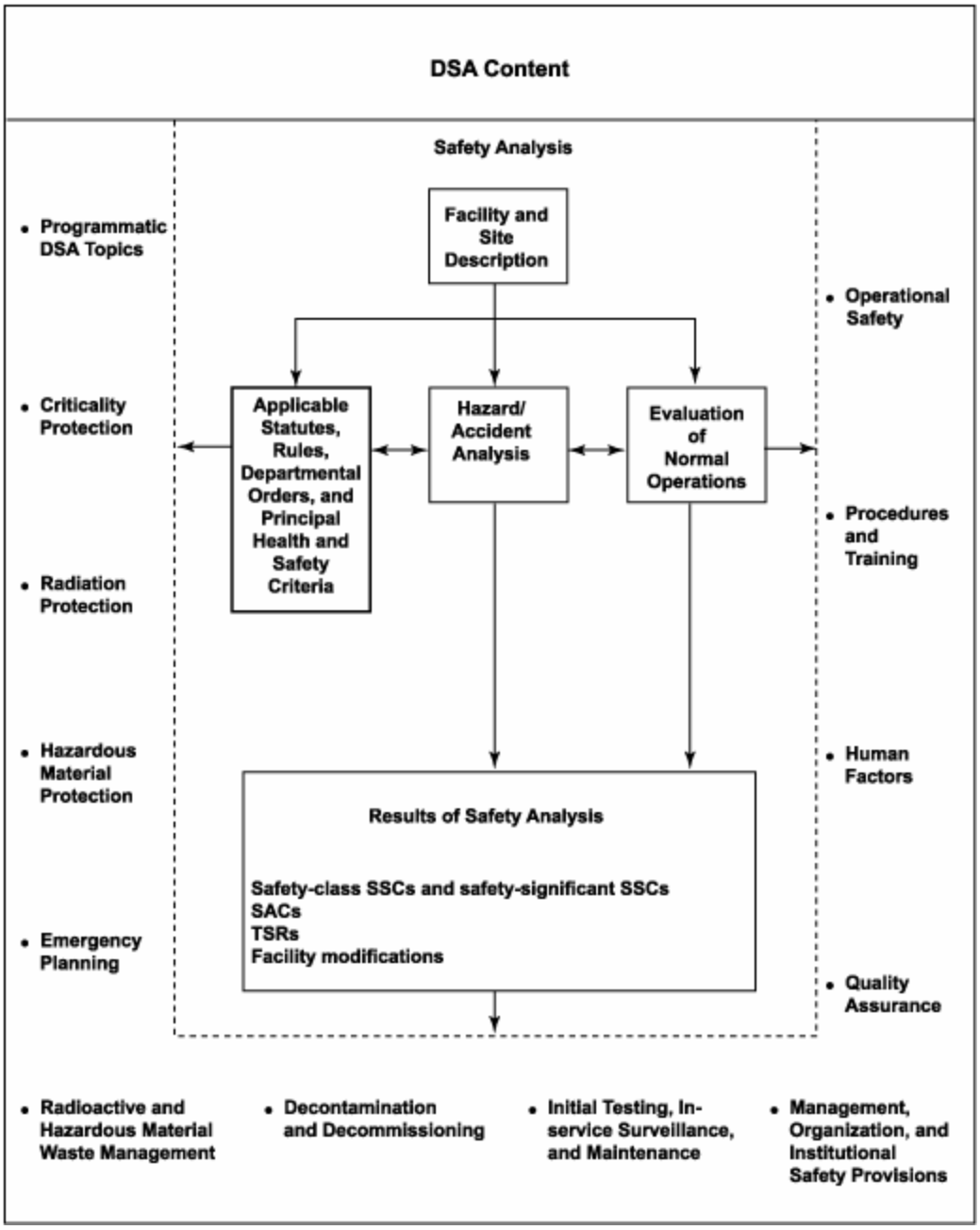


Figure I-1 DSA scope and integration

The DSA preparation process is illustrated in Figure I-2. The level of detail provided in the DSA depends on numerous factors. Applying the guidance for the graded approach in this Standard will assist the preparer in establishing 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 are required to be addressed in the DSA. In determining the makeup of the preparation team, careful consideration should be given to the key hazard analysis activity. In general, the safety analysis base 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 matter such as nuclear criticality, radiological safety, fire safety, chemical safety, or process operations may be needed in the hazard analysis on a regular or as needed basis. Such individuals will typically be necessary in the development of programmatic DSA chapters as well. Consistent, accurate exchange of information among the team members is at least as important as the makeup of the team itself. This can be assured through meaningful integration of the required tasks.

Once team makeup is determined, base information needed to support DSA development is gathered. 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. Other information arises from existing sources such as process hazards analyses (PrHAs), fire hazards analyses (FHAs), explosive safety analyses, health and safety plans (HASPs), environmental impact statements (EISs), etc. The need for additional or specific information becomes apparent throughout the hazard analysis process. The remaining key steps for efficient completion of the safety analysis and the DSA development process are:

- Identify the DSA project functions using project information and ensure the team matches the functions that are required.
- Perform hazard analysis to provide facility hazard classification, evaluate worker safety and defense in depth, and identify unique and representative accidents to be carried forward to accident analysis. Safety-significant SSCs, SACs and TSRs are designated in hazard analysis as well, with a preference given to safety-related SSCs over SACs.
- Perform an accident analysis and assess the results to identify any safety-class SSCs, SACs and accident specific TSRs based on comparison of accident consequences to the Evaluation Guideline.
- Develop the chapters for the DSA by providing information necessary to support the results of the safety analysis. These chapters detail the results of the analysis, describe the facility and the safety SSCs, and the safety management programs that relate to the facility safety basis.
- Prepare the Executive Summary.

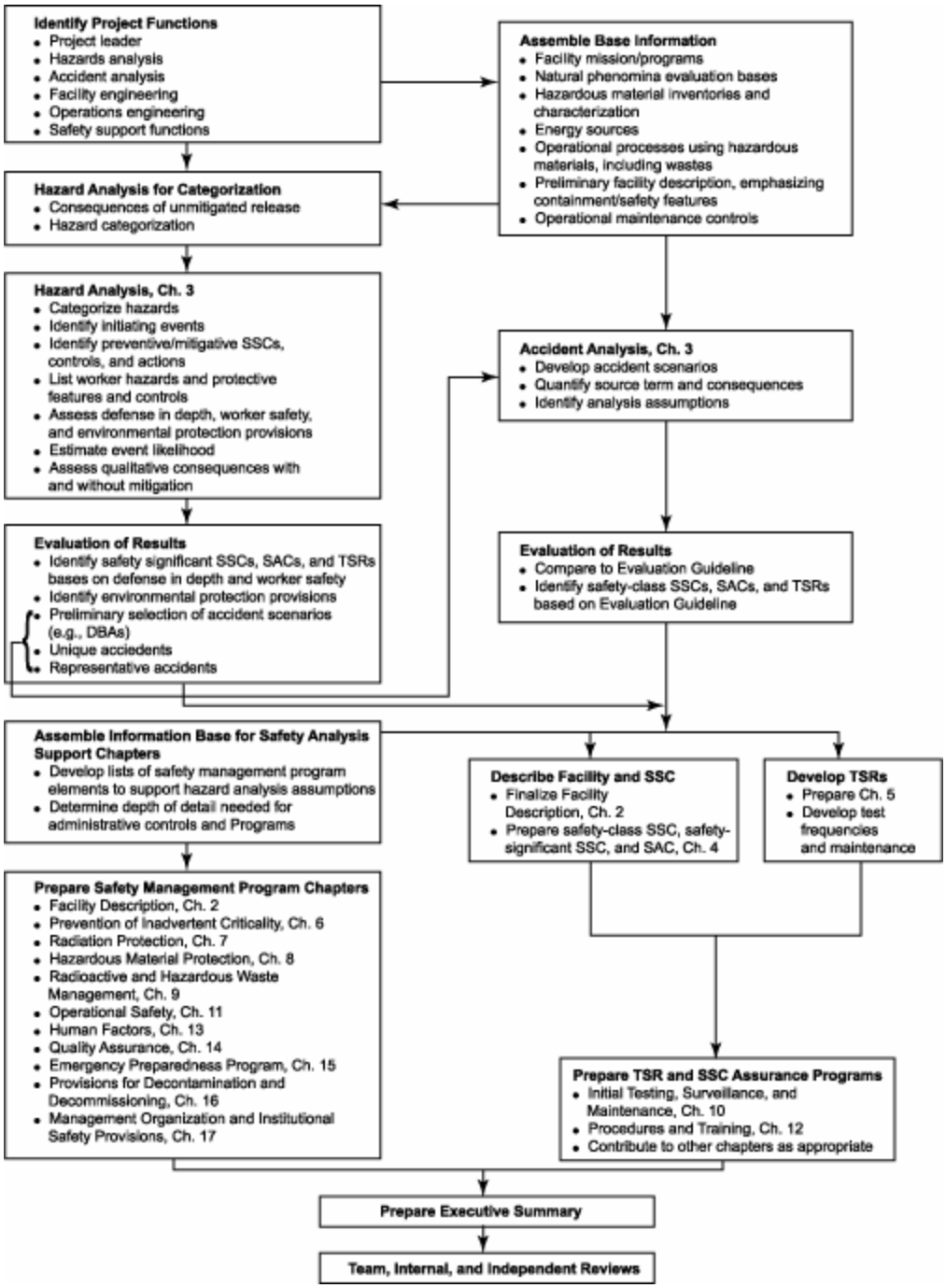


Figure I-2. DSA preparation process

The process of developing a DSA is a process that may require numerous iterations depending on the complexity of the facility and the level of detail required. The hazard and accident analyses (hazard analysis is adequate for Category 3 facilities) are the central elements of this process. The results of the hazard analysis form the basis for grading the level of detail necessary to ensure an acceptable DSA. The hazard analysis specifically identifies safety-significant SSCs and SACs for defense in depth and worker safety, and TSR controls. The results of the accident analysis form the basis for determining additional safety controls imposed on the facility (e.g., safety-class SSCs and TSRs) as a function of the Evaluation Guideline. These specific controls are then factored into overall safety management programs that ensure the operational discipline required by the hazards identified is maintained.

Several specific topics are directly relevant to understanding the conceptual basis of this Standard. These topics are worker safety, defense in depth, programmatic commitments, SSC and TSR commitments, and correlation of this Standard to 10 CFR 830 requirements. The remainder of this section discusses each of these topics in discrete subsections.

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 CFR 830, the importance of including worker safety in safety analyses by specifically noting the worker as a population of concern. Developing a conceptual basis for the methodology used in this Standard requires answering the fundamental question of how worker safety is most appropriately addressed in the DSA.

The Occupational Health and Safety Administration (OSHA) has published 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals." OSHA defines the purpose of this regulation in summary fashion as, "Employees have been and continue to be exposed to the hazards of toxicity, fires, and explosions from catastrophic releases of highly hazardous chemicals in their workplaces. The requirements in this standard are intended to eliminate or mitigate the consequences of such releases." Many of the topics requiring coverage in this federal regulation, such as design codes and standards, process hazard analysis, human factors, training, etc., are directly parallel to the requirements in 10 CFR 830.

DOE O 440.1 and the OSHA standard address the issue of worker safety from process accidents by requiring the performance of hazards analyses for processes (exclusive of standard industrial hazards) in conjunction with implementation of 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 (PSM) described by OSHA regulations and the manuals and codes of practice described in DOE O 440.1 are philosophically accepted as appropriate for DSAs. This Standard effectively merges PSM principles with traditional DSA precepts.

Defense in Depth

Defense in depth as an approach to facility safety has extensive precedent in nuclear safety philosophy. It builds in layers of defense against release of hazardous materials so that no one layer by itself, no matter how good, is completely relied upon. To compensate for potential human and mechanical failures, defense in depth is based on several layers of protection with successive barriers to prevent the release of hazardous material to the environment. This approach includes protection of the barriers to avert damage to the plant and to the barriers themselves. It includes further measures to protect the public, workers, and the environment from harm in case these barriers are not fully effective.

The defense-in-depth philosophy is a fundamental approach to hazard control for nonreactor nuclear facilities even though they do not possess the catastrophic accident potential associated with nuclear power plants. In keeping with the graded-approach concept, no requirement to demonstrate a generic, minimum number of layers of defense in depth is imposed. However, defining defense in depth as it exists at a given facility is crucial for determining a safety basis. Operators of DOE facilities need to use the rigorous application of defense-in-depth thinking in their designs and operations. Such an approach is representative of industrial operations with an effective commitment to public and worker safety and the minimization of environmental releases.

For high hazard operations, there are typically multiple layers of defense in depth. The inner layer of defense in depth relies upon a high level of design quality so that important systems, structures, and components will perform their required functions with high reliability and high tolerance against degradation. The inner layer also relies on competent operating personnel who are well trained in operations and maintenance procedures. Competent personnel translate into fewer malfunctions, failures, or errors and, thus, minimize challenges to the next layer of defense.

In the event that the inner layer of defense in depth is compromised from 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 upon. It can consist of: (1) automatic systems; or (2) 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.

Mitigation of the consequences of accidents is provided in the outer layer of defense in depth. Passive, automatically or manually activated features (e.g., containment or confinement system, deluge systems, filtered exhaust), and/or safety management programs (i.e., emergency response) minimize consequences in the event that all other layers have been breached. The contribution of emergency response actions to minimizing consequences of a given accident cannot be neglected as they represent a truly final measure of protection for releases that cannot be prevented.

Structures, systems, or components that are major contributors to defense in depth are designated as safety-significant SSCs. Additionally, this Standard provides guidance on grading the safety management programs (e.g., radiation protection, hazardous material protection, maintenance, procedures, training) that a facility must commit to compliance in order to establish an adequate safety basis. The discipline imposed by safety

management programs goes beyond merely supporting the assumptions identified in the hazard analysis and is an integral part of defense in depth.

Administrative Controls (AC) that are major contributors to defense in depth are designated as Specific Administrative Controls (SAC) that are required for safety because they are the basis for validity of the hazard or accident analyses, or they provide the main mechanisms for hazard control. This Standard, along with DOE-STD-1186, "Specific Administrative Controls," provides guidance applicable to these types of controls. SACs provide preventive and/or mitigative functions for specific potential accident scenarios, which also have safety importance equivalent to engineered controls that would be classified as safety-class or safety-significant if the engineered controls were available and selected. The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs be 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.

In accordance with nuclear safety precepts, a special level of control is provided through use of TSRs. DOE Guide 423.1-1, "Implementation Guide for Use in Developing Technical Safety Requirements," provides screening criteria for converting existing Technical Specifications and Operational Safety Requirements (OSRs) into TSRs. For the purposes of this Standard, the screening criteria are considered a generally reasonable set of criteria to designate TSRs for defense in depth. The safety items identified in the hazard analysis are examined against those criteria to identify a subset of the most significant controls that prevent uncontrolled release of hazardous materials and nuclear criticality. These TSR controls may be captured in operational limits or in administrative controls, including those on safety management programs. This collection of TSRs formally acknowledges features that are of major significance to defense in depth.

Safety Management Program Commitments

Sections 10 CFR 830.204(b)(5) and 830.204(b)(6) of the Rule 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, 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, are recognized as being important to facility safety, which is the rationale for a top level program commitment becoming part of the safety basis.

As appropriate to the hazard, the safety basis may identify specific controls (e.g., hazardous material inventory limits) that are required for safety. These controls should be considered for designation as a SAC as discussed in this Standard and DOE-STD-1186.

The importance of the program commitments, which can be incorporated in TSRs as administrative controls, cannot be overestimated. The safety basis, however, includes only the top-level summary of program elements, not the details of the program or its governing documents. Inspection discrepancies in a program would not constitute violation of the safety basis unless the discrepancies were so gross as to render premises

of the summary invalid.

By virtue of application of the graded approach, the majority of the engineered features in a facility will not be identified in the categories of safety-class or safety-significant SSCs even though they may perform some safety functions. However, such controls noted as a barrier or preventive or mitigative feature in the hazard and accident analyses must not be ignored in managing operations. Such a gross discrepancy would violate the safety basis documented in the DSA even if the controls are not designated safety-class or safety-significant, because programmatic commitments extend to these SSCs as well. For example, the commitment to a maintenance program means that the preventive and mitigative equipment noted as such in the DSA hazard analysis is included in the facility maintenance program. 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, however, are developed in the maintenance program as opposed to 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., exact type of maintenance items and associated periodicities) are not developed in or part of the DSA.

An overall commitment made in a DSA is that the contractor will not change the facility configuration underlying the documented safety basis without implementing and completing the unreviewed safety question (USQ) process. However, situations do occur where a USQ process is not necessary. For example, a stipulation to have a radiation protection program in the administrative control section of the TSR is a commitment; however, changes to specific program provisions do not require going through the USQ process. Further clarification of such interpretations can be found in DOE G 424.1-1, "Implementation Guide for Use in Addressing Unreviewed Safety Question (USQ) Requirements".

DOE facilities that use and rely on site-wide, safety support services, organizations, and procedures, may summarize the applicable site-wide documentation provided 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. Any documents referenced in the DSA are to be made available upon request.

TSR and SSC Commitments

In order to comply with 10 CFR 830, specific safety controls are to be developed in the DSA. In keeping with the graded-approach principle, distinctions are made to avoid wasting effort by providing detailed descriptions of all facility SSCs. While a basic descriptive model of the facility and its equipment must be provided in Chapter 2, "Facility Description," highly detailed descriptions are reserved for two categories of SSCs comprising the most crucial aspects of facility safety. These two categories are safety-class SSCs and safety-significant SSCs.

Detailed descriptions are provided for safety-class and safety-significant SSCs and SACs in Chapter 4 of the DSA because of the importance of their safety functions. Descriptions result in the definition of functional requirements and associated performance criteria used to derive TSRs. TSRs are safety controls developed in accordance with the precepts of 10 CFR 830. TSR and SSC commitments encompass the following:

Technical safety requirements. TSRs comprise: (1) safety limits (SLs); (2) operational limits consisting of limiting control settings (LCSs) and limiting conditions for operation (LCOs) and associated surveillance requirements (SRs); (3) ACs, (4) SACs, (5) use and application provisions, (6) design features, and (7) Bases Appendix. Based on the results of hazard and accident analysis TSRs are designated for: (1) safety-class SSCs and controls established on the basis of application of the Evaluation Guideline; (2) safety-significant SSCs; (3) defense in depth in accordance with the screening criteria of DOE G 423.1-1; and (4) safety management programs for defense in depth or worker safety. The Bases Appendix provides the linkage to the DSA.

It is important to develop TSRs judiciously. TSRs should not be used as a vehicle to cover the many procedural and programmatic controls inherent in any operation. Excessive use of TSR limits to manage operations will result in distortion of the regulatory structure DOE is attempting to develop and will dilute the emphasis intended for the most critical controls.

SLs should be limited in number and designated with caution. In accordance with Table 4 of Appendix A to Subpart B of 10 CFR 830, SLs are generally reserved for 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. The associated operating limits apply to active SSCs that prevent exceeding SLs. The only candidates for SLs should be safety-class SSCs and any non-SSC controls established on the basis of the application of the Evaluation Guideline. Nuclear industry precedent is that only a limited subset of safety-class SSCs, if any, require definition of associated SLs, which are intended to prevent significant accidents as opposed to mitigating their effects.

TSRs assigned for defense in depth or safety-significant SSCs do not have SLs and are not required to use operational limits (i.e., LCSs, LCOs). They should, however, receive coverage in the administrative control section of TSRs as a minimum. Judgment should be used to determine what controls warrant use of operational limits. When TSR administrative controls are used for purposes other than generic coverage of safety management programs (e.g., SAC), descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why. Beyond safety-significant SSCs designated for worker safety and their associated TSR coverage, additional worker safety issues should be covered in TSRs only by administrative controls on overall safety management programs.

Safety-class structures, systems, and components. The Rule defines safety-class designation for SSCs that are established on the basis of application of the Evaluation Guidelines. This designation carries with it the most stringent requirements (e.g., enhanced inspection, testing and maintenance, and special instrumentation and

control systems). Appendix A provides guidance for implementing the Evaluation Guideline to classify SSCs as safety-class SSCs.

Safety-significant structures, systems, and components. This category of SSCs is provided to ensure that important SSCs will be given adequate attention in the DSA and facility operations programs. Safety-significant SSCs are those of particular importance to defense in depth or worker safety as determined in hazard analysis. Control of such SSCs does not require meeting the level of stringency associated with safety-class SSCs.

The Evaluation Guideline is not used for designating safety-significant SSCs. Safety-class SSCs are designated to address public risk, which makes a dose guideline at the site boundary a useful tool. Safety-significant SSCs address risk for all individuals within the site boundary as well as additional defense in depth for the public, making a dose guideline at any one point an artificial distinction distorting the process of systematically evaluating SSCs.

TSRs covering SSCs ensuring defense in depth should generally correlate with safety-significant SSC designation for defense in depth, but exact one-to-one correlation is not required.

Specific administrative controls. This category of ACs is provided to ensure that controls important to safety that are needed to prevent or mitigate an accident scenario will be given equivalent attention in the safety basis documents had that safety function been provided by a safety-class or safety-significant SSC. Safety analyses shall establish the identification and functions of SACs and the significances to safety of the functions of the SAC. The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs be preferable to ACs or SACs due to the inherent uncertainty of human performance. SACs may be used to help clarify and implement an AC.

HAZARD ANALYSIS

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 focus of the hazard analysis is on thoroughness and requires evaluation of the complete spectrum of hazards and accidents. This largely qualitative effort forms the basis for the entire safety analysis effort, including specifically addressing defense in depth and protection of workers and the environment. Basic industrial methods for hazard analysis, its interface with more structured quantitative evaluations, and the basis for both have been described in references such as the American Institute of Chemical Engineers *Guidelines for Hazard Evaluation Procedures* (1992). OSHA has accepted these guidelines as the standard for analytical adequacy in characterizing commercial chemical processes that perform the same type of unit operations conducted at DOE nonreactor nuclear facilities. Appropriately applied, they help fulfill the requirements of DSAs for Hazard Category 2 and 3 facilities as specified in 10CFR830.

The largely qualitative techniques described in the above reference on hazard analysis provide methodologies for comprehensive definition of the accident spectrum for workers and the public. The basic identification of hazards inherent in the process provides a broad, initial basis for identification of safety programs needed (e.g., radiation protection, hazardous chemical protection). The hazard analysis then moves beyond basic hazard identification to evaluation of the expected consequences and estimation of likelihood of accidents, an activity that in no way connotes the level of effort of a probabilistic or quantitative risk assessment.

Throughout the evaluation process, preventive and mitigative SSCs, and SACs and pertinent elements of programmatic controls are identified. This identification also establishes functional requirements, which will subsequently delineate the technical information (i.e., response parameters) needed to establish performance criteria. The DSA summarizes these requirements and criteria for safety-class and safety-significant SSCs and SACs only. Refinement of the information obtained in hazard evaluation leads to overall definition of defense in depth, worker safety, and environmental protection.

The most significant aspects of defense in depth and worker safety are subject to designation as safety-significant SSCs and coverage by TSRs. Other items noted are encompassed by the details of safety management programs (e.g., procedures, training, maintenance, quality assurance), which can be captured in top-level fashion in TSR administrative controls. However, programmatic administrative controls should not be used to provide preventive or mitigative functions for accident scenarios identified in the safety basis where the safety function has importance similar to, or the same as the safety function of safety-class or safety-significant SSCs. The classification of SAC was specifically created for this safety function. The hazard evaluation conducted to assess the accident spectrum associated with hazards germane to the DSA indicates the adequacy of programmatic efforts and provides input to programmatic activities whose discipline provides a significant margin of safety.

The process outlined above is self-grading for analytical effort. Analytical effort can be limited to a simple, resource efficient hazard analysis geared to facility needs, unless events are noted that are of sufficient complexity to require more detailed, quantitative evaluations to understand the basis for safety assurance. Implicit in this methodology is the statement of DOE-STD-1027 that the largely qualitative level of effort in hazard analysis is appropriate and sufficient for accident analysis of Hazard Category 3 facilities. It is again noted that the hazard analysis effort is not a quantitative risk assessment. Preparers (and subsequent reviewers) cannot expect the level of detail associated with a quantitative risk assessment in a hazard analysis, as the hazard analysis is focused on systematically assessing what can go wrong in a facility as opposed to deriving mathematical expressions of risk.

The final purpose of hazard analysis is to identify a limited subset of accidents to be carried forward to accident analysis. Identification of DBAs in safety analysis and use of DBAs is appropriate in defining a facility safety basis. DBAs are accidents that are utilized to provide the design parameters for release barriers and mitigating systems. DBAs are a “front-end” device for designing individual equipment or systems to meet functional requirements, as evidenced by use of the phrase “utilized to provide the design parameters.” An accident can be defined as a DBA if relevant SSCs were specifically

designed to function during that accident and appropriate documentation of this fact exists.

The range of accident scenarios analyzed in a DSA should be such that a complete set of bounding conditions to define the envelope of accident conditions to which the operation could be subjected are evaluated and documented. This necessitates the consideration of accidents other than DBAs for two cardinal reasons. First, even if DBAs exist, they may not adequately cover "the range of accident scenarios" needed to establish the facility safety basis. Secondly, DBAs may not cover a "complete set of bounding conditions." Either of these conditions may arise for a number of reasons, such as the original design not being related to bounding conditions, the criteria for determining facility safety basis having significantly changed, operations or types of hazards having changed, or magnitude of hazards having increased. Any one of these reasons may make the DBA inadequate for determining a facility safety basis.

The most obvious and extreme reason for examining accidents other than DBAs for existing facilities is a lack of design documentation. If appropriate design documentation is not available, postulated accidents are not DBAs. The front-end purpose of a DBA (i.e., "to provide the design parameters") cannot be meaningfully addressed even if existing design parameters are estimated and used to develop an accident scenario. The reconstructed accident would not determine design parameters. It would be determined by them. The need to analyze a range of scenarios that bound conditions would not clearly be met by such an exercise. This potential lack of relevance is one of the reasons that the DSA is not the proper vehicle for formally filling gaps in existing design documentation.

Where DBAs do not exist, or do not adequately cover the range of scenarios or bounding conditions, surrogate evaluation bases are needed. These derivative DBAs are used to estimate the response of SSCs to "the range of accident scenarios" and stresses that bound "the envelope of accident conditions to which the facility could be subjected" in order to evaluate accident consequences. The derivative DBAs should take maximum advantage of the pertinent existing design information (i.e., requirements and bases) that is immediately available or can be retrieved through reasonable efforts. To the extent necessary, this information can be supplemented by testing, extrapolation, and engineering judgments.

Existing facilities, like all industrial facilities, were generally built with standard process and utility SSCs with a high consideration for basic safety. For the majority of these facilities, adequate facility design and process information exist that, while not of the quality and detail expected for current conceptual design, is typical of many commercial processing operations, which comprise the majority of industrial practices. This information can be used in estimating SSC response to derivative DBAs whose evaluation will satisfy the requirements of safety analysis.

For operational accidents, a derivative DBA is defined based on the physical possibility of phenomena as defined in the hazard analysis. Use of a lower binning threshold such as 10^{-6}/yr is generally appropriate, but should not be used as an absolute cutoff for dismissing physically credible low probability operational accidents (e.g., red oil explosions) without any evaluation of preventive and mitigative features in hazard analysis. This distinction is made to prevent "pencil sharpening" at the expense of objective evaluation of hazards. Examples of a candidate derivative DBA would be an

ion exchange column or a red oil explosion at a facility where the phenomena is physically possible and documentation is not available substantiating ventilation and building confinement systems were specifically designed for such an occurrence. For natural event accidents, derivative DBAs are defined by a frequency of initiator based on DOE 420.1, "Facility Safety", and its associated implementation standards. For external man-made accidents, derivative DBAs are assumed if the event can occur with a frequency $>10^{-6}$/yr as conservatively estimated, or $>10^{-7}$/yr as realistically estimated. Use of a frequency cutoff for external events represents a unique case for external events only, based on established Nuclear Regulatory Commission (NRC) precedents. For simplicity, use of the term DBA throughout this Standard is inclusive of both DBAs and derivative DBAs.

ACCIDENT ANALYSIS

The complete spectrum of accidents is examined in hazard analysis. A limited subset of accidents, (i.e., DBAs and derivative DBAs) that bound "the envelope of accident conditions to which the operation could be subjected" are carried forward to accident analysis where safety-class SSCs are designated by comparison of accident consequences to the Evaluation Guideline. These scenarios are the accidents requiring formal definition. Information obtained from specific accidents or representative accidents enveloping many small accidents is used to specify functional requirements for safety-class SSCs in Chapter 4.

An accident analysis is performed for the bounding accidents. Accident analysis in this Standard refers to the formal quantification (i.e., all assumptions identified and justified and individual computations presented or summarized) of accident consequences. The general binning estimates used in hazard analysis are adequate and representative of the level of effort desired for frequency determination. Accordingly, accident analysis need only document the basis used in hazard analysis for assigning accident likelihood to two-orders-of-magnitude bins. The quantified consequences are compared to the numerical Evaluation Guideline for the purpose of identifying safety-class SSCs and any accident specific assumptions requiring coverage by TSRs.

APPLICATION OF THE GRADED APPROACH

10 CFR 830 prescribes the use of a graded approach for the effort expended in safety analysis and the level of detail presented in associated documentation. The graded approach applied to DSA preparation and updates is intended to produce cost efficient safety analysis and DSA content that provide adequate assurance to the DOE that a facility has acceptable safety provisions without providing unnecessary information. As described in 10 CFR 830, the graded approach adjusts the magnitude of the preparation effort to the characteristics of the subject facility based on seven factors:

- 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.

The Rule provides for developing the DSA based on judgment of the facility in relation to these seven factors. For example, simple Hazard Category 3 facilities or facilities that have a short operational life may only require a limited but adequate analysis documented to 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 to meet the requirements of 10 CFR 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 of these facilities. For facilities of little hazard, or hazards at the Hazard Category 3 level, for which only a modest reduction of risk is required, the DSA may be simple and short. In such cases all of the topics for the DSA listed in this Standard may not be necessary and with proper technical bases some topics may be omitted or reduced in the detail that would otherwise be required of Hazard Category 1 or 2 facilities.

Thus, with application of the graded approach, DSAs for Hazard Category 3 facilities or facilities with short operational lives will normally require more simplified DSA analysis and documentation. Specific minimum levels of detail for these facilities are given in options #3 and #8 in Table 2 of Appendix A to 10 CFR 830 Subpart B and the graded approach section of each chapter in this Standard. As a minimum, a DSA would be found acceptable for a simple Hazard Category 3 facility if it used the methods in Chapters 2, 3, 4, and 5 of this Standard to address in a simplified fashion:

- The basic description of the facility and its operations, including safety structures, systems, and components;
- A qualitative hazards analysis; and
- The hazard controls (consisting primarily of inventory limits and safety management programs) and their bases.

Executive Summary

PURPOSE. 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:

- Summary of the facility background and mission.
- Overview of the facility including location and boundaries.
- Description of the facility hazard category.
- Summary of the results of the facility safety analysis including operational hazards analyzed, DBAs, and significant preventive and mitigative features.
- Summary of the acceptability of the facility safety basis.
- Guide to the structure and content of the DSA (i.e., "road map").

APPLICATION OF THE GRADED APPROACH. This summary is intended as an overview of the facility safety basis and presents information sufficient to provide a basic understanding of the facility, operations, and results of safety analysis. It is prepared upon completion of all the other DSA chapters since it predominately draws upon the information in those chapters (see the Introduction and Figure 1-2). Information provided should be top-level in nature and avoid reproducing the details of material documented in subsequent chapters.

CONTENT GUIDANCE FOR SECTIONS OF THE 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 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) impacting the extent of 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, relationship 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, then provide a brief explanation of 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 to include:

- Description of the facility operations analyzed in the DSA.
- Summary of the significant hazards associated with the facility processes including DBAs.
- Summary of the main preventive and mitigative features relied upon in the facility safety basis.

E.5 ORGANIZATIONS

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

E.6 SAFETY ANALYSIS CONCLUSIONS

This section should provide a brief assessment of the appropriateness of the facility safety basis. As part of this summary, this section would identify any issues significant to the facility safety basis recognized by the facility operators to require 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 appendixes. If the main body of the DSA parallels the format delineated in this Standard, a simple statement to that effect will suffice.

Chapter 1
Site Characteristics

PURPOSE. The purpose of this DSA chapter is to provide information necessary to support the safety basis requirements of 10 CFR 830.

This chapter provides a description of site characteristics necessary for understanding the facility environs important to the safety basis. Information is provided to support and clarify assumptions used in the hazard and accident analyses to identify and analyze potential external and natural event accident initiators and accident consequences external to the facility. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the location of the site, location of the facility within the site, its proximity to the public and to other facilities, and identification of the point where the Evaluation Guideline is applied.
- Specification of population sheltering, population location and density, and other aspects of the surrounding area to the site that relate to assessment of the protection of the health and safety of the public.
- Determination of the historical basis for site characteristics in meteorology, hydrology, geology, seismology, volcanology, and other natural events to the extent needed for hazard and accident analyses.
- Identification of design basis natural events.
- Identification of sources of external accidents, such as nearby airports, railroads, or utilities such as natural gas lines.
- Identification of nearby facilities impacting, or impacted by, the facility under evaluation.
- Validation of site characteristic assumptions common to safety analysis that were used in prior environmental analyses and impact statements, or of the need to revise and update such assumptions used in facility environmental impact statements.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Hazard Category 3 facilities may not have the potential for resulting in significant radiological consequences beyond the immediate facility. Therefore, the description of site characteristics, as a minimum, locates the facility on the overall site, shows the facility boundaries, and identifies any other facilities that can significantly impact the facility being examined. For Hazard Category 3 facilities, onsite meteorological conditions, hydrology, population information, and offsite accident pathways are not typically required, since consequences are limited to the facility itself. Note, however, that if significant chemical hazards are present in a Hazard Category 3 facility that have the potential to cause significant offsite consequences, more information is necessary.

For Hazard Category 2 facilities the emphasis of site characteristics description is focused within site boundaries unless hazards have the potential to cause offsite consequences of concern. For Hazard Category 2 facilities with the potential for an accident resulting in consequences of concern at the site boundary, site characteristics information is extended beyond the site boundary to support assessment of population dose, land contamination, and emergency planning external to the site.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 1

1.1 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.

1.2 REQUIREMENTS

This section lists the design codes, standards, regulations, and DOE Orders that have been used for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific for this chapter and pertinent to the safety analysis, and 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 describes the site boundary and facility area boundary.

1.3.1 Geography

This section provides basic geographic information, such as:

- State and county in which the site is located.

- Location of the site relative to prominent natural and man-made features such as rivers, lakes, mountain ranges, dams, airports, population centers.
- General location map to define the boundary of the site and show the correct distance of significant facility features from the site boundary.
- Public exclusion areas and access control areas.
- Identification of the point where the Evaluation Guideline is applied.
- Additional detail maps, as needed, to present near plant detail, such as orientation of buildings, traffic routes, transmission lines, and neighboring structures.

1.3.2 Demography

Population information based on recent census data is 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, hospitals, etc., to the degree warranted by potential offsite consequences. The minimum area addressed is defined by the area significantly affected by the accidents analyzed in Chapter 3, "Hazard and Accident Analyses."

1.4 ENVIRONMENTAL DESCRIPTION

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

1.4.1 Meteorology

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

1.4.2 Hydrology

This section provides the hydrological information necessary to understand any regional hydrological phenomena of concern for facility operation and 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 provides the geological information necessary to understand any regional geological phenomena of concern for facility operation. 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 provides identification of specific natural events, such as design basis earthquakes considered to be potential accident initiators. Summarize assumptions supporting the analysis in Chapter 3, "Hazard and Accident Analyses."

1.6 MAN-MADE EXTERNAL ACCIDENT INITIATORS

This section provides identification of specific man-made external events associated with the site - events such as explosions from natural gas lines or accidents from nearby transportation activities - considered to be potential accident initiators, exclusive of sabotage and terrorism. Summarize assumptions supporting the analysis in Chapter 3, "Hazard and Accident Analyses."

1.7 NEARBY FACILITIES

This section identifies any nearby facilities that could be affected by accidents within the facility being evaluated. Conversely, this section also identifies any hazardous operations or facilities onsite or offsite that could adversely impact the facility under evaluation. Summarize assumptions supporting the analysis in Chapter 3, "Hazard and Accident Analyses."

1.8 VALIDITY OF EXISTING ENVIRONMENTAL ANALYSES

This section assesses 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.

Chapter 2
Facility Description

PURPOSE. The purpose of this DSA chapter is to provide information necessary to support the safety basis requirements of 10 CFR 830.

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. Expected products of this chapter, as applicable based on the graded approach, include:

- Overview of the facility, its inputs and its outputs, including mission and history.
- Description of the facility structure and design basis.
- Description of the facility process systems and constituent components, instrumentation, controls, operating parameters, and relationships of SSCs.
- Description of confinement systems.
- Description of the facility safety support systems.
- Description of the facility utilities.
- Description of facility auxiliary systems and support systems.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The development of this chapter for Hazard Category 2 and 3 facilities is 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 develop an understanding of facility operations and an appreciation of 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 preventive and mitigative features identified and the degree of facility context necessary to understand the analyses. For a Hazard Category 3 facility, provide a brief description of the facility, processes, and major SSCs. Grading will be based predominantly on complexity.

This chapter does not include information at the level of functional requirements and performance criteria. That information is provided for safety SSCs only in Chapter 4. In the basic description of safety SSCs, their categorization as safety-class SSC or safety significant SSC should simply be noted.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 2

2.1 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.

2.2 REQUIREMENTS

This section lists 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 for 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.

2.3 FACILITY OVERVIEW

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

2.4 FACILITY STRUCTURE

This section provides an overview of the basic facility buildings and structures, including construction details such as basic floor plans, equipment layout, construction materials, controlling dimensions, and dimensions significant to the hazard and accident analysis activity. Supply 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 describes the individual processes within the facility. Include details on basic process parameters, including summary of types and quantities of hazardous materials, process equipment, instrumentation and control systems and equipment, basic flow diagrams, and operational considerations associated with individual processes or the entire facility, including major interfaces and relationships between SSCs. The intent is to supply information to provide an understanding of the assessment of normal operations, the safety analysis and its conclusions, and insight into the types of operations for which a safety management program must be devised.

2.6 CONFINEMENT SYSTEMS

This section identifies and describes the set of structures, systems, and components that perform confinement functions such as process vessels, glove boxes, ventilation systems, and facility walls.

2.7 SAFETY SUPPORT SYSTEMS

This section identifies and describes the principal systems that perform safety support functions (i.e., safety functions not part of specific processes). State the purpose of each system and provide and 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), effluent monitoring, etc.

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

2.8 UTILITY DISTRIBUTION SYSTEMS

This section provides a schematic outline of the basic utility distribution systems, including a description of the offsite power supplies and onsite 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 provides information on the remaining portions of that facility that have not been covered by the preceding sections and which are necessary to create a conceptual model of the facility as it pertains to the hazard and accident analyses

Chapter 3
Hazard and Accident Analyses

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830 to evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or process that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility.

This chapter describes the process used to systematically identify and assess hazards to evaluate the potential internal, man-made external, and natural events that can cause the identified hazards to develop into accidents. This chapter also presents the results of this hazard identification and assessment process. Hazard analysis considers the complete spectrum of accidents that may occur due to facility operations; analyzes potential accident consequences to the public and workers; estimates likelihood of occurrence; identifies and assesses associated preventive and mitigative features; identifies safety-significant SSCs; and identifies a selected subset of accidents, designated DBAs, to be formally defined in accident analysis. Subsequent accident analysis evaluates these DBAs for comparison with the Evaluation Guideline. This chapter covers the topics of hazard identification, facility hazard categorization, hazard evaluation, and accident analysis. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the methodology for and approach to hazard and accident analyses.
- Identification of hazardous materials and energy sources present by type, quantity, form, and location.
- Facility hazard categorization, including segmentation in accordance with DOE-STD-1027.
- Identification in the hazard analysis of the spectrum of potential accidents at the facility in terms of largely qualitative consequence and frequency estimates. The summary of this activity will also include:
    - — Identification of planned design and operational safety improvements.
    - — Summary of defense in depth, including identification of safety-significant SSCs, SACs and other items needing TSR coverage in accordance with10 CFR 830.
    - — Summary of the significant worker safety features, including identification of safety-significant SSCs and any relevant programs to be covered under TSR and administrative controls., including those controls designated as SACs.
    - — Summary of design and operational features that reduces the potential for large material releases to the environment.

  - Identification of the limited set of unique and representative accidents (i.e., DBAs) to be assessed further in accident analysis.

- Accident analysis of DBAs identified in the hazard analysis. The summary of this activity will include for each accident analyzed, the following:
  - Estimation of source term and consequence.
  - Documentation of the rationale for binning frequency of occurrence in a broad range in hazard analysis (detailed probability calculations not required).
  - Documentation of accident assumptions and identification of safety-class SSCs based on the Evaluation Guideline.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The results of the hazard analysis provide a comprehensive evaluation of the complete DSA accident spectrum. This evaluation will be essentially qualitative in that its aim is to produce a well-reasoned and clear assessment of facility hazards and their associated controls. The focus of hazard analysis is on the completeness of consideration given to the accident spectrum, as opposed to a formalized definition of accident sequences and assumptions. Summary discussion of methodology is appropriate, but detailed bases for judgment and any simple mathematical estimates used in the hazard analysis to guide the judgments of the analysis for specific accident scenarios are not required to be formally documented in the DSA. For a small subset of accidents, the accident analysis documents individual calculations in the DSA, including references to its supporting documents. The accident analysis only needs to provide sufficient calculations to support a comparison to the Evaluation Guideline for the purpose of identifying safety-class SSCs.

In general, a graded approach dictates a more thoroughly documented assessment of complex, high hazard facilities than simple, lower hazard facilities since grading is a function of both hazard potential and complexity. The basic elements of hazard identification, categorization, evaluation, and analysis are required for any facility preparing a DSA in accordance with 10 CFR 830. The graded approach for hazard analysis is a function of selecting techniques for hazard evaluation. The techniques used for hazard evaluation can range from simple checklists or What-If analyses to systematic parameter examinations such as Hazard and Operability Analyses (HAZOPs). The technique selected need not be more sophisticated or detailed than is necessary to provide a comprehensive examination of the hazards associated with the facility operations. For example, a simple storage operation may be adequately evaluated by a preliminary hazard analysis or a structured What-IF analysis. There is no obligation for the analysts to perform a complete HAZOP.

To achieve the objectives of analysis of accidents, the graded approach ranges from a hazard analysis to a detailed quantitative analysis where formally quantified event trees

and/or fault trees form the bases for physical phenomena modeling and engineering analysis. The level of analytical effort employed is primarily a function of magnitude of hazard, but also takes into account system complexity, and the degree to which detailed modeling can be meaningfully supported by system definition. For nonreactor nuclear facilities, these considerations do not support a need for probabilistic/qualitative risk assessment of overall facility operations. This Standard does not present an expectation of or a requirement for probabilistic/qualitative risk assessment. Additionally, in accordance with DOE-STD-1027, the hazard analysis as described in Section 3.3, "Hazard Analysis," of this Standard is sufficient to meet the 10 CFR 830 requirements of accident analysis for Hazard Category 3 facilities. The hazard analysis should be adequate to provide a simple estimate of bounding consequences for Hazard Category 3 facilities.

It must be kept in mind that Hazard Category 3 facilities may also have chemical hazards. The hazard classification mechanism used in DOE-STD-1027 does not consider the potential hazardous chemical releases. The results of the hazard analysis will indicate whether a facility contains significant chemical hazard(s) that may necessitate accident analysis.

Accident analysis is also inherently graded in terms of the degree of physical modeling and engineering analysis needed to quantify accident consequences and likelihood. The use of bounding assumptions and less detailed physical modeling in accident analysis is appropriate. For example, where a given release has low consequences even if a filtered ventilation system is bypassed, detailed modeling of filtered release parameters such as filter differential pressure, plenum temperature, etc, is not needed for the given accident.

Formal, quantitative analysis of potential accident sequences as described in Section 3.4, "Accident Analysis," is not required to assess worker safety issues in addition to the hazard analysis. The largely qualitative hazard evaluation described in Section 3.3, which is a thorough analysis of potential accidents, is a more relevant vehicle for worker safety assurance.

Additional guidance on hazard and accident may be gained from the following references:

- *Guidelines for Hazard Evaluation Procedures*, American Institute of Chemical Engineers, 1992.
- "Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports" DOE-STD-1027.
- "Recommended Values and Technical Bases for Airborne Release Fractions (ARFs), Airborne Release Rates (ARRs), and Respirable Fractions (RFs) at DOE Non-Reactor Nuclear Facilities" DOE Handbook (HDBK)-3010.
- *Nuclear Fuel Cycle Facility Accident Analysts Handbook*, Nuclear Regulatory Commission NUREG-1320.
- "A Strategy for Occupational Exposure Assessment," American Industrial Hygienists Association, 1991.
- "Application of Hazard Evaluation Techniques to the Degree of Potentially Hazardous Industrial Chemical Processes," National Institute of Occupational

Safety and Health No. 88-79897, March 1992.

- 29 CFR 1910.119, "Process Safety Management of High Hazardous Chemicals."

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 3

3.1 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.

3.2 REQUIREMENTS

This section lists 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 for 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.

3.3 HAZARD ANALYSIS

This section describes the hazard identification and evaluation performed for the facility. The purpose of this information is to present a comprehensive evaluation of potential process related, natural events, and man-made external hazards that can affect the public, workers, and the environment due to single or multiple failures. Consideration will be given to all modes of operation, including startup, shutdown, and abnormal testing or maintenance configurations. As is standard industrial practice, examination of all modes of operation considers the potential for both equipment failure and human error.

Hazard identification and evaluation provide a thorough, predominantly qualitative evaluation of the spectrum of risks to the public, workers, and the environment due to accidents involving any of the hazards identified. The evaluation identifies preventive and mitigative features, including identification of expected operator response to incidents (e.g., accident mitigation actions or evacuation) and provisions for operator protection in the accident environment (see Table 3-1, Action item/Comment column).

A basic flowchart for hazard/accident analysis is provided in Figure 3-1. The major features of hazard analysis and the graded approach are captured in this figure. Hazard identification provides the basis for the final hazard categorization of the facility. That categorization is input for the graded approach for hazard evaluation. Hazard Category 3 facilities are not required to perform formal, quantitative accident analysis.

Figure 3-1 identifies the specific point where the analyst must move beyond the general outline of this Standard and use the graded approach to specifically determine appropriate hazard analysis methodology. Application of a graded approach is based on the judgment and experience of the analysts and results in the selection of a hazard evaluation technique such as Preliminary Hazard Analysis (PHA), HAZOP, etc. As previously noted, more elaborate techniques will generally be associated with more complex processes. Experience and capabilities of analysts are also a major consideration in efficient performance of a comprehensive hazard evaluation.

Systematic application of the chosen techniques to the operations in a facility generates a number of basic accidents based on types of events and system performance in response to the events. These accidents can be binned in accordance with predefined consequence and frequency ranking thresholds. Products of the hazard evaluation include:

- Identification of planned design and operational safety improvements.
- Summary of defense in depth including identification of safety-significant SSCs and other items needing TSR coverage, including relevant programs covered under TSR administrative controls.
- Summary of significant worker protection features including identification of safety-significant SSCs and relevant programs covered under TSR administrative controls.
- Summary of design and operational features that reduces the potential for large material releases to the environment.
- Selection of a limited set of bounding accidents (i.e., DBAs) to be further developed in Section 3.4, “Accident Analysis.”

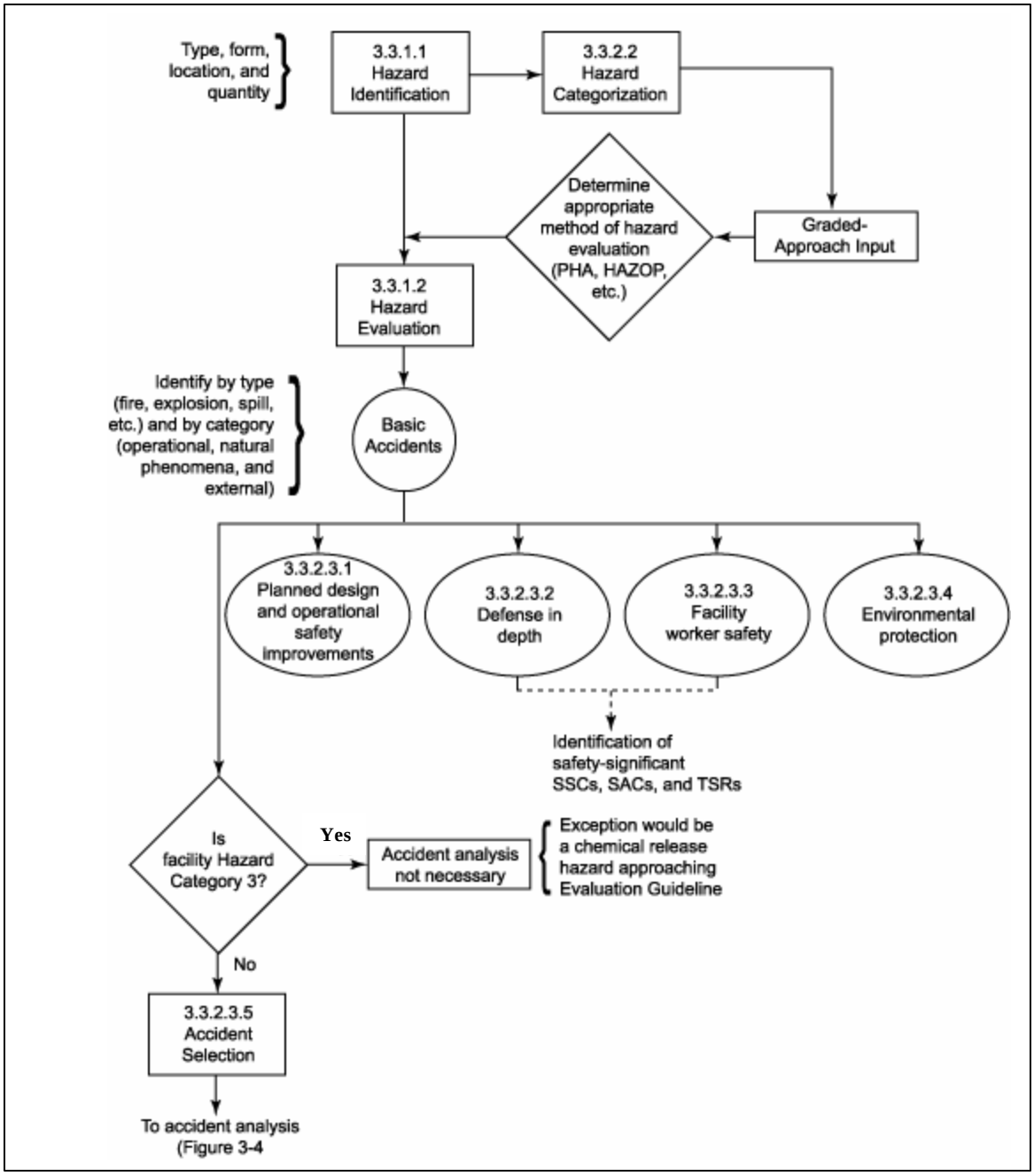


Figure 3-1. Flowchart for performing a hazard analysis.

3.3.1 Methodology

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

3.3.1.1 Hazard Identification

This subsection identifies the method used by analysts to identify and inventory 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 methodology first identifies sources of referenced information that are not an integral part of the DSA hazard identification. Possible sources of such information include fire hazard analyses, health and safety plans, job safety analyses, occurrence reporting histories, etc.

The DSA covers worker safety issues related to hazards in processes and associated activities. It is not the intention of the DSA to cover safety as it relates to the common industrial hazards that make up a large portion of basic OSHA regulatory compliance. It is important not to expend DSA resources on those hazards for which national consensus codes and/or standards (e.g., OSHA regulations) already define and regulate appropriate practices without the need for special analysis. As noted in this Standard's definition of "hazard," standard industrial hazards are identified only to the degree they are initiators and contributors to accidents in main processes and activities. For example, worker electrocution from electrical wiring faults is not a DSA issue. However, the existence of 440 volt AC cabling in a glovebox would be identified as a potential accident initiator for a scenario (i.e., fire) involving hazardous materials.

The distinction cited in the previous examples makes careful identification of hazards covered in the DSA essential so that potential worker hazards are not overlooked. As part of the identification process, the basis that was used in the hazard screening to remove standard industrial hazards or insignificant hazards from further consideration needs to be presented as well. For these cases, the DSA hazard analysis process interfaces with other programs such as specific topics of OSHA compliance or general industrial safety. These interfaces must be identified. Some of these compliance issues, while not presented in the DSA as such, may be a portion of a safety management program committed to by the facility. An example of this is the Health and Safety Plans required by OSHA in accordance with the Hazard Waste Operations and Emergency Response program. This could be one element of the "plans, procedures, and training for governing operations involving radioactive and hazardous waste" specified in Section 9.3, "Radioactive and Hazardous Waste Management Organization."

This subsection also indicates the sources from which information was obtained, such as flowsheet inventories, maximum historical inventories, vessel sizes, contamination analyses, etc. The interpretation of the data used to

derive conservative inventory values needs to be provided.

3.3.1.2 Hazard Evaluation

This subsection presents, in summary fashion, the basic approach and guidance used for generating the largely qualitative consequence and likelihood estimates in hazard evaluation. Reference detailed guidance as necessary. Additionally, present any screening logic used for binning accidents. The appropriateness of the overall methods used to evaluate hazards is presented and justified. This justification focuses on the selection of a technique for given processes, not justification from first principles of standard analysis methods, such as HAZOP.

3.3.2 Hazard Analysis Results

3.3.2.1 Hazard Identification

This subsection presents the results of the hazard identification activity, either by direct inclusion of or by reference to the hazard identification data sheets. As a minimum, provide a summary table identifying hazards by form, type, location, and total quantity. The attributes of hazards identified in this section are the basis for subsequent hazard evaluation and accident analysis. Include in the basic set of hazards identified 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 accident progression involving such materials.

To provide a perspective on facility hazards, summarize in this subsection the major accidents or hazardous situations (e.g., fires, explosions, loss of confinement) that have occurred in the facility's operating history. Specific details on each occurrence are not required. A general summary by type with emphasis on the major occurrences will suffice.

3.3.2.2 Hazard Categorization

This subsection presents the results of the final hazard categorization activity specified in DOE-STD-1027. Include the facility hazard categorization and, where segmentation has been employed, the segment boundaries and individual segment classifications. Justify any segmentation in terms of independence. Where facility segmentation is used, provide the hazard breakdown by segment in the summary table required in Section 3.3.2.1.

3.3.2.3 Hazard Evaluation

Hazard evaluation characterizes the identified hazards in the context of the actual facility and process. For example, simple hazard identification would be that 2000 grams of plutonium oxide are in a steel container under a hood waiting for entry into a glove box. One accident, which places this hazard in the actual context of facility parameters, involves spilling the container on the room floor. The hazard evaluation would qualitatively consider the action of moving the container into the glove box to evaluate the likelihood of spilling the contents. It would also consider mitigative features that would affect potential consequences. References such as *Guidelines for Hazard Evaluation Procedures* (1992) provide acceptable guidelines for selecting hazard evaluation techniques and generic lists of initiators that need to be incorporated in systematic evaluation with a given technique.

Public and worker safety issues are the traditional focus of hazard evaluations. The DSA hazard evaluation also examines the potential for large-scale environmental contamination. The information on environmental contamination may be used in a separate cost-benefit analysis, not related to the DSA effort, to determine if additional preventive or mitigative features are needed in the facility.

Tables 3-1 and 3-2 provide two examples of hazard analysis output. Table 3-1 is an example of a portion of the evaluation of a hydrogen fluoride unloading operation. It identifies accident initiators, associated preventive and mitigative functions, and operational safety enhancements determined to be necessary. The parenthetical numbers in the table under the headings of "Cause," "Consequence," and "Frequency" distinguish a numbering system that serves to identify specific accident scenarios (i.e., cause #1 is an event that has been judged to have consequence #1 and frequency #1, resulting in the overall ranking aligned with frequency #1). The ranking (i.e., low, medium, and high) of estimated consequences and frequencies are based on judgment of analysts, and the overall binning rank is in accordance with the numbers assigned to the example in Figure 3-2. Table 3-1 demonstrates how a number of basic accidents can be identified and evaluated in a concise manner. The last column of Table 3-1 presents safety enhancements in the form of two procedural verifications and two action items for procedural alteration that were identified in the course of the evaluation.

Table 3-1 also provides an example of how worker safety issues are integrated into this presentation. However, significant worker safety evaluations unrelated to the hazard scope defined for a DSA (i.e., standard industrial hazards) will be occurring outside the DSA. This reinforces the importance of the emphasis in Section 3.3.1.1, "Hazard Identification," of identifying the dividing line between process/activity hazards covered in the DSA and those covered by direct OSHA regulatory compliance. Specifying the location of this dividing line is essential to developing an integrated safety posture where the functions of DSA hazard analysis vis-à-vis health and safety plans, job task

analyses, etc., is understood.

Table 3-2, although not filled out, provides an example of another type of evaluation table. Whereas Table 3-1 is based more on a What-if or PHA-type approach, Table 3-2 is based on a failure modes and effects analysis (FMEA) approach. The basic outputs, however, remain unchanged. The second example is provided to indicate there is no one correct approach or presentation. The only constant is that effort needs to be expended only to the level necessary to basically characterize the accident spectrum.

Hazard evaluation presents potential accidents in terms of hazards, energy sources, causes, preventive and mitigative features, consequence estimates, and frequency estimates. Where a large number of scenarios are involved, present simple summaries in the text of this chapter with detailed tables generated in the performance of the hazard evaluation included as an appendix to the DSA.

Beyond the basic results, the individual subheadings (Sections 3.3.2.3.1 through 3.3.2.3.5) of Section 3.3.2.3, “Hazard Evaluation,” present organized summaries of specific topics of concern.

Table 3-1. Example process hazard analysis worksheet

Facility: Example Refinery Date: 04/07/90 Page 3 of 30
Area: HF Alkylation
Unit: Unloading HF from Supply Tanker

Hazard	Cause	Protection and mitigative systems	Consequence	Frequency	Ranking	Action item/ Comment
(1) Anhydrous HF, 5,000 gallons. (2) <100 psi potential energy from nitrogen blanket.	(1) Leak at connection point. (2) HF hose ruptures. (3) HF hose ruptures, flow not immediately shut off. (4) Truck relief valve fails open. (5) Truck relief valve opens; over-pressure conditions. (6) Tanker failure from over-pressure. (7) N_2 hose ruptures. (8) N_2 hose ruptures, check valve fails. (9) HF line not swept after unloading.	(A) Operators in chemical suits with respirators for emergency use. (B) Specific procedures, trained operators. (C) HF detectors. (D) HF line remote shutoff valve on truck. (E) Emergency relief valve capping kit available. (F) Two N_2 pressure regulators. (G) Check valve on N_2 gas line. Maximum N_2 pressure less than tanker design pressure. (H) Emergency water deluge system.	(1) Minor operator exposure – **LOW.** (2) Minor operator exposure off site <ERPG-2 – **LOW.** (3) Operator exposure, possibly ERPG-2 off site – **MEDIUM.** (4) Typically (a) **LOW** if capped. Possibly (b) **MEDIUM** if not capped and no deluge. (5) Typically (a) **LOW** if short duration. Possibly (b) **MEDIUM** if longer and no change. (6) Possible operator fatalities and ERPG-3 off site – **HIGH.** (7) N_2 leak – **LOW.** (8) See item #5 above. (9) Minor operator exposure – **LOW.**	(1) **HIGH** (2) **MEDIUM** (3) **LOW** (4) (a) **MEDIUM** (4) (b) **LOW** (5) (a) **LOW** (5) (b) **LOW** (6) **LOW** (7) **MEDIUM** (8) See #5 frequency (9) **HIGH**	4 2 3 2 3 1 3 6 2 See item #5 4	(1) Verify that procedures provide consistent leak-check on fitting. (2) Verify that procedures provide appropriately defined interaction between plant personnel and truck operators. (3) Area should be roped off and access controlled during unloading. (4) Specific evacuation routes for operators should be defined in procedures.

Table 3-2. Hazard analysis worksheet based on failure modes and effects analysis.

Location _____	Sheet _____of _____
Project _____	Ref. Drawing _____
Date _____	Process _____
	Plant Section _____

Item	Line or equipment designation	Failure or error mode	Effects on		How detected	How corrected	Frequency class	Consequence class	Action required
			Components/ people	System					

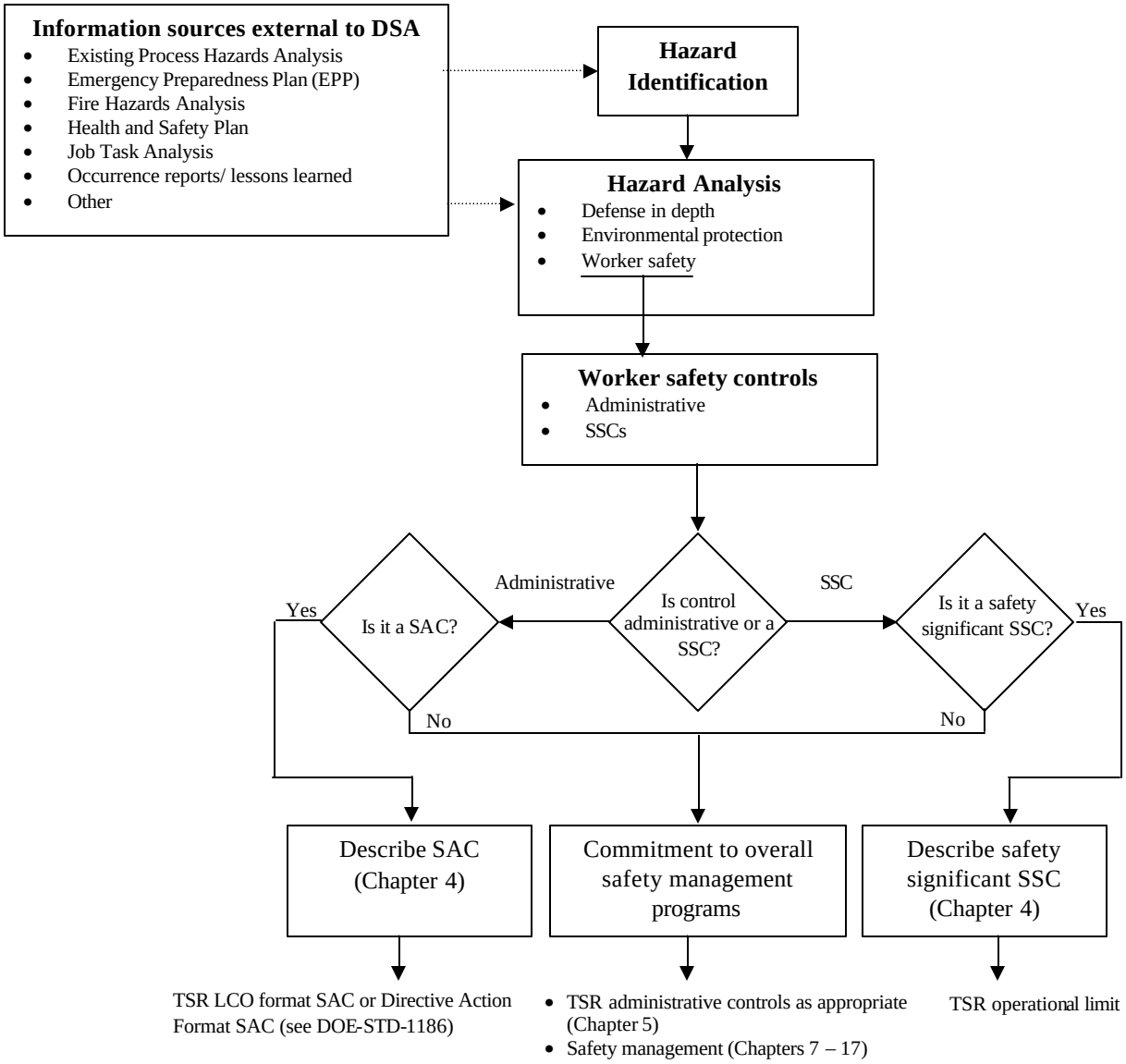


Figure 3-2. Worker safety evaluation.

3.3.2.3.1 Planned Design and Operational Safety Improvements

If the DSA preparer wants to make commitments to planned improvements not yet implemented (as a result of the hazard evaluation), this section will identify those major design and operational improvements. Summarize the basis for committing to the improvement and, if needed, any interim controls proposed until the improvement is implemented. Provide a general outline of the improvement intended to the degree it has been conceptually finalized. Due to capital costs, 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 prior to DSA submittal. DOE does not desire to unduly delay DSA completion for such items, and numerous safety precedents acknowledge accepting work in progress. Accordingly, the facility operator may choose to commit to implementation of an improvement that is not reflected in current design or facility operations.

3.3.2.3.2 Defense in Depth

This section summarizes significant aspects of defense in depth, and identifies associated safety-significant SSCs, SACs and other items needing TSR coverage. Include both the facility design and administrative features of defense in depth.

Facility design germane to defense in depth typically includes SSCs that function as:

- Barriers to contain uncontrolled hazardous material or energy release (e.g., metal dissolver vessel).
- Preventive systems to protect those barriers (e.g., hydrogen detection, air purge, and shutdown systems for metal dissolver).
- Systems to mitigate uncontrolled hazardous material or energy release upon barrier failure (e.g., ventilation zone confinement).

Administrative features are typically linked to the overall safety management programs that directly control operations. Administrative features include the following aspects of operator interfaces:

- Procedural restrictions or limits imposed.
- Manual monitoring of critical parameters.
- Equipment support functions.
- Responses or actions counted on to limit abnormal conditions, accident progression, or potential personnel exposure.

The individual features that comprise defense in depth are identified in "Hazard Evaluation," Section 3.3.2.3. Table 3-1 provides an example of how existing and proposed features (barriers to uncontrolled hazardous material or energy release) for specific operations are identified. The raw information in the hazard evaluation tables will be examined and distilled into an organized discussion of the elements of defense in depth. Relevant accidents may be used to frame and focus the discussion, but the hazard evaluation already provided in or appended to the DSA in tabular form should not be duplicated. Organize the presentation in a systematic manner (i.e., inner to outer) to clearly identify the layers of defense. Note that there is no requirement to demonstrate any generic, minimum number of layers of defense. The intent is to support the conclusion that defense in depth for a given hazard is commensurate with industrial practices for the relevant type of activity.

Identify the broad purpose and importance of defense-in-depth features, not the details of their design or implementation. For example, a glovebox represents an aspect of defense in depth. Only its major features and interactions with other elements of defense in depth, such as ventilation zone confinement, need to be summarized. It is not necessary to discuss the individual penetration fittings, welded piping junctions, gloveport designs, etc., which allow the glovebox to function as designed. Likewise, if there is a procedural requirement for the operator to perform an action if a parameter is exceeded, it is not necessary to identify the exact procedure, the exact phrasing of the requirement, the specific details of how the operator accomplishes that action, etc. Stating the action, providing a brief summary of its rationale, and noting that both procedures and training needed to cover that action are sufficient.

Safety-Significant SSCs

Distinguish safety-significant SSCs from among those structures, systems, and components contributing to defense in depth. To effectively use the graded-approach concept, focus on the most important items of defense in depth whose failure could result in the most adverse uncontrolled releases of hazardous material. This Standard maintains that all SSCs with a safety function do not require classification as equipment requiring detailed description in the DSA (i.e., safety-class SSCs and safety-significant SSCs). As noted in the Introduction, this is one of the principle reasons for the emphasis on programmatic commitments.

The major features of defense in depth typically comprise the outer or predominant means of mitigating uncontrolled release of hazardous materials [e.g., ventilation system directing airflow to High Efficiency Particulate Air (HEPA) filters, overall building structure], any preventive features that are designed to preclude highly energetic events that potentially threaten multiple layers of defense in depth or essentially defeat any one layer (e.g., a hydrogen detector and purge flow interlock on a vessel that prevents a large hydrogen explosion, a sprinkler system that prevents a large fire that is physically possible for a type of operation), or any SSCs needed to insure the availability

of such preventive or mitigative functions (e.g., electrical power sources for ventilation).

The total layers of defense in depth available are also key considerations in designating safety-significant SSCs. If many effective barriers are available, the significance of any one barrier is limited. If only one or two barriers can be realistically counted on, their individual significance increases. Likewise, if total hazardous material inventory is distributed over a hundred containers (e.g., waste drum storage pad, plutonium storage vault), the failure of any one container does not necessarily constitute a major uncontrolled hazardous material release, depending on the nature of the material and the design adequacy of the container. If all material is held in one container (e.g., 3000 gallon hydrogen fluoride storage tank), the failure of that container is of major concern in controlling the release of hazardous material. In the case where quantities of hazardous materials are being stored so that breached nuclear material storage packages might result from facility accident conditions, the containers themselves may need to be upgraded or another facility level method (secondary containment or confinement) considered for defense-in-depth.

A principle reason for designating such major features as safety-significant SSCs is that they typically represent facility specific systems as opposed to more generic systems. While all glovebox line facilities use zone systems of ventilation for confinement, there is an enormous variation in the DOE complex with regard to specific design parameters such as number and types of exhaust systems, means of flow control, etc. Accordingly, more detailed descriptions of such equipment in a DSA is considered both appropriate and necessary for Hazard Category 2 facilities. Such description would not provide the same utility for relatively generic confinement items such as 55-gallon waste drums. The need for designation as a safety-significant SSC would also be superseded if that SSC was designated as a safety-class SSC in accident analysis.

TSRs

Summarize those safety-significant SSCs, SACs and other aspects of defense in depth that require TSR coverage. The scope of the TSR coverage is determined by the degree to which barriers or the facility-safety basis are seriously challenged.

Vital, passive components such as piping, vessels, supports, structures, and containers would typically be considered design features. These components are discussed in the Design Features Section of the TSR document. For example, a glovebox is an obvious barrier to uncontrolled material release. The windows, gloves, and cable/piping connectors are all necessary to maintain the barrier, but do not specifically require operational limits or administrative controls as contributors to defense in depth.

DOE G 423.1-1 provides basic screening criteria to identify defense-in-depth

features/items that may require specific TSR coverage. Such features include instrumentation designed to detect significant barrier degradation; equipment that actuates or controls so as to reduce the likelihood of significant barrier challenges; process variables controlled for that purpose; and active controls that prevent criticality. Every control or indicator does not require specific TSR coverage. Likewise, every design feature malfunction or abnormal condition does not constitute a major barrier or facility safety basis degradation/challenge.

Significant challenges to the facility safety basis are typically those events which have a genuine potential to seriously damage safety SSCs, require actuation of safety SSCs not on line as part of normal operations, or approach conditions TSR controls are designed to prevent. Significant barrier degradation is generally considered to mean substantial loss of barrier function resulting in significant hazardous material release to areas of personnel occupancy, or the occurrence of highly energetic events with the potential to damage multiple barriers. To further explore barrier degradation, consider a glovebox containing a dissolver vessel. A leak from the dissolver would not be a major degradation of overall confinement because:

- It is a slow, low energy phenomenon where the primary vessel itself remains intact.
- The release is into another layer of confinement not occupied by personnel.

Process upsets resulting in an eructation from the vessel would not be major degradation either. Even small, vapor space deflagrations that rupture vessel blowout ports would not be a major degradation if the glovebox itself would not sustain significant damage.

In contrast, consider a large hydrogen deflagration or detonation that ruptures the vessel and piping, drives debris through the glovebox structural elements, and momentarily pressurizes the glovebox. This is a highly energetic event and multiple barriers have been damaged allowing a potentially significant release of hazardous material directly to occupied areas. Possible TSR coverage could include the maximum hydrogen concentration limits or requiring an air purge system to be functioning when the dissolver is operating.

TSRs may also be provided for safety management programs in the form of TSR administrative controls to support adequate defense in depth. Such all-encompassing TSRs should be used in lieu of individual TSRs for numerous specific aspects of programs unless the control is significant to specific accident risk reduction. These administrative controls, designated as SACs, are addressed in the TSRs as limiting conditions for operation with surveillance requirements, or as specific directive action AC in the Administrative Controls section of the TSR. DOE Standard 1186 provides additional guidance for implementing SACs in TSRs.

3.3.2.3.3 Worker Safety

This section summarizes the major features protecting workers from the hazards of facility operation, exclusive of standard industrial hazards. Summary products germane to worker safety typically include:

- General overview of worker safety in terms of SSCs and administrative features.
- Identification of any safety-significant SSCs and SACs.
- Identification of any safety management programs that will be assigned TSR coverage in the form of administrative controls for adequate worker safety.

General prioritization of the features needs to be included and expressed in terms of the magnitude of process hazard, number of potentially affected employees, pertinent aspects of operation history, and projected lifetime of the process. Only a summary level discussion is required, not a detailed discussion or defense of the prioritization logic. The safety features to be addressed in this section fall into one of three categories:

- Structures, systems, and components.
- Specific administrative controls.
- Administrative features..

This subsection is derived from examining the raw information in the hazard evaluation tables (see Table 3-1 for example) and distilling it into a clear overview of worker safety features at the facility. This presentation may use relevant accidents to frame and focus the discussion, but need not duplicate the hazard evaluation already provided in or appended to the DSA in tabular form. If the basic function of a worker safety feature has already been discussed in Section 3.3.2.3.2, "Defense in Depth," that feature may simply be identified by name and referenced.

Identify structures, systems, and components as safety-significant SSCs where appropriate. As a general rule of thumb, safety-significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in a prompt worker fatality or serious injuries to workers or significant radiological or chemical exposures to workers (see definition of safety-significant SSCs for further clarification). Inadvertent worker exposure to materials from breached nuclear storage packages during inspections or handling may fit this description.

Identify specific administrative controls important to safety that are needed to prevent or mitigate an accident scenario as appropriate. In general, SAC designations based on worker safety are limited to those administrative controls that would have been safety-significant had that safety function been provided by a safety-significant SSC. The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related

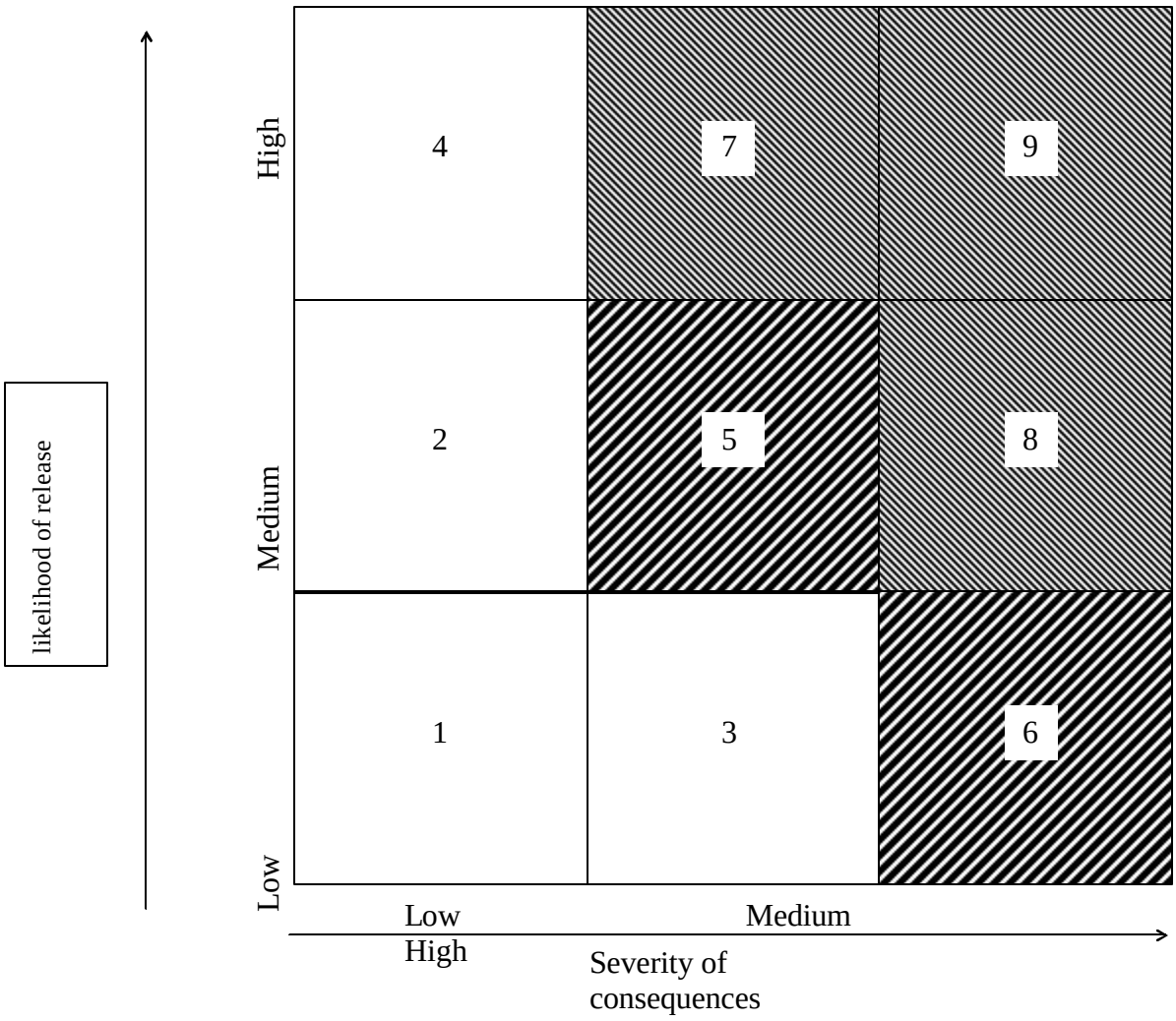
SSCs be preferable to ACs or SACs due to the inherent uncertainty of human performance.

Categorize administrative features in terms of the programmatic elements covered in later chapters of the DSA. With the exception of safety-significant SSCs, TSR designation is made in the form of administrative controls for overall programs only for worker safety. Typical safety-management programs include criticality protection, radiation protection, hazardous material protection, institutional safety provisions, procedures and training, operational safety, and emergency preparedness. Specifically note programs that will be provided TSR coverage as administrative controls in Chapter 5, "Derivation of Technical Safety Requirements."

Figure 3-3 shows how worker safety is addressed in the hazard analysis process. This subsection provides documented evidence that worker safety features are an integral part of facility design and operation, that basic facility operations for worker safety are adequate, and that workers are protected by a number of means including programs described elsewhere in the DSA (e.g., Chapters 7 and 8). It is emphasized again that this subsection is written at a summary level. Identify the broad purpose of features, but not the details of their design.

3.3.2.3.4 Environmental Protection

This subsection summarizes the design and operational features that reduce the potential for large material releases to the environment. Document pathways for uncontrolled release of large amounts of hazardous materials to the environment identified in the hazard evaluation. Estimate potential consequences and preventive and mitigative features associated with specific pathways. If specific pathways have previously been addressed (e.g., Section 3.3.2.3.2, "Defense in Depth"), a reference is sufficient.



(Taken from EPA Technical Guidance for Hazards Analysis)

Figure 3-3. A three-by-three likelihood and consequence ranking matrix for hazard evaluation.

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

This subsection is not intended to present detailed, cost-benefit conclusions about the adequacy of design related to potential environmental contamination. It may serve as input to separate cost-benefit analysis to determine if additional preventive or mitigative features are to be added to the facility. However, such analyses are not related to the DSA effort.

The numerical Evaluation Guideline and legal limits on normal operations [i.e., Environmental Protection Agency (EPA) regulations] inherently place an upper bound on potential environmental releases. Further, issues of environmental contamination are not direct safety issues. Safety SSC designations are not required for issues solely related to environmental protection. In accordance with 10 CFR 830, TSR designations are not required for such issues either. TSR designation associated with prevention of uncontrolled release of hazardous materials would typically be assigned for defense-in-depth considerations.

3.3.2.3.5 Accident Selection

Accident analysis entails the formal quantification of a limited subset of accidents (i.e., DBAs). These accidents represent a complete set of bounding conditions. The identification of DBAs results from the hazard evaluation ranking of the complete spectrum of facility accidents.

Figure 3-2 and Tables 3-3 through 3-5 provide examples of hazard evaluation ranking mechanisms. Two examples are provided to indicate there is more than one correct approach. The approach used at any specific facility is based on the detail needed for a given facility and the experience of the analysts. Figure 3-2 is a graphical example of a common three-by-three frequency and consequence ranking matrix. This particular example was used for evaluating airborne hazardous

Table 3-3. Qualitative severity classification table.

Descriptive Word	Description
No	Negligible on-site and off-site impact on people or the environs.
Low	Minor on-site and negligible off-site impact on people or the environs.
Moderate	Considerable on-site impact on people or the environs; only minor off-site impact.
High	Considerable on-site and off-site impacts on people or the environs.

Table 3-4. Qualitative likelihood classification table.

Descriptive word	Estimated annual likelihood of occurrence	Description
Anticipated	$10^{-1}>p>10^{-2}$	Incidents that may occur several times during the lifetime of the facility. (Incidents that commonly occur)
Unlikely	$10^{-2}>p>10^{-4}$	Accidents 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	$10^{-4}>p>10^{-6}$	Accidents that will probably not occur during the life cycle of the facility. This class includes the design basis accidents.
Beyond Extremely Unlikely	$10^{-6}>p$	All other accidents.

Table 3-5. Qualitative ranking.

Description	Risk evaluation
No impact or beyond extremely unlikely. Low severity and extremely unlikely. Moderate severity and extremely unlikely or low severity and unlikely.	Acceptable
High severity and extremely unlikely or low severity and anticipated. Moderate severity and Unlikely.	Marginal
Moderate severity and anticipated or high severity and unlikely. High severity and anticipated.	Unacceptable

material releases. The logic behind Figure 3-2 is elaborated on in Tables 3-3 through 3-5, which provide a description of a four-by-four frequency and consequence-ranking matrix. Although differing in presentation and structural details, the philosophical basis and objectives for both examples are identical. The ranking schemes are designed to separate the lower risk accidents that are adequately assessed by hazard evaluation from higher risk accidents that may warrant additional quantitative analysis if the phenomena involved are not simplistic. A limited number of moderate risk accidents between the two extremes may also be identified for assessment. Tables 3-3 through 3-5 provide typical descriptions of consequence and likelihood thresholds for binning. Ranking should use broad bins. For example, frequency bins should typically cover two orders of magnitude.

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 nonindependent events, 0.1 to human errors, and 0.01 to genuinely independent failures. Another methodology would be to use a summary of historical data. Likewise, before beginning the evaluation, a conservative Gaussian plume estimation of the amount of material needed outside the building to cause a certain dose might be performed to aid in defining thresholds of significance. Briefly discuss or reference any such guidelines in Section 3.3.1.2, “Hazard Evaluation.” Note, however, that the ranking of

frequency and consequence into such broad categories is more of a qualitative than a quantitative exercise. This effort does not constitute the need for, or expectation of, a probabilistic / quantitative risk assessment.

An important factor in estimating binning thresholds for public consequences is to tie the thresholds to the Evaluation Guideline so that accidents that could challenge the guideline are correctly identified for formal accident analysis. The binning requirement of this subsection does not preclude the use of other sorting mechanisms in addition to risk sorting if an analyst finds such mechanisms useful.

This accident selection activity identifies the process and criteria used to select the unique and representative potential accidents (i.e., DBAs) to be included in accident analysis. Unique accidents are those with sufficiently high-risk estimates that individual examination is needed (e.g., a single fire whose specific parameters result in approaching the Evaluation Guideline, situations of major concern from Figure 3-2). Representative accidents bound a number of similar accidents of lesser risk (e.g., the worst fire for a number of similar fires, situations of concern in Figure 3-2). Representative accidents are examined to the extent they are not bounded by unique accidents. In any case, at least one bounding accident from each of the major types determined from the hazard analysis (e.g., fire, explosion, spill, etc.) should be selected unless the bounding consequences are "Low" (See Figure 3-2). Accidents are identified and listed by accident category (i.e., internally and externally initiated) and type (e.g., fire, explosion, spill, etc.).

Since the hazard analysis activity is considered sufficient for Hazard Category 3 facilities, DSAs for these facilities need simply summarize the maximum consequences expected from facility operation and state that detailed accident quantification is not necessary because potential consequences are well below the Evaluation Guideline. A possible exception to this case, as previously noted, is a facility with Hazard Category 3 quantities of radionuclides but possessing large amounts of toxic chemicals. Such facilities need to summarize the maximum radiological consequences expected and identify the chemical accidents selected for accident analysis.

3.4 ACCIDENT ANALYSIS

This section presents the formal development of the potential accidents identified in Section 3.3.2.3.5, "Accident Selection," beginning with a formal sequence of developing connecting initiating events to preventive feature and mitigative feature responses. A basic flowsheet for accident analysis is presented in Figure 3-4. The principal purpose of the accident analysis is to identify any safety-class SSCs, SACs and TSRs needed for protection of the public.

Each accident sequence needs to be analyzed through the use of a documented, deterministic, DBA. Whenever possible, DBAs are analyzed using the simplest applicable deterministic, phenomenological calculations (e.g. pressure estimates from a simple ideal gas law calculation, hand calculated Gaussian plume

dispersions). The nondeterministic aspects of DBA analysis are simplified by estimating overall sequence frequencies in broad frequency ranges in hazard analysis. This process is considered sufficient for DSA purposes and accident analysis need only document the basis for the binning performed in hazard analysis. Detailed probabilistic calculations are neither expected nor required. Natural events and man-made external events are special cases. Natural event DBAs are those events with a phenomenon initiating frequency as specified in DOE 420.1 and its applicable standards. External events are not typically design bases for facilities. However, they will be referred to as DBAs and analyzed as such if frequency of occurrence is estimated to exceed 10^{-6}/yr conservatively calculated, or 10^{-7}/yr realistically calculated.

Accident analysis typically starts with formal descriptions of accident scenarios. Basic event trees may support such descriptions. All major assumptions in scenarios must be identified. The next step is determination of accident source terms. Source terms for accidents are obtained through phenomenological and system response calculations. Once a source term has been determined, consequences due to atmospheric dispersion or other relevant pathways of concern are determined. As with every phase of the analysis, the effort expended is a function of the estimated consequence. If the source term is small, a simple, dispersion hand calculation for consequences would be sufficient. If source terms are large, computer modeling to determine consequences may be required. The consequences finally determined are compared to the Evaluation Guideline (see Appendix A). From this activity, it is determined if safety-class SSC designation is needed. The need for accident specific TSRs to meet the Evaluation Guideline will also be determined. Detailed description of safety-class SSCs, SACs and TSRs are presented in Chapter 4, "Safety Structures, Systems, and Components," and Chapter 5, "Derivation of Technical Safety Requirements." The nature of the accidents to be analyzed will vary depending upon the facility and processes considered. However, it is anticipated that for most facilities or processes, the number of accidents requiring formal analysis will not be large. The categories of DBAs examined are:

- Operational accidents (caused by initiators internal to the facility).
- Natural events (e.g., earthquakes, tornadoes).
- Man-made external events (caused by man-made initiators external to the facility).

All assumptions made in the accident analysis (i.e., defining points in scenario progression) are to be validated as part of the accident analysis activity.

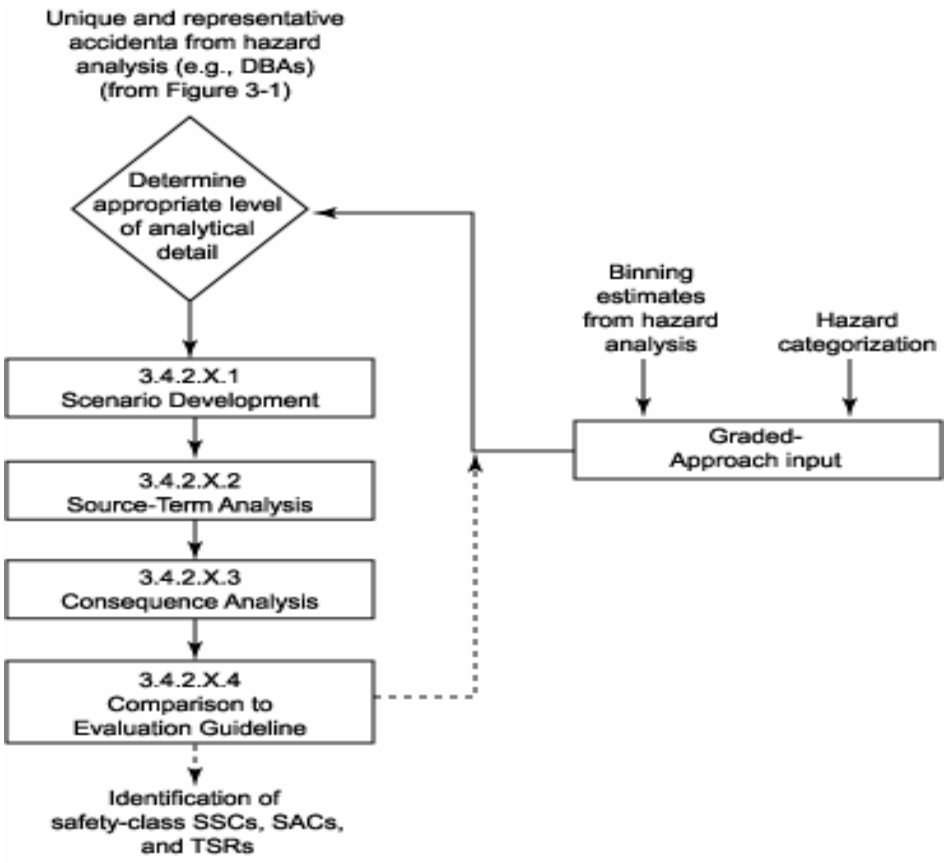


Figure 3-4. Flowchart for performing and accident analysis.

For example, if an operator is supposed to push Button Z to stop an accident progression, the accident analysis needs to make it clear that the operator can actually do so. Making it clear may simply involve noting there is no physical phenomena associated with the accident that would preclude him from doing so. Likewise, basic assurance must be provided that equipment relied upon in unusual or severe environments will function. This assurance does not constitute the need for or expectation of full, formal environmental qualification.

The above guidance is not meant to imply that the DSA must contain detailed validations for all assumptions. The DSA needs to present information at a level that is considered sufficient for review and approval of the DSA. Referencing an auditable trail of information as part of the controlled supporting documentation is acceptable.

3.4.1 Methodology

This section summarizes the methods used to quantify the consequences of operational accidents, natural external events, and man-made external events selected in Section 3.3.2.3.5, "Accident Selection." Identify and describe any computer programs used to implement methods discussed below. Include in the description the origin of the code, its precedent for use, input data, the range of variables investigated, the basic analytical models, their interrelationships, and the progression of the analysis. Briefly summarize and reference detailed information on algorithms, computational and analytical bases, and software quality assurance measures.

Documentation of methodology should include the following:

- Methods used to estimate radiological or other hazardous material source terms for DBAs including: (1) basic approach for estimating physical facility damage from DBAs; (2) general basis for assigning material-at-risk quantities not directly derived from hazard identification, if differing values are used; and (3) basis for material release and respirable fractions or release rates used.
- Methods used to estimate dose and exposure profiles including assumptions on variables such 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 Design Basis Accidents

This section analyzes DBAs for each of the major categories to quantify consequences and compare them to the Evaluation Guideline. The major categories are: internally initiated operational accidents (e.g., fires, explosions, spills, criticality); natural events for the site (e.g., earthquakes, tornadoes) that could affect the facility; and man-made externally initiated events such as airplane crashes, transportation accidents, adjacent facility events, etc., that can either cause releases at the facility under examination or have a major impact on facility operations. Beyond DBAs are discussed in Section 3.4.3, "Beyond Design Basis Accidents."

Quantification methods are typically limited to calculating the dose profile of a release. The process is iterative, starting by taking no credit for mitigative features and comparing results to the Evaluation Guideline. Continue taking credit for additional mitigative features incrementally and comparing the results to the Evaluation Guideline until below the guideline. This iterative process, however, does not require denying the physical design of facility structures, systems, and components. 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. Simply admitting they exist does not require safety-class SSC designation either. Stated another

way, facilities should be analyzed as they exist when quantifying meaningful release mechanisms.

Note: The following format is repeated sequentially for each ("X") DBA.

3.4.2.X [Applicable DBA]

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

3.4.2.X.1 Scenario Development

This subsection describes accident progression linking initiating events with preventive and mitigative events and other contributing phenomena to formally define the accidents identified in Section 3.3.2.3.5, "Accident Selection." Note each response, action, or indication required to initiate action that is relevant to the scenario progression. Document the rationale used in hazard analysis for binning the DBA in a broad frequency range.

When summarizing the initiating event for a given natural event DBA, use DOE 420.1 and its applicable standards (i.e., DOE-STD-1020 through -1024) to determine the natural event DBAs for the facility. Design basis guidelines include, among others, load factors, return periods, amplification factors for the facility, etc. Summarize facility and equipment response (emphasizing preventive or mitigative equipment) to the loads postulated to be present at the time the given natural event occurs. Reference the facility documentation of this evaluation and summarize relevant assumptions. Discuss the degree of conservatism of the evaluation.

Evaluate secondary events directly caused by natural events, such as earthquake induced fires, based on their physical possibility for facility conditions (i.e., the induced accident must already potentially exist in the absence of the seismic event). For example, seismic induced fires should be considered DBAs where significant accumulations of flammable material are exposed to fire initiators by seismic damage to the facility. If minimal combustible material is present in a given location, a large seismic induced fire in that location would not be a DBA as the potential is not physically possible.

Although external events are not typically design bases, this Standard considers them as DBAs if the frequency of occurrence is estimated to exceed 10-6/yr conservatively calculated, or 10-7/yr realistically calculated. The specific use of this NRC frequency precedent is limited to external events only due to their unique nature. External events are presented because frequency criteria for inclusion are met. Accordingly, the analysis that substantiates frequency need only be referenced.

3.4.2.X.2 Source Term Analysis

This subsection determines the accidental material or energy released through the pathways of concern. Define all parameters and phenomenological models used to derive the source term. As a minimum, this definition includes the material at risk (as derived from the hazard identification), the release fraction or rate that determines the initial source term, and the overall facility leakpath factors that determine the final source term released external to the facility. The degree of conservatism believed to be present in the calculation needs to be consistent with the Evaluation Guideline definition. Detailed quantification of uncertainty is not required.

3.4.2.X.3 Consequence Analysis

This subsection determines the receptor doses associated with the relevant pathways. Derive the doses in accordance with the definition of the Evaluation Guideline.

The information derived from the hazard and accident analyses related to protection of the public and potential insights gained for environmental contamination issues needs to be compared to the facility National Environmental Policy Act (NEPA) documentation to ensure that no significant discrepancies exist between the DSA and that documentation.

3.4.2.X.4 Comparison to the Evaluation Guideline

This subsection compares the unmitigated receptor dose for the accident sequence to the Evaluation Guideline. If the Evaluation Guideline is exceeded, provide a summary assessment of the significance of the exceedance and administrative and/or engineered controls whose implementation would prevent or mitigate the accident sequence. Detailed cost-benefit analyses to evaluate potential changes are beyond the scope of the DSA.

3.4.2.X.5 Summary of Safety-Class SSCs, SACs and TSR Controls

This subsection identifies the safety-class SSCs (or equivalent SAC) and assumptions judged to require TSR coverage. Any TSR assumption not directly related to exceeding of the Evaluation Guideline should be defined in section 3.3.2.3.2, “Defense in Depth.” For details, refer to Chapter 4, “Safety Structures, Systems, and Components,” and Chapter 5, “Derivation of Technical Safety Requirements.”

3.4.3 Beyond Design Basis Accidents

The Rule requires consideration of the need for analysis of accidents which may be beyond the design basis of the facility to provide a perspective of the residual risk associated with the operation of the facility The beyond DBAs serve as bases for cost-benefit considerations if consequences exceeding the Evaluation Guideline are identified in the beyond DBA range. However, such cost-benefit analysis would be performed outside the DSA with the concurrence of DOE.

It is expected that beyond DBAs will not be analyzed to the same level of detail as DBAs. The requirement is that an evaluation be performed that simply provides insight into the magnitude of consequences of beyond DBAs (i.e., provide perspective on potential facility vulnerabilities). This insight from beyond DBA analysis has the potential for identifying additional facility features that could prevent or reduce severe beyond DBA consequences. For nonreactor nuclear facilities, however, the sharp increase in consequences from DBA to beyond DBA is not anticipated to approach that found in commercial reactors where the beyond DBA precedent was generated. No lower limit of frequency for examination is provided for beyond DBAs whose definition is frequency dependent. It is understood that as frequencies become very low, little or no meaningful insight is attained.

Operational beyond DBAs are simply those operational accidents with more severe conditions or equipment failures than are estimated for the corresponding DBA. For example, if a deterministic DBA assumed releases were filtered because accident phenomenology did not damage filters, the same accident with loss of filtration is a beyond DBA. The same concept holds true for natural events, but beyond DBAs are defined by the initiating frequency of the natural event itself (i.e., frequency of occurrence less than DBA frequency of occurrence). Beyond DBAs are not evaluated for man-made external events.

Chapter 4
Safety Structures, Systems, and Components

PURPOSE. The purpose of this DSA chapter is to provide information necessary to support the safety basis requirements of 10 CFR 830 for derivation of hazard controls.

This chapter provides details on those facility structures, systems, and components that are necessary for the facility to protect the public, provide defense in depth, or contribute to worker safety. Similarly, this chapter provides details on specific administrative controls that are significant to specific accident risk reduction. Descriptions are provided of 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. Expected products of this chapter, as applicable based on the graded approach, include:

- Descriptions of safety SSCs and SACs including safety functions.
- Identification of support systems safety SSCs depend upon to carry out safety functions.
- Identification of the functional requirements necessary for the safety SSCs and SACs to perform their safety functions, and the general conditions caused by postulated accidents under which the safety SSCs or SACs must operate.
- Identification of the performance criteria necessary to provide reasonable assurance that the functional requirements will be met.
- Identification of assumptions needing TSR coverage.

Existing supporting documentation is to 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. Include a brief summary for each such reference that explains its relevance to this chapter and provides an introductory understanding of the reference.

APPLICATION OF THE GRADED APPROACH. Hazard Category 3 facilities will not have safety-class SSCs and the number of safety-significant SSCs and SACs if any, will be less than that of a Hazard Category 2 facility due to the reduced magnitude of hazards. As noted in Chapter 3, "Hazard and Accident Analyses," a possible exception to this general guidance pertains to chemical hazards. The hazard classification mechanism used in DOE-STD-1027-92 does not consider potential hazardous chemical releases. It is possible that a Hazard Category 3 facility could need safety-class items for large chemical hazards, although it is not typically expected.

Hazard Category 2 facilities have the potential for an accident resulting in significant onsite consequences and may have offsite consequences. These facilities

characteristically have safety-significant SSCs. They may need safety-class SSCs as well, although this is not typically expected.

Hazard Category 2 and 3 facilities do not have the consequence potential associated with Hazard Category 1 facilities, such as Class A reactors. Consequently, in keeping with the use of a graded approach, the means of safety assurance expected of Class A reactors, such as formal design reconstitution and full, formal environmental qualification, are generally unsuitable for Hazard Category 2 and 3 facilities. DSA preparers (and subsequent reviewers) should not expect this level of information to be attained, especially for SSCs for which the original design is not documented.

Precedent for dealing with facilities where the original technical information is undocumented and must be estimated has been provided by OSHA in the PSM rulemaking where it was stated "OSHA believed that a properly conducted process hazard analysis should systematically identify technical information regarding the process and allow adequate estimation of safe parameters for the process." The actual requirement imposed by OSHA was "where the original technical information no longer exists, such information may be developed in conjunction with the process hazard analysis in sufficient detail to support the analysis."

The DSA specifically requires determination of safety functions and functional requirements for safety SSCs and designation of performance criteria. However, a DSA prepared in accordance with this Standard is focused on identifying functional requirements that, in general, are neither absolute nor subject to fine safety margin resolution. Further, associated performance criteria are only defined for critical operational aspects of SSCs, not general design. As noted in the preceding paragraph, if the design information no longer exists, new information may be developed as part of the process hazard analysis. However, pertinent existing safety analyses and design information (requirements and their bases) that is immediately available or can be retrieved through reasonable efforts should be used. For additional technical information that is critical to the DSA development and is not retrievable through such efforts, new information may be developed as part of the hazard analyses and accident analyses. Documented engineering judgments (including their bases) and testing can be used to extrapolate the available existing information and hence establish the performance capabilities of the existing SSCs. In general, safety-class SSCs require more formality in establishing functional requirements and performance criteria than safety-significant SSCs due to their public protection function.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 4

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 lists 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 for 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.

4.3 SAFETY-CLASS SYSTEMS, STRUCTURES, AND COMPONENTS

Relevant information is provided, in the following SSC specific subsections, for safety-class SSCs with descriptions sufficiently detailed to provide an understanding of the safety function of safety-class SSCs. Descriptions for each safety-class SSC must be complete enough to indicate suitability of safety analysis inputs and assumptions. Provide a summary list of safety-class SSCs. This summary list should identify, in tabular form, safety-class SSCs, the accidents from Chapter 3 for which safety-class 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") safety-class SSC. The examples provided are for illustration purposes only, and should not be construed as a requirement to designate such systems safety-class or safety significant.

4.3.X [Applicable Safety-class System, Structure, or Component]

Identify the safety-class SSC.

4.3.X.1 Safety Function

This subsection states the reason for designating the SSC as a safety-class 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 shutdown the dissolving operation before explosive concentrations of hydrogen are reached." The specific accidents associated with the safety function should be identified.

4.3.X.2 System Description

This subsection provides a description of the safety-class SSC and the basic principles by which it performs its safety function (e.g., sensor and interlock for hydrogen detector discussed in section 4.3.X.1). Describe its boundaries and interface points with other SSCs relevant to the safety function.

Identify SSCs whose failure would result in a safety-class SSC losing the ability to perform its required safety function. These SSCs would also be considered safety-class SSCs for the specific accident conditions for which the safety-class designation was made originally.

When describing the SSC, provide a basic summation of the physical information known about the SSC, including Process and Instrumentation Drawings (P&IDs), or a simplified system drawing with reference to P&IDs. If known, abstract and reference pertinent aspects of manufacturer's specifications. 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) as opposed to general industrial equipment specifications that fall out 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 subsection identifies requirements that are specifically needed to fulfill safety functions. Such functional requirements are specified for both the safety class SSC and any needed support safety-class SSCs.

Limit functional requirement designation to those requirements necessary for the safety function. Functional requirements are provided for safety-class SSCs for the specific accident(s) where the safety-class SSC must function (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 being relied upon. In the hydrogen detector example, one obvious parameter would be maintaining 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

This subsection provides performance criteria imposed on the safety-class 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.

Engineering judgment may be used to develop performance criteria for existing safety SSCs (i.e., already designed) where documentation of design and operational responses may not exist. In determining performance criteria for safety-class SSCs, existing criteria traditionally associated with safety-class designation, such as single failure criteria, should be considered in the judgment process. However, for existing SSCs, formal design comparison and compliance with traditional safety-class performance criteria is not required.

Evaluate the capabilities of the SSC to meet performance criteria. The evaluation should be as simple as possible, and rely on engineering judgment, calculations, or performance tests as opposed to formal design reconstitution. For example, the hydrogen detector could be fed a test gas composition that would exceed its interlock trip point. Such a pass-fail test would typically bound the needed equipment performance as response time is not a highly sensitive parameter.

4.3.X.5 Controls (TSRs)

This subsection identifies those assumptions requiring TSRs to ensure performance of the safety function.

4.4 SAFETY-SIGNIFICANT STRUCTURES, SYSTEMS, AND COMPONENTS

Relevant information is provided, in the following SSC specific subsections, with descriptions sufficiently detailed to provide an understanding of the safety function of safety-significant SSCs. Descriptions for each safety-significant SSC must be complete enough to allow for verification of the accuracy of the safety analysis inputs and assumptions.

Provide a summary list of safety-significant SSCs. This summary list should identify, in tabular form, safety-significant SSCs, the rationale from Chapter 3 for which safety-significant 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") safety significant SSC. The examples provided are for illustration purposes only, and should not be construed as a requirement to designate such systems safety-class or safety-significant.

4.4.X [Applicable Safety-significant System, Structure, or Component]

Identify the safety-significant SSC.

4.4.X.1 Safety Function

This subsection states the reason for designating the SSC as a safety-significant 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 shutdown 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. Safety-significant SSCs are designated for overall purposes such as defense-in-depth, for which even normal operation considerations are involved. There may, or may not be, a single accident that, by itself, completely defines the safety function.

4.4.X.2 System Description

This subsection provides a description of the safety-significant SSC and the basic principles by which it performs its safety function (e.g., sensor and interlock for hydrogen detector discussed in section 4.3.X.1). Describe its boundaries and interface points with other SSCs relevant to the safety function.

Identify SSCs whose failure would result in a safety-significant SSC losing the ability to perform its required safety function. These SSCs would also be considered safety-significant SSCs for the specific accident conditions or general rationale for which the safety-significant designation was made originally.

When describing the SSC, provide a basic summation of the physical information known about the SSC, including simplified system drawings. If known, summarize pertinent aspects of manufacturer's specifications. 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) as opposed to general industrial equipment specifications that fall out 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 subsection identifies requirements that are specifically needed to fulfill safety functions. Such functional requirements are specified for both the safetysignificant SSC and any needed support safety-significant SSCs.

Limit functional requirement designation to those requirements necessary for the safety function. Functional requirements are provided for safety-significant SSCs for the specific accident(s) or general rationales for which the 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 being relied upon. In the hydrogen detector example, one obvious parameter would be maintaining 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.

4.4.X.4 System Evaluation

This subsection provides performance criteria imposed on the safety-significant 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.

Safety-significant SSCs, are not required to consider performance criteria traditionally associated with safety-class SSCs or traditional nuclear standards in general. Performance criteria for a safety-significant SSC should be representative of the general rigor associated with non-nuclear power reactor industrial and OSHA practices. Performance criteria for safety-significant SSCs are developed by DSA preparers using engineering judgment based on the expected functions for which it was designated a safety-significant SSC and its overall importance to safety.

Evaluate the capabilities of the SSC to meet performance criteria. The evaluation should be as simple as possible, and rely on engineering judgment, calculations, or performance tests as opposed to formal design reconstitution. For example, the hydrogen detector could be fed a test gas composition that would exceed its interlock trip point. Such a test would typically bound the needed equipment performance as response time is not a highly sensitive parameter.

4.4.X.5 Controls (TSRs)

This subsection identifies those assumptions requiring TSRs to ensure performance of the safety function.

4.5 SPECIFIC ADMINISTRATIVE CONTROL

Relevant information is provided, in the following SAC specific subsections, for SACs with descriptions sufficiently detailed to provide an understanding of the safety function of the SAC. Descriptions for each SAC must be complete enough to indicate suitability of safety analysis inputs and assumptions (see DOE-STD-1186). Provide a summary list of SACs. This summary list should identify, in tabular form, SACs, the accidents from 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 administrative controls as SACs.

4.5.X [Applicable Specific Administrative Controls]

Identify the SAC.

4.5.X.1 Safety Function

This subsection states the reason for designating an administrative control as a 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 Material at Risk 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 subsection provides a description of the SAC and the basic principles by which it performs a safety function (e.g., nuclear material control procedure for the MAR limit discussed in section 4.5.X.1). Describe its boundaries and interface points with any SSCs relevant to the safety function, such as procedural actions interfacing with sensors/instrumentation and equipment.

If a SAC is utilized in lieu of the identification of safety SSCs, clearly identify and discuss the rationale for this decision. Engineering controls are preferable over ACs and SACs, and emphasis should be placed on identifying safety SSCs. Include a discussion regarding why SSC(s) are not plausible or practical for accomplishing the safety function.

Identify SSCs whose failure would result in losing the ability to complete the action required by the SAC. These SSCs would also be considered safety-class or safety-significant based on the significance of the SAC safety function.

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

4.5.X.3 Functional Requirements

This subsection identifies requirements that are specifically needed to fulfill safety functions. Such functional requirements are specified for both the SAC and any needed support SSCs.

Limit functional requirement designation to those requirements necessary for the SAC safety function. Functional requirements are 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 must fully address all aspects important for ensuring the SAC can be accomplished.

4.5.X.4 SAC Evaluation

This subsection provides 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.

The formulation of SACs should include a process that validates that plant operators can perform the task(s) called for in a 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
- Stress levels induced by the external environment, e.g., noise, heat, light and protective clothing worn.

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 available time interval necessary 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 subsection identifies those assumptions requiring TSRs to ensure performance of the safety function. SACs are implemented in TSRs generally by either of two forms, as identified below.

- LCO/Surveillance Requirement – SACs can often be written in the format of an LCO.
- Specific "Directive Action" Administrative Control – A Specific "Directive Action" administrative control TSR can be in the Administrative Controls section of the TSRs.

Section 4 of DOE-STD-1186 "Specific Administrative Controls" discusses the treatment of SACs in TSRs.

Chapter 5
Derivation of Technical Safety Requirements

PURPOSE. The purpose of this DSA chapter is to provide information necessary to support the safety basis requirements for the derivation of hazard controls in 10 CFR 830.

This chapter builds upon the control functions determined to be essential in Chapter 3, "Hazard and Accident Analyses," and Chapter 4, "Safety Structures, Systems, and Components," to derive TSRs. This chapter is meant to support and provide the information necessary for the separate TSR document required by 10 CFR 830.205. Derivation of TSRs consists of summaries and references to pertinent sections of the DSA in which design (i.e., SSCs) and administrative features (i.e., non-SSCs) are needed to prevent or mitigate the consequences of accidents. Design and administrative features addressed include ones which: (1) provide significant defense in depth; (2) provide for significant worker safety; or (3) provide for the protection of the public. Expected products of this chapter, as applicable based on the graded approach, include:

- Information with sufficient basis from which to derive, as appropriate, any of the following TSR parameters for individual TSRs:
  - Safety Limits (SLs).
  - Limiting Control Settings (LCSs).
  - Limiting Conditions for Operation (LCOs).
  - Surveillance Requirements (SRs).
- Information with sufficient basis from which to derive TSR administrative controls for specific control features (SACs) or to specify programs necessary to perform institutional safety functions.
- Identification of passive design features addressed in the DSA.
- Identification of TSRs from other facilities that affect the facility's safety basis.

Existing support documentation is to be referenced. Include brief abstracts of referenced documentation with enough essential facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Hazard Category 2 and 3 facilities include TSR information based on material detailed in Chapters 3 and 4. For Hazard Category 3 facilities, TSRs may consist solely of an inventory limit to maintain the Hazard Category 3 classification and provide appropriate commitments to safety programs in the administrative controls section of TSRs.

It can be expected that Hazard Category 2 facilities will have more TSRs than Hazard

Category 3 facilities. The application of graded approach for TSR designation is, however, still significant. Hazard Category 2 facilities include process operations that have traditionally made limited use of TSR limits. These facilities have few scenarios where one failure directly leads to large hazardous material releases, and therefore do not warrant a large number of TSRs. Defaulting all controls to TSR coverage will create a regulatory environment that is difficult to manage and would downplay needed emphasis on the most significant controls. This could produce a negative impact on facility safety.

The majority of Hazard Category 2 facilities are not anticipated to need SLs. Even facilities that designate SLs will not need many. Potential candidates for SL designation are restricted to those controls that prevent exceeding Evaluation Guidelines. TSRs assigned for defense in depth and safety-significant SSCs (i.e., not related to meeting Evaluation Guidelines) will not use SLs. The decision as to whether an operating limit (such as an LCO) or a TSR administrative control is more appropriate is left to the judgment of the DSA preparer. If TSR administrative controls are used, descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why.

For administrative controls designated as specific administrative controls, the DSA preparer should refer to DOE-STD-1186-2004, "Specific Administrative Controls," for implementing SACs into TSRs.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 5

5.1 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.

5.2 REQUIREMENTS

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

- Provide significant defense in depth. These features are safety-significant

SSCs or SACs noted in Section 3.3.2.3.2 and their associated assumptions requiring TSR coverage identified in Section 4.4.X.5, and any other TSR assumptions.

- Provide for significant worker safety. These features are safety-significant SSCs or SACs identified in Section 3.3.2.3.3 and their associated assumptions requiring TSR coverage identified in Section 4.4.X.5, and any programs identified as needing coverage in TSR administrative controls in Section 3.3.2.3.3.
- Provide for significant public safety in accordance with implementation of the Evaluation Guideline. These features are safety-class SSCs or SACs, and assumptions requiring TSR coverage identified in Sections 3.4.2.X.5, and 4.3.X.5.

Presentation of the summary of TSRs could easily become disorganized and difficult to follow. It is recommended that the information be distilled into an organized presentation (e.g., table format) that identifies the relevant hazard and the major features relied on for protection against that hazard. This presentation will form the basis for organization of the remainder of the chapter. Associated TSR SLs, LCSs, LCOs, surveillance requirements, administrative controls and Design Features identified throughout the remainder of the chapter need to be noted in this presentation for overall clarity.

This subsection will specifically note those safety SSCs listed, if any, that will not be provided with TSR coverage and provide accompanying explanation.

5.4 DERIVATION OF FACILITY MODES

This section derives basic operational modes (e.g., startup, operation, shutdown) used by the facility that are relevant to derivation of TSRs. The definition of modes required in this subsection expands and formalizes the information provided in Chapter 3, "Hazard and Accident Analyses," regarding operational conditions associated with accidents.

5.5 TSR DERIVATION

Note: This information can be organized by the hazard protected against, the specific features or even actual TSRs if desired. The choice of a specific 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 subsection identifies the specific feature(s) listed in 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 provides the basis and identifies information sufficient to derive SLs, LCSs, and LCOs to support the facility TSR documentation required by 10 CFR 830.205. SLs, if used, are reserved for a small set of extremely significant features that prevent potentially major offsite impact. 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 SL identified, thereby providing a margin of safety. Most LCOs are assigned without an accompanying SL.

Generally SLs are applicable only for protection of passive barriers as close to the accident source as possible whose failure, due to the occurrence of a specific event, will result in exceeding the Evaluation Guideline. Mitigation of releases is generally not amenable to useful definition of SLs. For example, a ventilation system directing airflow through HEPA filters to keep offsite radiological dose below the Evaluation Guideline during an accident is mitigative and is more appropriately covered by a LCO. Temporary loss of its 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 a SL would be academic 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 Evaluation Guideline without ventilation mitigation. If that tank could experience a hydrogen explosion and rupture, then the tank hydrogen concentration may warrant coverage by a SL.

5.5.X.2 Surveillance Requirements

This section provides the basis and identifies 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 provides the basis and identifies information necessary to derive TSR administrative controls. This section is the only applicable section for those features listed in Section 5.3, “TSR Coverage,” that are provided with only TSR administrative controls. The rationale for assigning TSR administrative controls need to be clearly and briefly stated.

A special type of TSR administrative control is that covering a safety management program. The administrative controls section of the TSR document will contain commitments to establish, maintain, and implement these programs at the facility and, as appropriate, facility staffing requirements. Specific administrative controls, 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 Chapter 2, "Facility Description" for the descriptions if that chapter contains the desired information.

5.7 INTERFACE WITH TSRs FROM OTHER FACILITIES

This section summarizes TSRs from other facilities that affect this facility's safety basis and briefly summarize the provisions of those TSRs.

Chapter 6
Prevention of Inadvertent Criticality

PURPOSE. The purpose of this chapter is to provide information that will support the development of a safety basis in compliance with the provisions of 10 CFR 830.204(b) (6) regarding the definition of a criticality safety program. If this information is available in a site-wide criticality safety program description, and it complies with the Rule requirements, then it can be included by reference and summarized in this chapter.

Expected products of this chapter include:

- Definition of a criticality safety program that (1) ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions, (2) identifies applicable nuclear criticality safety standards, and (3) describes how the program meets applicable nuclear criticality standards.
- Description of the basis and analytical approach the facility uses for deriving operational criticality limits.
- Summary of design and administrative controls used by the criticality safety program.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Hazard Category 3 facilities, by definition, do not contain sufficient fissile materials to present a criticality hazard. This chapter is, therefore, not applicable to Hazard Category 3 facilities. Inventory limits specified in the TSRs will control the amount of fissile materials. This chapter applies only to Hazard Category 2 facilities with inventories of fissile materials sufficient to present an inadvertent criticality hazard.

CONTENT GUIDANCE FOR SECTIONS OF 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 REQUIREMENTS

This section lists 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 for 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.

6.3 CRITICALITY CONCERNS

This section identifies the fissile material available within the facility and provides information on the location of potential criticality hazards (e.g., description, and drawing), the fissile material form (e.g., chemical and/or physical, including isotopic content, concentration, densities), and the maximum quantities involved. This information should be summarized from Chapter 3, "Hazard and Accident Analyses."

6.4 CRITICALITY CONTROLS

This section summarizes information relevant to criticality control. Include a general discussion of the criticality safety design limits, their bases, and any design criteria used to ensure subcritical configurations under all normal, abnormal, and accident conditions (i.e., ensure criticality limits are not exceeded); the parameters used for the prevention and control of criticality and the methods for the application and validation of these parameters; and the application of the double contingency principle in criticality safety. It is not the intention of this section to individually list all criticality safety design limits.

6.4.1 Engineering Controls

This section summarizes the safety design limits on engineered controls, either passive or active, and the bases placed on equipment designs or operations to ensure subcritical conditions under all normal, abnormal, and accident conditions. Include in the summary of these engineered controls use of geometry, spacing, and any other engineered controls (e.g., neutron absorbers, elimination of moderators, storage location limitations, and level detectors). This section also summarizes the configuration control program as it relates to

the configuration of the equipment used to store, handle, transport, or process fissile material.

6.4.2 Administrative Controls

This section summarizes the administrative controls used to prevent accidental criticality. Include in the discussion the administrative controls on nuclear material safety limits such as mass, moderators, changes in geometry configurations, and procedures for handling, storing, and transporting fissile materials. Discuss also the administrative controls for reviewing and approving changes to process or system configurations.

6.4.3 Application of Double Contingency Principle

This section summarizes the methods used to ensure that at least more than one unlikely, independent, and concurrent changes in process conditions would be necessary before a criticality accident is possible (e.g., contingency or criticality safety evaluation). The contingency or criticality safety evaluation will identify how the double contingency principle, as defined in DOE O 420.1, is being met (i.e., control of two independent process parameters or a system of multiple controls on a single parameter). It is not the intention of this section to individually present all facility contingency or criticality safety evaluations.

The results of the contingency or criticality safety evaluation helps identify safety SSCs, controls, and the TSR limit designations (safety control parameters). The identification of safety SSCs and safety control parameters for TSR controls should be done as part of Chapter 3, "Hazard and Accident Analyses," Chapter 4, "Safety Structures, Systems, and Components," and Chapter 5, "Derivation of Technical Safety Requirements."

6.5 CRITICALITY SAFETY PROGRAM

This section presents an overview of the organizational structure and interfaces, and the technical and administrative practices of the criticality protection policy and programs. It shows how the criticality safety program satisfies the criticality safety standards.

6.5.1 Criticality Safety Organization

This section summarizes the organizational structure that administers the criticality safety program. Include information about staffing levels, positions of authority and responsibilities, and staff qualifications. Discuss the interfaces and interrelationships with other safety organizations and facility operations. Reference the administrative plans and procedures that implement the criticality safety program.

Include in the summary the purpose, organization, and functions of any committees responsible for criticality safety. Include in the description the charter of responsibilities, scope of reviews, and qualifications and

requirements for committee members. This summary may be provided in this chapter or Chapter 17, "Management, Organization, and Institutional Safety Provisions."

6.5.2 Criticality Safety Plans and Procedures

This section summarizes the criticality safety plans and procedures for governing operations involving fissile materials. Discuss the document control measures employed to ensure that plans and procedures, including changes, are reviewed for adequacy, approved for release by authorized personnel, and distributed to and used at the locations where fissile materials are used, processed, or stored.

Include in the summary abstracts of procedures for posting criticality safety limits, material and operational controls, review of operations, emergency evacuation, and guidelines for permitting fire fighting water or other moderating materials used to suppress fires within or adjacent to moderation control areas. These guidelines on fire fighting are based on comparisons of risks and consequences of accidental criticality with the risks and consequences of postulated fires for the respective areas. The bases for guidelines for fire fighting are to be referenced or documented here. This section is interdependent with Chapter 11, “Operational Safety” and Chapter 17, “Management, Organization, and Institutional Safety Provisions.”

6.5.3 Criticality Safety Training

This section summarizes the scope of facility wide criticality safety training as well as the specific training requirements for personnel associated with the operation of the facility. Discuss specifically the training of personnel on the configuration of the equipment used to store, handle, transport, or process fissile material. Reference, as appropriate, Chapter 12, “Procedures and Training” if that chapter presents requested information.

6.5.4 Determination of Operational Nuclear Criticality Limits

This section summarizes the analytical approach (i.e., methods, codes, and analysis techniques) used to derive operational nuclear criticality limits, including the error contingency criteria or margin of error (uncertainty), the use of contingency analyses, and the basic justification of the appropriateness of such an approach (i.e., bases and design criteria). This section should not include detailed calculations and limits for the facility.

This section explains and demonstrates the relationship between operational nuclear criticality limits and their TSR designations.

6.5.5 Criticality Safety Inspections/Audits

This section summarizes the criticality safety inspection and audit programs that verify the established procedures used for preventing inadvertent criticalities. This includes their responsibilities and authorizations and the

criteria used to select items, functions, analysis, etc., for inspections and audits. This section also provides a discussion of associated facility record keeping.

6.5.6 Criticality Infraction Reporting and Follow-Up

This section provides a brief summary of the criticality infraction program for reporting and follow-up of criticality infractions. Include in the discussion provisions for the recovery from criticality infractions. Provide brief assurances that program results and lessons learned are incorporated into the safety analysis.

6.6 CRITICALITY INSTRUMENTATION

This section summarizes the criticality alarm system and detection systems used to mitigate exposures from a criticality event. Include in the summary the methods and procedures used to determine the placement of the monitoring equipment and the selection of the equipment functions and sensitivity, if required.

Chapter 7
Radiation Protection

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the radiation protection program. It is intended to describe the essential characteristics of the program as it relates to facility safety.

This chapter summarizes provisions for radiation protection. Summaries focus on radiation protection based on facility hazards to provide a basic understanding of the scope of the radiation protection program. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the overall radiation protection program and organization.
- Description of the radiological As Low As Reasonably Achievable (ALARA) policy and program.
- Description of radiation exposure control including administrative limits, radiological practices, dosimetry, and respiratory protection.
- Identification of radiological monitoring to protect workers, the public, and the environment.
- Discussion of radiological protection instrumentation.
- Description of the plans and procedures for maintaining records of radiation sources, releases, and occupational exposures.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Summaries focus on the major provisions of the facility radiation protection program based on the type and magnitude of hazards identified in the hazard analysis (Chapter 3). Type of hazard determines generic applicability of certain provisions, and magnitude of hazard can influence the breadth of description (e.g., larger quantities of material may warrant a wider range of dosimetry concerns). However, the descriptions should be at summary level only, with reference to the facility document(s) controlling the program. Additionally, simply note where any generic programmatic aspects identified in this chapter are not relevant for a facility.

Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 7

7.1 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.

7.2 REQUIREMENTS

This section lists the design codes, standards, regulations (e.g., 10 CFR 835, "Occupational Radiation Protection"), and DOE Orders which are required for establishing the safety basis of the facility. The intent is to provide only the requirements that are specific for 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.

7.3 RADIATION PROTECTION PROGRAM AND ORGANIZATION

This section summarizes the program, including the safety management policies and philosophies used as a basis for the program. Reference facility documents detailing the program. Identify the organizational structure of the radiation protection program including staffing levels and qualifications, positions of authority and responsibilities, and interfaces with other safety organizations and facility operations. The organizational summary may be provided in this chapter or Chapter 17, "Management, Organization, and Institutional Safety Provisions."

7.4 ALARA POLICY AND PROGRAM

This section summarizes the ALARA policy and program for the facility.

7.5 RADIOLOGICAL PROTECTION TRAINING

This section summarizes plans and procedures for training general employees, radiation workers, radiation protection technicians, supervisors, and managers who are involved in operations or maintenance activities in any area where radiological protection is required. Reference, as appropriate, Chapter 12, "Procedures and Training" if that chapter presents requested information.

7.6 RADIATION EXPOSURE CONTROL

This section summarizes the plans and procedures for controlling: (1) external occupational exposure to radiation; (2) spread of contamination; and (3) inhalation or ingestion of radioactive materials.

7.6.1 Administrative Limits

This section summarizes facility administrative control levels and dose limits, including process for planned special exposures.

7.6.2 Radiological Practices

This section summarizes exposure controls directly associated with radiological activities. Include in this summary generic precautions for conduct of radiological tasks, special personnel protective equipment, and permanent shielding used to control exposures.

This section specifically summarizes plans and procedures for posting, labeling, or signifying boundaries for facility areas containing radioactive material and material containers and entry and exit control for personnel in radiological areas in the facility. Include in the summary use of radiation work permits and provisions for controlling access and stay times, and definition and posting requirements for the following radiological areas: radiation area, high radiation area, very high radiation area, airborne radioactivity area, high contamination area, and radiological buffer areas.

7.6.3 Dosimetry

This section summarizes the basis of the dosimetry program for external and internal radiation monitoring of workers. Include in the summary basis for use of various types of dosimeters including accident dosimetry and bioassay requirements (i.e., bases for selecting personnel, frequency of routine in vivo and in vitro and any nonroutine bioassay conducted). Briefly discuss the program in terms of issuance, control, and monitoring of dosimeters and documentation of dosimetry results including combining internal and external dosimetry results.

7.6.4 Respiratory Protection

This section summarizes plans and procedures for respiratory protection for workers. Include in this summary types of respiratory protection equipment and their usage in normal, abnormal, and accident conditions; control and issuance of respirators (training; fitness and medical testing); inspection of equipment (cleaning, maintenance, and repair); and documentation of associated records.

7.7 RADIOLOGICAL MONITORING

This section summarizes the radioactive material sampling and monitoring program conducted internal and external to the facility. This summary should address overall facility monitoring to prevent the spread of radioactive contamination, operational monitoring of workers, and monitoring and sampling for detection of material release by airborne and other pathways (e.g., water, soil), programs for continuing collection of relevant meteorological data, and records, and reports generated in the monitoring program.

7.8 RADIOLOGICAL PROTECTION INSTRUMENTATION

This section summarizes plans and procedures governing radiation protection instrumentation. Such instrumentation, whether fixed, portable, or laboratory use, includes instruments for radiation and contamination surveys; sampling; area radiation monitoring; and personnel monitoring during normal operations and accidents. Include in the summary selection and placement criteria for technical equipment and instrumentation, types of detectors and monitors, and their quantity, sensitivity, and range. This section also summarizes plans and procedures for control of calibration processes and for quality assurance for calibration and maintenance. Reference Chapter 2, "Facility Description," Chapter 10, "Initial Testing, In-Service Surveillance, and Maintenance," and Chapter 14, "Quality Assurance," if those chapters contain requested information.

7.9 RADIOLOGICAL PROTECTION RECORD KEEPING

This section summarizes plans and procedures for retention, and disposition of records and reports. Discuss document control measures used to ensure that records are reviewed for adequacy, approved for release by authorized personnel, and distributed to and used at the locations where required and when needed.

7.10 OCCUPATIONAL RADIATION EXPOSURES

This section summarizes the predicted annual exposures to workers from radiation sources. Worker exposure information will be based on historical facility radiation data if the operations have not changed.

For new operations or facilities that do not have historical records, provide an estimate of the projected (calculated) annual exposures to the workers from normal operations (not including accidents). Base such estimates on expected average and maximum operating conditions, inventories, operating cycles, personnel occupancy factors, etc., for the facility. Identify the methods, and assumptions used in estimating occupational exposures. It is acceptable to estimate exposures based on historical data for similar facilities.

Finally, this section provides a comparison of the measured, estimated (calculated), or both, worker exposures with the maximum allowable limits. Any discrepancies among these estimated, measured, or allowed values need to be discussed.

Chapter 8
Hazardous Material Protection

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the hazardous material protection program. It is intended to describe the essential characteristics of the program as it relates to facility safety.

This chapter summarizes provisions for hazardous material protection other than radiological hazards. Summaries focus on hazardous material protection based on facility hazards to provide a basic understanding of the scope of the hazardous material protection program. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the overall hazardous material protection program and organization.
- Description of the hazardous material ALARA policy and program.
- Description of hazardous material exposure control including identification of hazardous material, administrative limits, occupational medical programs, and respiratory protection.
- Identification of hazardous material monitoring to protect workers, the public, and the environment.
- Discussion of hazardous material protection instrumentation.
- Description of the plans and procedures for maintaining hazardous material records, hazard communications, and occupational exposures.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Summaries focus on the major provisions of the facility hazardous material protection program based on the type and magnitude of hazards identified in the hazard analysis (Chapter 3). Type of hazard determines generic applicability of certain provisions, and magnitude of hazard can influence the breadth of description (e.g., larger quantities of material may warrant a wider range of monitoring concerns). However, the descriptions should be at summary level only, with reference to the facility document(s) controlling the program. Additionally, simply note where any generic programmatic aspects identified in this chapter are not relevant for a facility.

Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 8

8.1 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.

8.2 REQUIREMENTS

This section lists 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 for 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.

8.3 HAZARDOUS MATERIAL PROTECTION AND ORGANIZATION

This section summarizes the program, including the safety management policies and philosophies used as a basis for the program. Reference facility documents detailing the program. Identify the organizational structure of the hazardous material protection program including staffing levels and qualifications, positions of authority and responsibilities, and interfaces with other safety organizations and facility operations. The organizational summary may be provided in this chapter or Chapter 17, "Management, Organization, and Institutional Safety Provisions."

8.4 ALARA POLICY AND PROGRAM

This section summarizes the ALARA policy and program for the facility. Historically, hazardous materials, unlike radioactive materials, have often been evaluated assuming de minimis level below which little harm is associated with exposures (e.g., OSHA Permissible Exposure Limits). Where this is the case for given subject matter, ALARA needs to be considered a qualitative concept evaluated against OSHA and industrial hygiene exposure standards and guidelines.

8.5 HAZARDOUS MATERIAL TRAINING

This section summarizes plans and procedures for general training of employees on hazardous material safety, training of workers, supervisors, and managers who are involved in activities involving hazardous materials protection, and training of industrial hygiene technicians. Reference, as appropriate, Chapter 12, "Procedures and Training" if that chapter presents requested information.

8.6 HAZARDOUS MATERIAL EXPOSURE CONTROL

This section summarizes the plans and procedures for controlling: (1) occupational exposure to hazardous materials; and (2) spread of hazardous material contamination.

8.6.1 Hazardous Material Identification Program

Summarize the plans and procedures the facility uses for the identification and evaluation of material hazards, (e.g., toxicity, flammability, reactivity). Include in this summary overall industrial hygiene programs, plans, and procedures, and hazard elimination or control measures. Reference and abstract any relevant site manuals detailing these programs.

8.6.2 Administrative Limits

This section summarizes facility administrative control levels and exposure limits.

8.6.3 Occupational Medical Programs

This section summarizes the components of the occupational medical program relevant to hazardous material protection, including physical examinations, medical evaluations, medical surveillance (including bioassay), and medical record keeping.

8.6.4 Respiratory Protection

This section summarizes plans and procedures for respiratory protection for workers. Include in this summary types of respiratory protection equipment and their usage in normal, abnormal, and accident conditions; control and issuance of respirators (training; fitness and medical testing); inspection of equipment (cleaning, maintenance, and repair); and documentation of associated records. If no special distinctions exist with regard to the respiratory protection program described in section 7.6.4, simply reference that section

8.7 HAZARDOUS MATERIAL MONITORING

This section summarizes the hazardous material sampling and monitoring program conducted internal and external to the facility. This summary should address overall facility monitoring to prevent the spread of hazardous materials, operational monitoring of workers, and monitoring and sampling for detection of material release by airborne and other pathways (e.g., water, soil), programs for continuing collection of relevant meteorological data, and records, and reports generated in the monitoring program.

8.8 HAZARDOUS MATERIAL PROTECTION INSTRUMENTATION

This section summarizes plans and procedures governing hazardous protection instrumentation. Such instrumentation, whether fixed, portable, or laboratory use, includes instruments for hazardous material and contamination surveys; sampling; area hazardous material monitoring; and personnel monitoring during normal operations and accidents. Include in the summary selection and placement criteria for technical equipment and instrumentation, types of detectors and monitors, and their quantity, sensitivity, and range. This section also summarizes plans and procedures for control of calibration processes and for quality assurance for calibration and maintenance. Reference Chapter 2, "Facility Description," Chapter 10, "Initial Testing, In-Service Surveillance, and Maintenance," and Chapter 14, "Quality Assurance," if those chapters contain requested information.

8.9 HAZARDOUS MATERIAL PROTECTION RECORD KEEPING

This section summarizes plans and procedures for retention, and disposition of records and reports. Discuss document control measures used to ensure that records are reviewed for adequacy, approved for release by authorized personnel, and distributed to and used at the locations where required and when needed.

8.10 HAZARD COMMUNICATION PROGRAM

This section summarizes the facility's hazard communication program for obtaining material safety data sheets, providing for employee information and training, directions for nonroutine tasks and outside contractor, and information for multi employer worksites and hazardous material labeling.

8.11 OCCUPATIONAL CHEMICAL EXPOSURES

This section summarizes the predicted annual exposures to workers from hazardous material sources. Worker exposure information will be based on historical facility data if the operations have not changed.

For new operations or facilities that do not have historical records, provide an estimate of the projected (calculated) annual exposures to the workers from normal operations (not including accidents). Base such estimates on expected average and maximum operating conditions, inventories, operating cycles, personnel occupancy factors, etc., for the facility. Identify the methods, and assumptions used in estimating occupational exposures. It is acceptable to estimate exposures based on historical data for similar facilities.

Finally, this section provides a comparison of the measured, estimated (calculated), or both, worker exposures with the maximum allowable limits. Any discrepancies among these estimated, measured, or allowed values need to be discussed.

Chapter 9
Radioactive and Hazardous Waste Management

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the radioactive and hazardous waste management program. It is intended to describe the essential characteristics of the program as it relates to facility safety.

This chapter describes the provisions for radioactive and hazardous waste management. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the overall radioactive and hazardous waste management program and organization.
- Description of the site-specific radioactive, mixed, and hazardous material waste management policy, objectives, and philosophy.
- Identification of hazardous waste streams, including types, sources, and quantities.
- Description of the waste management process, and waste treatment and disposal systems, including design and administrative controls.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. In general, the complexity of waste systems and the management of waste is directly proportional to the quantities and types of wastes associated with facility operations. If facilities handle very low quantities or concentrations of material, the aspects of waste treatment become less significant. For facilities whose mission is D&D or environmental restoration, this chapter addresses those aspects of radioactive and hazardous waste management that are a result of operations pertaining to the mission. For example, for a facility doing environmental restoration, a summary of the management of radioactive and hazardous waste streams that result from that operation are included in this chapter. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis. Do not describe waste minimization aspects of operations.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 9

9.1 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.

9.2 REQUIREMENTS

This section lists 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 for 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.

9.3 RADIOACTIVE AND HAZARDOUS WASTE MANAGEMENT PROGRAM AND ORGANIZATION

This section summarizes the program, including the safety management policies and philosophies used as a basis for the program. Reference facility documents detailing the program. Identify the organizational structure that administers the radioactive and hazardous waste management program. This summary includes the plans, procedures, and training for governing radioactive and hazardous waste management activities. The organizational summary may be provided in this chapter or Chapter 17, "Management, Organization, and Institutional Safety Provisions."

9.4 RADIOACTIVE AND HAZARDOUS WASTE STREAMS AND SOURCES

Summarize the solid, liquid, and gaseous waste streams and sources, including estimated inventories. Identify the waste management and waste handling process or treatment system for each of the following waste types:

- Radioactive waste.
- Mixed Waste
- Hazardous waste.

Simply reference the hazard identification of Chapter 3, "Hazard and Accident Analysis," and information in Chapter 2, "Facility Description," if these chapters contain requested information.

9.4.1 Waste Management Process

This section summarizes the overall waste management plan, including an overall management policy or philosophy. Summarize the administrative and

operational practices important to the effective management of each of the waste types, such as waste segregation.

9.4.2 Waste Sources and Characteristics

This section summarizes how and where the waste is generated (i.e., waste streams) and how it enters the appropriate waste handling or treatment system. For each waste type (i.e., radioactive, mixed, or hazardous) discuss by characteristics, composition, and waste material form (i.e., gaseous, liquid, or solid) the effluent discharges, emission limits, and permitting.

9.4.3 Waste Handling or Treatment Systems

This section summarizes the processes to treat different waste types and forms produced in the facility. This brief summary should include system function, and basic chemical or physical operating principles (e.g., sedimentation, ion exchange, decanting). Also include or reference simplified process flow diagrams that show the location of equipment and instrumentation (including monitoring equipment).

Chapter 10
Initial Testing, In-Service Surveillance, and Maintenance

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. . This chapter is not intended to be the vehicle for review and approval of the surveillance, testing, or maintenance programs. It is intended to describe the essential characteristics of the program as it relates to facility safety.

This chapter describes the essential features of the testing, surveillance, and maintenance programs. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the facility initial testing program.
- Description of the facility in-service surveillance program.
- Description of the planned, predictive, preventive, and corrective facility maintenance programs.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. For Hazard Category 2 facilities, the discussion is expected to focus on the surveillance of safety SSCs. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 10

10.1 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.

10.2 REQUIREMENTS

This section lists 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 for 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.

10.3 INITIAL TESTING PROGRAM

This section briefly summarizes the initial testing program. This summary includes the initial testing program that ensures operability of a facility modification prior to service and information to ensure that adequate testing activities exist to support facility safety management. Reference relevant site manuals as appropriate.

10.4 IN-SERVICE SURVEILLANCE PROGRAM

This section summarizes the in-service surveillance program. The summary should cover provisions for testing and calibrations, control and calibration of test equipment, trending of surveillance test results, programmatic review, and training of personnel performing surveillance. Reference relevant site manuals as appropriate.

10.5 MAINTENANCE PROGRAM

This section summarizes the maintenance program supporting safe operation of the facility. The summary should include the maintenance organization, training of maintenance personnel, maintenance facilities and equipment, post maintenance testing; control and calibration of measuring equipment, and maintenance history and trending. Reference relevant site manuals as appropriate.

Chapter 11
Operational Safety

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of an operational safety or fire protection program. It is intended to describe the essential characteristics of the programs as they relate to facility safety.

This chapter discusses general aspects of operational safety. It specifically focuses on the bases for the conduct of operations program specified by DOE 5480.19, "Conduct of Operations Requirements for DOE Facilities." It is recognized, however, that DOE 5480.19 addresses many of the other DSA topics covered in 10 CFR 830 (e.g., management, organization, and the institutional safety provisions, procedures and training, human factors). The attachment to DOE 5480.19 specifically notes that "these guidelines have, therefore, been prepared to assist facilities in the review and development of programs important to operations." Therefore, elements of conduct of operations are discussed elsewhere in this standard. Major issues of operations organization and administration and training are covered in Chapter 12, "Procedures and Training," and Chapter 17, "Management, Organization, and Institutional Safety Provisions." Major issues of notification and reporting practices, and investigation of abnormal events are covered in Chapter 17. Control of procedures is covered in Chapter 12.

Discussion of all the sub-headings of Attachment 1 to DOE 5480.19 is not necessary in this chapter. Again, this chapter is not intended to be the vehicle for demonstrating compliance with DOE 5480.19 (i.e., review and approval of a conduct of operations program). It is intended to acknowledge the intent of conduct of operations, indicate the aspects of conduct of operations directly applicable to the facility, and summarize the main aspects of conduct of operations implementation at the facility.

This chapter describes: (1) the bases for the conduct of operations program; and (2) the fire protection program. Expected products of this chapter, as applicable based on the graded approach, include:

- Identification of the aspects of Conduct of Operations directly applicable to the facility.
- Integrated summary of the main features of the facility Conduct of Operations program.
- Description of facility fire protection program

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The level of detail in this chapter is dependent on hazards associated with facility operations and the complexity of those operations. Conduct of operations also becomes more important as facility complexity increases.

The full conduct of operations program was originally developed for nuclear reactors, and DOE 5480.19 acknowledges that the guidelines are written so as to allow flexibility. For example, a facility that consists of a sequence of manual operations may not have a control room, and thus would not need to address control area activities. Remediation sites may not have a need for shift operations as anticipated by the Order or specific shift activities, such as on shift training.

The presentation of conduct of operations focuses, however, on a brief description of what aspects of conduct of operations are directly applicable and to what extent they are applied based on the type of operation occurring. Salient features may be referred to by general title only with reference to more detailed procedures or policies.

A description of the fire prevention program is required for all facilities as well. The level of detail should be directly related to either direct fire potential due to processing large amounts of flammable material or the quantity and type of hazardous materials that could be affected by a fire. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 11

11.1 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.

11.2 REQUIREMENTS

This section lists 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 for 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.

11.3 CONDUCT OF OPERATIONS

This section summarizes applicability of conduct of operations to the facility and briefly identifies salient features of the conduct of operations program. Specific topical areas from DOE 5480.19 that should be considered are:

- Shift routines and operating practices.
- Control area activities.
- Communications.
- Control of on shift training.
- Control of equipment and system status.
- Lockouts and tagouts.
- Independent verification.
- Log keeping.
- Operations turnover.
- Operations aspects of facility chemistry and unique processes.
- Required reading.
- Timely orders to operators.
- Operator aid postings.
- Equipment and piping labeling.

11.4 FIRE PROTECTION

11.4.1 Fire Hazards

This section provides a realistic discussion of the magnitude of facility fire hazards in terms of overall combustible and explosive loading in proximity to hazardous materials being protected. This information should be based on and correlate with accident descriptions in Chapter 3, "Hazard and Accident Analyses."

Results of overall assessments, such as Fire Hazards Analyses and actual facility walkdowns, should be summarized as appropriate to put fire interaction with material into a proper perspective (e.g., will material be within flame zone, heated indirectly, or largely unaffected). The purpose of this section is to define the main fire protection issues of interest in the DSA.

11.4.2 Fire Protection Program and Organization

This section summarizes the program, including the safety management policies and philosophies used as a basis for the program. These elements should include the overall conceptual approach to fire and explosion

prevention, and the means used to identify facility fire and explosive hazards, including periodic update reviews. Reference facility documents detailing the program.

Identify the organizational structure that administers the fire protection program and the main elements of the program. Organizational aspects of this summary may be provided in this chapter or Chapter 17, "Management, Organization, and Institutional Safety Provisions."

11.4.3 Combustible Loading Control

This section summarizes the program used to prevent unnecessary combustible loading in the facility. The bases for the program, storage practices for allowed flammable, combustible, and reactive materials loading, the main mechanisms for limiting combustible loading during operations, maintenance, etc. for the types of activities performed, and the frequency of inspections are noted here.

11.4.4 Fire Fighting Capabilities

Based on the fire hazards, this section summarizes available fire fighting equipment, fire response procedures, basic training and personnel qualifications for fire fighters, and special precautions taken for fire fighting in radiological and hazardous chemical environments. Reference, as appropriate, Chapter 12, "Procedures and Training" if that chapter presents requested information.

11.4.5 Fire Fighting Readiness Assurance

This section summarizes: (1) the fire prevention inspection program, including basic scheduling and resolution of inspection findings; (2) types and frequencies of fire safety drills and exercises, and (3) the fire protection program record keeping requirements.

Chapter 12
Procedures and Training

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the procedures or training programs. It is intended to describe the essential characteristics of the programs as they relate to facility safety.

This chapter describes the processes by which the technical content of the procedures and training programs are developed, verified, and validated. These processes will ensure that the facility is operated and maintained by personnel who are well qualified and competent to carry out their job responsibilities using procedures and training elements that have been well developed and are kept current by the use of feedback and continuous improvement. A programmatic commitment to ongoing procedures and training programs is considered to be a necessary part of safety assurance. Expected products of this chapter, as applicable based on the graded approach, include:

- Summary of the overall facility procedures and training programs.
- Description of the processes by which the form and content of procedures and training materials are developed, verified and validated for normal, abnormal, and emergency operations; surveillance testing and maintenance.
- Summary of the processes for maintaining written procedures, training materials, and training records.
- Summary of the processes for modifying procedures and training materials.
- Summary of the methods used to feed back operations experience, new analyses, other DSA changes, etc., to the procedures and training programs.
- Description of the mechanisms to identify and correct technical or human factors deficiencies.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Distinction is limited for this chapter and relates only to varying scope of procedure and training programs required for a given hazard and complexity level. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 12

12.1 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.

12.2 REQUIREMENTS

This section lists 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 for 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.

12.3 PROCEDURE PROGRAM

This section summarizes the facility procedures program, including brief statements addressing the safety management policies and philosophies used as a basis for the program. Reference facility documents detailing the program. Do not list specific procedures.

12.3.1 Development of Procedures

This section summarizes how procedures are selected for development and describes the processes by which the technical content of procedures is developed, verified, and validated for normal, abnormal, and emergency operations; and for surveillance testing and maintenance.

12.3.2 Maintenance of Procedures

This section summarizes provisions for documenting and controlling procedures and providing the necessary training and coordination before the introduction of new procedures, or the introduction of changes in the human-machine interface covered by procedures.

Document control in this instance refers to the program that maintains the latest revision of the procedures; captures and corrects errors; changes training when procedures change; and, in general, maintains congruence between the facility's actual condition, the procedures, and the training for the procedures.

12.4 TRAINING PROGRAM

This section summarizes the facility training program, including brief statements addressing the safety management policies and philosophies used as a basis for the program. Reference facility documents detailing the program.

12.4.1 Development of Training

This section summarizes the processes by which the technical content of training programs is developed, verified, and validated. This summary includes training methods and qualification requirements for:

- Conduct of normal, abnormal, and emergency operations.
- Onshift and classroom training.
- Criticality training.
- Radiation and hazardous material protection training.
- Surveillance testing and maintenance training.
- Fire protection training.
- Quality assurance training.
- Emergency preparedness training.

12.4.2 Maintenance of Training

This section summarizes the provisions that ensure training programs reflect actual plant conditions and current procedures, and that necessary coordination is done before introducing new training programs or introducing changes in procedures covered by training programs.

Include in this section a description of the maintenance of training records or a reference to the plant procedure for maintaining such records.

12.4.3 Modification of Training Materials

This section summarizes the process by which technical or human factors deficiencies in training programs are identified and corrected.

Chapter 13
Human Factors

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the human factors process. It is intended to describe the essential characteristics of the process as it relates to facility safety.

This chapter focuses on human factors engineering, its importance to facility safety, and the design of the facility to optimize human performance. Human factors consists of:

- Human factors engineering that focuses on designing facilities, systems, equipment, and tools so they are sensitive to the capabilities, limitations, and needs of humans.
- Human reliability analysis that quantifies the contribution of human error to the facility risk.

This chapter focuses exclusively on human factors engineering. Use of the term human factors in this Standard does not connote an expectation of or requirement for human reliability analysis.

This chapter demonstrates that human factors are considered in facility operations where humans are relied upon for preventive actions (e.g., surveillance and maintenance activities during normal operations), and for operator mitigative actions during abnormal and emergency operations. In this respect, the human-machine interface is an integral part of facility safety and, thus, requires special treatment in the DSA. The emphasis is on human-machine interfaces required for ensuring the safety function of safety SSCs that are important to safety and on the provisions made for optimizing the design of those human-machine interfaces to enhance reliable human performance.

A complete discussion of human factors without application of the graded approach includes:

- Description of the human-factors process for systematically inquiring into the importance of human factors in facility safety.
- Description of human-machine interfaces with safety-significant SSCs and safety-class SSCs that are important to safety.
- Description of the systematic inquiry into the optimization human-machine interfaces with safety-significant SSCs and safety-class SSCs to enhance human performance.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. Discussion is limited to those areas in which human performance plays an important role in ensuring the performance of safety SSCs. The preparer of the DSA will present information at a level that is considered sufficient for the review and approval of the DSA.

Hazard Category 2 facilities may have human-machine interfaces with safety-class SSCs and safety-significant SSCs. Hazard Category 3 facilities do not have safety-class SSCs but may have human-machine interfaces with safety-significant SSCs. Discussions pertain only to the human-machine interfaces with safety SSCs and in proportion to the importance of those human-machine interfaces to the performance of those safety SSCs. To meet the human factors safety requirements of 10 CFR 830, a systematic inquiry of human factors must be presented. An inexpensive yet effective method for accomplishing this is through application of basic human factors checklists. Such checklists typically examine preparation, validation, and use of written procedures; qualification and training of operating crews; staffing; design of the human-machine interfaces; and allocation of control functions to workers versus automatic devices. Although application of a checklist is not a requirement, implementation of such a checklist will satisfy the documentation requirements associated with systematic inquiry into human factors. Discussions can be brief and are limited to summaries of the major features of the systematic inquiry.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 13

13.1 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.

13.2 REQUIREMENTS

This section lists 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 for 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.

13.3 HUMAN FACTORS PROCESS

This section summarizes the human factors process for systematically evaluating the importance of human factors in facility safety. This summary includes the process features to provide assurance that the importance of human-machine interfaces is considered in facility safety.

13.4 IDENTIFICATION OF HUMAN-MACHINE INTERFACES

This section summarizes the safety SSCs requiring human-machine interfaces to function, and the required human-machine interface. These are identified in conjunction with the results of the hazard analysis and accident analysis in Chapter 3 that identifies safety SSCs. Include human-machine interfaces necessary for the surveillance and maintenance of safety SSCs during normal operations, and the human-machine interfaces required for ensuring safety function during normal, abnormal, and emergency operations. Describe the actions identified so that the reviewer can understand what the humans are expected to do (i.e., close isolation valves) and the importance to facility safety of their action (e.g., ensures confinement, actuates a protective response system, etc.).

13.5 OPTIMIZATION OF HUMAN-MACHINE INTERFACES

This section summarizes a systematic inquiry into the optimization of human machine interfaces with safety SSCs to enhance human performance. Checklists serve to document the systematic inquiry. Discussions will be proportionate to the importance to safety and may consider the following design elements:

- Furnished instrumentation, provisions for communication and operational aids to support timely, reliable performance for safety functions.
- Layout and design of controls and instrumentation, and provision for labeling that apply the principles of ergonomics and human engineering.
- Work environments, including physical access, need for protective clothing or breathing apparatus, noise levels, temperature, humidity, distractions, and other factors bearing upon physical comfort, alertness, fitness, etc.
- Staffing considerations (e.g., minimum staffing levels, allocation of control functions, overtime restrictions, facility status turnover between shifts, procedures, training, etc.).

As necessary, reference documentation existing elsewhere in the DSA (i.e., Chapter 12, “Procedures and Training”).

Chapter 14
Quality Assurance

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the quality assurance program to ensure compliance with 10 CFR 830 Subpart A, "Quality Assurance Requirements". It is intended to describe the essential characteristics of the program as it relates to facility safety.

This chapter describes the provisions for a quality assurance program. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of quality assurance program and organization.
- Description of document control and records management.
- Description of the quality assurance process ensuring that performed safety related work meets requirements.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The level of quality control and assurance required is directly related to the magnitude of hazards and incorporates considerations of stage and complexity of the facility or activity. A higher hazard facility with complex systems requires a more formalized quality assurance program. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 14

14.1 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.

14.2 REQUIREMENTS

This section lists 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 for 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.

14.3 QUALITY ASSURANCE PROGRAM AND ORGANIZATION

This section summarizes the program, including the safety management policies and philosophies used as a basis for the program. Reference facility documents detailing the program.

Identify the organizational structure of the quality assurance program including staffing levels and qualifications, positions of authority and responsibilities, and interfaces with other safety organizations and facility operations. The organizational summary may be provided in this chapter or Chapter 17, "Management, Organization, and Institutional Safety Provisions."

14.4 QUALITY IMPROVEMENT

This section briefly describes management's programs and processes used to correct adverse conditions affecting quality. Specifically include identification of control and disposal of nonconforming materials, parts, and components.

14.5 DOCUMENTS AND RECORDS

This section briefly describes the document control and records management program associated with quality assurance.

14.6 QUALITY ASSURANCE PERFORMANCE

This section presents an overview of process to ensure that the performed work meets requirements.

14.6.1 Work Processes

Briefly describe management's programs that ensure performance of tasks under controlled conditions, with applicable calibrated instrumentation, and in accordance with established technical standards administrative controls.

14.6.2 Design

This section briefly describes how quality assurance is integrated into design activities.

14.6.3 Procurement

This section briefly describes how quality assurance is integrated into the procurement process. Describe also how prospective suppliers are evaluated, selected, and their acceptability monitored.

14.6.4 Inspection and Testing for Acceptance

This section briefly describes how quality assurance is integrated into inspection and testing of programs.

14.6.5 Independent Assessment

This section briefly describes how internal independent assessments and external verifications and audits of the quality assurance program are performed.

Chapter 15
Emergency Preparedness Program

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830. This chapter is not intended to be the vehicle for review and approval of the emergency preparedness program. It is intended to describe the essential characteristics of the program as it relates to facility safety.

This chapter summarizes the emergency preparedness functions and response at the facility. Expected products of this chapter, as applicable based on the graded approach, include:

- Identification of the scope of the facility Emergency Preparedness Plan (EPP) (i.e., spectrum of emergencies encompassed).
- Description of the philosophy, objectives, organization, and emergency response of facility emergency preparedness.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The level of detail required by this chapter depends on the quantities, the physical and chemical state, and the potential for release of the hazardous materials involved. However, it is expected that Hazard Category 3 facilities will not require extensive emergency response unless they present a significant hazard from a chemical release or where emergency action might be necessary due to significant localized consequences.

Hazard Category 2 facilities may have impacts beyond the immediate facility and, therefore, a more detailed summary of the EPP would be appropriate. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 15

15.1 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.

15.2 REQUIREMENTS

This section lists 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 for 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.

15.3 SCOPE OF EMERGENCY PREPAREDNESS

This section summarizes the spectrum of emergencies that the EPP is designed to encompass. Focus discussions on demonstrating that emergency preparedness planning adequately encompasses the facility hazards discerned in the hazard analysis. Use of bounding categories of emergencies (i.e., fire, spills, criticality) and bounding consequences from emergencies should be sufficient for documenting the scope of emergency preparedness.

15.4 EMERGENCY PREPAREDNESS PLANNING

This section summarizes facility emergency preparedness planning. The summary should include activation of emergency organizations, assessment actions, notification processes, emergency facilities and equipment, protective actions, training and exercises, and recovery actions.

15.4.1 Emergency Response Organization

This section summarizes the emergency response organization that is activated in case of onsite and offsite operational emergencies. Delineate authorities and responsibilities of key individuals and groups, and identify the communication chain for notifying, alerting, and mobilizing the necessary personnel. Identify the position of the person with the overall responsibility for directing emergency responses. This summary may be provided in this chapter or Chapter 17, “Management, Organization, and Institutional Safety Provisions.”

Describe interrelationships with federal, state, tribal, and local organizations for offsite emergency response and for the protection of the environment and the public. Briefly summarize and reference any prearranged plans, agreements, understandings, and/or other arrangements for mutual assistance

by non-DOE entities.

15.4.2 Assessment Actions

This section summarizes the processes by which the onset of an operational emergency is recognized. The methodology used to obtain meteorological information and estimate release rates and source terms needs to be identified. If computer models are used for consequence assessment, identify the specific models used and the plume methodologies employed (e.g., Gaussian plume).

15.4.3 Notification

This section summarizes the provisions for prompt initial notification of emergency response personnel and response organizations, including appropriate DOE elements and other federal, state, tribal, and local organizations. Summarize the follow-up notification processes, and how emergency public information is integrated into the emergency management program.

15.4.4 Emergency Facilities and Equipment

This section summarizes pertinent aspects of emergency facilities (i.e., location, function) and equipment (i.e., communication capabilities, hazardous material detection instrument ranges and types, dosimetry) required to support the facility emergency responses.

15.4.5 Protective Actions

This section summarizes the protective actions that are required to minimize the exposure of workers and the public. Discussions should include provisions made for medical support and decontamination. Important elements of population evacuations should be summarized including evacuation times, routes, methods of alerting.

15.4.6 Training and Exercises

This section summarizes the emergency training program, including initial and annual retraining for all facility emergency response personnel. Include a summary of the drills and exercises that are an integral part of the emergency management program. The summary should address the range of different populations exposed to facility hazards (e.g., public, general facility population, and facility visitors). Reference, as appropriate, Chapter 12, "Procedures and Training" if that chapter presents requested information.

15.4.7 Recovery and Reentry

This section summarizes the provisions for the recovery from an operational emergency and planned reentry provisions for the affected facility. Indicate the recovery organization and how the facility will transition from the emergency response organization to the recovery organization.

Chapter 16
Provisions for Decontamination and Decommissioning

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830 to define the characteristics of the provisions for decontamination and decommissioning necessary to ensure safe operation of the facility.

This chapter describes provisions that facilitate future D&D of a facility. Design of significant modifications to an existing facility must consider provisions for D&D. This chapter also contains guidance on the description of the conceptual D&D plan for existing facilities. Expected products of this chapter, as applicable based on the graded approach and project mission phase, include:

- Description of design features incorporated in major modifications of an existing facility to facilitate future D&D of the facility.
- Description of operational considerations to facilitate future D&D.
- Description of conceptual D&D plan.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The need for D&D provisions are dependent on the magnitude of the hazards and the complexity of the facility. For facilities whose mission is D&D, which includes deactivation, a DSA that addresses the safety aspects of the decontamination and decommissioning activities must be prepared. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 16

16.1 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.

16.2 REQUIREMENTS

This section lists 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 for 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.

16.3 DESCRIPTION OF CONCEPTUAL PLANS

This section summarizes conceptual plans for D&D. This summary documents that planning of operations and design or modifications minimizes the potential for spread of contamination that would complicate or reduce effectiveness of future D&D or environmental restoration activities. Assessment of future D&D activities must be based on an evaluation of the type and magnitude of hazards and the complexity of processes. The evaluation considers the vulnerabilities to normal and abnormal events and operational plans to minimize contamination and prevent an increase in residual risk during or after decommissioning in a manner similar to the hazard analysis described in Section 3.3, “Hazard Analysis.” The evaluation, however, is conceptual in nature and does not require the extent of documentation required of a DSA hazard analysis.

The description of design features to facilitate D&D operations is limited to major modifications of existing facilities.

Chapter 17
Management, Organization, and Institutional Safety Provisions

PURPOSE. The purpose of this DSA chapter is to provide information that will satisfy the requirements of 10 CFR 830 to define the management, organization and institutional safety provision necessary to ensure safe operation of the facility.

This chapter presents information on management, technical, and other organizations that support safe operation. This chapter also enumerates the requirements used to develop the safety management programs, includes descriptions of the responsibilities of and relationships between the non-operating organizations having a safety function and their interfaces with the line operating organization, and presents sufficient information on the safety management policies and programs to demonstrate that the facility operations are embedded in a safety conscious environment. Expected products of this chapter, as applicable based on the graded approach, include:

- Description of the overall structure of the organizations and personnel with responsibilities for facility safety and interfaces between those organizations.
- Description of the programs that promote safety consciousness and morale including safety culture, performance assessment, configuration and document control, occurrence reporting, and staffing and qualification.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

APPLICATION OF THE GRADED APPROACH. The level of detail required by this chapter is dependent upon magnitude of hazard and overall facility complexity. Discussions can be brief and are limited to summaries of the major features of the programmatic commitment to the safety basis.

CONTENT GUIDANCE FOR SECTIONS OF CHAPTER 17

17.1 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.

17.2 REQUIREMENTS

This section lists 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 for 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.

17.3 ORGANIZATIONAL STRUCTURE, RESPONSIBILITIES, AND INTERFACES

This section summarizes the overall structure of the organizations. Include in the summary the separate and distinct entities that are organized into a safety conscious and responsive organization to ensure and enhance the facility safety.

17.3.1 Organizational Structure

This section summarizes the organization, including the interfaces with respect to the management of the facility beyond the operating organization.

17.3.2 Organizational Responsibilities

This section summarizes the organization's responsibilities and authorities; its interfaces with other organizations described in this chapter or other chapters of the DSA, including the line operating organization; and the general safety programs and issues for which it is responsible. Also discuss:

- Technical and engineering support, maintenance, and modifications.
- Safety issue discovery, communication, management, and resolution.
- Independent safety review, audit, and compliance determination.
- Safety analysis services, including USQ evaluation.
- Support services such as utilities and other offsite support.

17.3.3 Staffing and Qualifications

This section summarizes the bases for the staffing levels and the knowledge, skills, and abilities of facility personnel in organizations covered in this

chapter. Describe the programs and provisions for monitoring safety performance of the staff.

17.4 SAFETY MANAGEMENT POLICIES AND PROGRAMS

This section identifies and describes programs to enhance facility safety.

17.4.1 Safety Review and Performance Assessment

This section summarizes the programs and procedures used to ensure independent oversight, safety review, USQ determination, and appraisal of the safety performance of all of the organizations involved in the management of safety, such as industrial safety, fire inspections, and hazardous material control.

17.4.2 Configuration and Document Control

This section summarizes programs for controlling modifications to the facility or to its operation. Describe the programs for control of all documentation serving a safety related function, such as as-built facility drawings, operating procedures, training manuals, etc.

17.4.3 Occurrence Reporting

This section summarizes provisions for investigating abnormal events and reporting procedures to DOE; selection and analysis of information for occurrence reports; the evaluation of operational experience and trends; and for the development of feedback, corrective action, and communicating lessons learned.

17.4.4 Safety Culture

This section summarizes the policies and programs used to: promote an interest in and involvement of all associated workers in facility safety; facilitate a questioning attitude toward safety related activities and equipment; and ensure that workers understand the potential risks to the facility and fellow workers as well the rewards and sanctions associated with personal safety performance.

Appendix A

Evaluation Guideline

Appendix A
Evaluation Guideline

A.1 INTRODUCTION

In accordance with the definition of Evaluation Guideline (EG) provided by this standard, this appendix specifies a numerical radiological dose value to be used in identifying safety-class (SC) Systems, Structures, and Components (SSC). Calculation methods and assumptions needed to provide general consistency in dose estimation are also described, with relevant background and interpretation discussions included as appropriate.

The methodology provided by this standard focuses on characterizing facility safety with or without well-documented design information. The EG construct as described in this appendix is primarily intended for use with existing facilities. Discussions relevant to new facilities are provided in the Implementation Guide for Section 4.1 (Nuclear and Explosive Safety Design Criteria) of DOE Order 420.1, "Facility Safety."

A.2 EVALUATION GUIDELINE

The EG is 25 rem total effective dose equivalent (TEDE). The dose estimates to be compared to it are those received by a hypothetical maximally-exposed offsite individual (MOI) at the site boundary for an exposure duration of 2 hours. The nominal exposure duration of 2 hours may be extended to 8 hours for those release scenarios that are especially slow to develop. Dose calculations for comparison against the EG are based on the concept of an unmitigated release to determine whether the potential level of hazard in the specific facility warrants SC SSC designation (see Section A.3.1 for details).

The value of 25 rem TEDE is not to be used as a 'hard' pass/fail level. Unmitigated releases should be compared against the EG to determine whether they challenge the EG, rather than exceed it. This is because consequence calculations are highly assumption driven and uncertain.

It should be made clear that the EG is not to be treated as a design acceptance criterion, nor as justification for nullifying the general design criteria relative to defense-in-depth safety measures. The value of 25 rem TEDE is not considered an acceptable public exposure either. It is, however, generally accepted as a value indicative of no significant health effects (i.e., low risk of latent health effects and virtually no risk of prompt health effects).

There is no predetermined frequency cutoff value, such as 1 E-6 per year, for excluding low frequency operational accidents (i.e., internally initiated). In fact, for operational accidents there is no explicit need for a frequency component to the unmitigated release calculations, since the determination of need is solely driven by the bounding consequence potential. Per the body of this Standard, natural events are defined in terms of the frequency of the initiating event, while external events (i.e., externally initiated man-made events) are defined with a cutoff frequency of 10^{-6} per year, conservatively calculated, or

10^{-7} per year, realistically calculated.

Unmitigated release is meant to consider material quantity, form, location, dispersability, and interaction with available energy sources, but not to consider safety features (e.g., ventilation systems, fire suppression, etc.) which would prevent or mitigate a release. Final dose estimations representing the anticipated behavior of the facility under accident conditions should be based on the mitigated design basis accidents (DBAs), wherein full or partial functionality of SC SSCs is assumed. In cases where the designated SC SSC are not capable of performing their required safety function without significant upgrade (i.e., backfit) other compensatory measures such as material-at-risk (MAR) limits may be implemented in the facility and incorporated into the DSA.

Comparison of the unmitigated consequences for a limited subset of potential accidents to the EG is performed to determine if the need for designation of SC SSCs exists. If the EG value is approached by the unmitigated consequences of a release scenario, a need for SC SSC designation is indicated. SC SSCs are only one of many layers of hardware- and administrative-based controls that are incorporated into a DOE operation for the protection of the public, worker, and environment consistent with the precepts of the defense-in-depth philosophy. The SC designation merely helps to focus a higher level of attention and requirements on this select subset of all controls intended for the protection of the public.

If the need for SC designation is determined, all preventive and mitigative features associated with the sequence of failures that result in a given release scenario, as well as any features whose functionality is assumed as part of the scenario definition itself are candidates for SC SSC designation. The process of designating one or more safety SSCs as SC is judgment-based and depends on many factors such as effectiveness, a general preference of preventive over mitigative and passive over active, relative reliability, and cost considerations.

A.3 DOSE COMPARISON CALCULATIONS

General discussion is provided for source term calculation and dose estimation, as well as prescriptive guidance for the latter. The intent is that calculations be based on reasonably conservative estimates of the various input parameters.

The dose estimate is that received during a 2-hour (with the exception mentioned earlier) exposure to plume, as discussed in section A.3.3, considering inhalation, direct shine, and ground shine. Other slow developing release pathways, such as ingestion of contaminated food, water supply contamination, or resuspension are not included. However, quick release accidents involving other pathways, such as a major tank rupture, which 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 Licenses," 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, but accident releases usually would be expected to develop more slowly than airborne releases. More

time would also be available for implementing preventive and mitigative measures. Therefore, the emphasis on SC SSCs in terms of immediate availability and operation is not generally necessary for safety SSCs associated with these pathways.

A.3.1 Scenario Definition

The concept of a DBA has historically been applied in the nuclear industry for deterministic evaluation of potentially high consequence accidents (primarily for nuclear power plants). The DBA analyses encompass evaluations of the need for and the adequacy of those important SSCs whose failure could have an adverse impact on the public (i.e., SC SSCs). For may DOE facilities, due largely to their age and the absence of safety documentation, the original design bases for their SSCs, including safety-related features, are severely lacking or nonexistent. In recognition of this deficiency, the standard requires the development and analysis of derivative DBAs (which for simplicity were also referred to as DBAs in the body of the standard) for the existing facilities in lieu of actual DBAs. The primary purpose of the DBA analysis is to identify SSCs that warrant SC designation. In doing so, the concept of "unmitigated release" was developed to conservatively estimate the consequence potential from the candidate DBAs that are selected from the hazard analysis without taking credit for any safety features. Note that the standard already requires that unmitigated consequences be estimated as part of a hazard analysis, though largely in a qualitative manner. Thus, the unmitigated release calculation is a critical step in the DBA formulation process that estimates the potential magnitude of the radiological release. The result of the calculation is compared to the EG to (1) determine if any SC SSC is required and (2) provide insight for selecting the appropriate SC SSC(s) for each DBA scenario.

For existing DOE non-reactor nuclear facilities, some safety systems may already be known and designated as such (e.g., fire protection systems and confinement systems, which include HEPA filtration). Some SC designations for such safety system may also be self-evident. Nevertheless, it is necessary to provide the basis for such designation, and this Appendix provides the guidance for the analysis and documentation required. In some cases it has been found that these analyses provide useful insight into subtle safety issues.

UNMITIGATED RELEASE CALCULATION. The unmitigated release calculation represents a theoretical limit to scenario consequences assuming that all safety features have failed, so that the physical release potential of a given process or operation is conservatively estimated. The unmitigated release should characterize both the energies driving the release, and the release fractions in accordance with the physical realities of the accident phenomena at a given facility or process. As a result, there may be assumptions that are necessary to make in order to define a meaningful scenario, but which also impact the magnitude of the resultant consequences. In order to clearly capture these assumptions, and their resulting potential impact on safety SSC designation and/or Technical Safety Requirements (TSR) protection, the unmitigated calculation should:

(1) Take no credit for active safety features – such as ventilation filtration

systems in the case of a spill.

(2) Take credit for passive safety features that are assessed to survive accident conditions where that capability is necessary in order to define a physically meaningful scenario. For example, in the case of a container drop where the impact of the drop does not challenge container integrity, it should not be assumed that the contents have dropped in an uncontained manner. Similarly, if the presence of permanently installed resilient flooring prevents an undesired consequence given 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 may warrant some level of safety SSC designation to assure that the assumptions remain valid in the future. In the above examples, the container and the flooring may warrant designation as SS or SC design features.

(3) Take no credit for passive safety features producing a leakpath reduction in source term, such as building filtration.

(4) Assume the availability of passive safety features 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 not affected by the accident are not ruptured or otherwise unavailable.

Defined as above, the unmitigated release calculation determines the need for SC SSC designation, and provides the framework against which SC SSC designation is made.

DESIGN BASIS ACCIDENT CALCULATION. Once a set of SC SSCs has been identified, accident consequences can be estimated in a DBA calculation, which represents the accident scenario progression where SC SSCs successfully perform their intended safety function.

For each scenario in the DSA, sufficient documentation of both the unmitigated and mitigated accident scenarios (DBAs) should be made such that the thought process of determining the SC SSCs is well understood. In all cases, the level of protection provided by the identified SC SSCs should be evident. However, this does not require explicit reporting of unmitigated consequences in the DSA, if it is evident that the unmitigated release consequences are large, i.e., well above the EG.

A.3.2 Source Term Calculation

The radioactive airborne source term is typically estimated as the product of five factors: (1) MAR, (2) damage ratio, (3) airborne release fraction, (4) respirable fraction, and (5) leakpath factor. Detailed discussion of these parameters is provided in DOE-HDBK-3010, "Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities."

MATERIAL-AT-RISK (MAR). The MAR values used in hazard and accident analysis must be consistent with the values noted in hazard

identification as described in section 3.3.2.1 of this standard, and should represent documented maxima for a given process or activity. Such documentation may be present in TSRs or lower-tier documents referenced in TSRs, as necessary. While DOESTD-1027 excludes material in qualified containers from consideration for the purposes of hazard classification, the existence of such material should be acknowledged in a DSA. Such material should later be excluded from the source term for the applicable accident scenarios if the containers can be shown to perform their functions under the accident environments. Exclusion of MAR from the source term may be based on qualified containers (which may then be designated as SC design features), consideration regarding the specifics of the accident scenario through the definition of the damage ratio (defined below), or other appropriate means.

DAMAGE RATIO (DR). The DR is that fraction of material actually impacted by the accident generating conditions. DOE-HDBK-3010 notes that some degree of ambiguity can result from overlapping definitions of MAR and DR in various applications. One consistent definition should be used throughout a given DSA.

AIRBORNE RELEASE FRACTIONS (ARFs) AND RESPIRABLE FRACTIONS (RFs). Bounding estimates for radionuclide ARFs and RFs for a wide variety of MAR and release phenomena are systematically presented in DOE-HDBK-3010. In those cases where there may be significant direct shine contribution to dose, that contribution should be evaluated without the use of the respirable fraction.

LEAKPATH FACTOR (LPF). The LPF is the fraction of material passing through some confinement deposition or filtration mechanism. Several LPFs may be associated with a specific accident, e.g., fraction passing from a glovebox, fraction passing from a room, fraction passing through filtration vis-à-vis door leakage. For the purposes of the unmitigated release calculation, the LPF should be set to unity.

A.3.3 Dose Estimation

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

DOSE CALCULATION LOCATION. For the purposes of comparison to the EG, the comparison point is take to be the location of a theoretical MOI standing at the site boundary. This location can also be beyond the DOE site boundary if a buoyant or elevated plume is not at ground level at the DOE site boundary. In such cases, the calculation location is taken at the point of maximum exposure, typically where the plume reaches the ground level. It is DOE practice and expectation that onsite individuals, both workers and public, are protected under the Emergency Response plans and capabilities of its sites. This protection, along with implementation of defense-in-depth and worker safety philosophy, Safety Significant (SS) (and indirectly, through SC) SSC

designation, and DOE's safety management programs, address onsite safety. However, an annual assessment of any changes in the site boundary and potential effects on safety SSC classification should be performed in association with the required annual update of the DSA for a facility. Privatization and site turnover initiatives may affect these determinations.

ATMOSPHERIC DISPERSION. The 95th percentile of the distribution of doses to the MOI, accounting for variations in distance to the site boundary as a function of direction, is the comparison point for assessment against the EG. The method used should be consistent with the statistical treatment of calculated X/Q values described in regulatory position 3 of NRC Regulatory Guide 1.145 for the evaluation of consequences along the exclusion area boundary. The determination of distance to the site boundary should be made in accordance with the procedure outline in position 1.2 of Regulatory Guide 1.145. NRC Regulatory Guide 1.23 describes acceptable means of generating the meteorological data upon which dispersion is based. Accident phenomenology may be modeled assuming straight-line Gaussian dispersion characteristics, applying meteorological data representing a 1-hour average for the duration of the accident. Accident duration is defined in terms of plume passage at the location of dose calculation, for a period not to exceed 8 hours. Prolonged effects, such as resuspension, need not be modeled. The accident progression should not be defined so that the MOI is not substantially exposed (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 time and windspeed so that the plume has not reached the MOI). The exposure period begins from the time the plume reaches the MOI.

For ground releases, the calculated dose equates to the centerline dose at the site boundary. For elevated, thermally buoyant, or jet releases, plume touchdown may occur beyond the site boundary. As noted in the discussion of receptor location, these cases should locate the dose calculation at the point of maximum dose beyond the site boundary, which is typically at the point of plume touchdown.

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

A.4 FUNCTIONAL CLASSIFICATION PROCESS

The use of the EG is only one element in a larger safety SSC functional classification process that is intended to contribute to adequate safety. Other contributors are disciplined conduct of operations, training, and safety management programs such as radiation protection and emergency response. The functional classification process must recognize competing interests for finite resources, and the need for optimization of the application of resources for safety in a facility, as well as across a DOE site. Some principles that should be incorporated in a functional classification process are:

- Protection of the public is contributed to by all facets of safety in design, including defense-in-depth, SC and SS SSCs, and in many cases in DOE, by remote siting. The expectation is that SSCs will function as designed in accident environments, resulting in public doses of small fractions of the EG.
- Protection of the public is paramount in safety design, but protection of workers is no less important. However, the degree of protection for facility workers achievable by safety SSCs is limited. Major contributions to overall safety assurance to the worker are institutional factors such as conduct of operations, training, and the entirety of safety management programs.
- Some considerations in the prioritization of facility safety issues include:
  - Hazardous material inventory should be minimized at all times.
  - Safety SSCs are preferred over administrative controls.
  - Passive SSCs are preferred over active SSCs.
  - Preventive controls are preferred over mitigative controls.
  - Controls closest to the hazard may provide protection to both workers and the public.
  - Facility safety SSCs are preferred over personal protective equipment.
  - Controls that are effective for multiple hazards can be resource effective.

A.5 ADDITIONAL CONSIDERATIONS

Selection of the terminology “Evaluation Guideline” is deliberate. It distinguishes this usage from ‘safety or risk acceptance criteria’ or ‘siting criteria.’ Such acceptance criteria have traditionally been used in the design and siting stage of nuclear power reactors.

Acceptance criteria have been inextricably linked to accident scenarios that are prescribed in some manner, i.e., deterministic DBAs. The results of quantitative probabilistic risk assessments (PRA), principally those of nuclear power or production facilities, are sometimes compared to another type of ‘risk acceptance criteria,’ referred to as safety goals. PRAs are fundamentally different analytical methods from deterministic safety analyses and produce a different type of product. For example, in PRAs the failure of a safety feature (hardware or human action) to perform an intended function is always postulated, irrespective of the safety classification of the feature. So, in contrast to assumptions employed in deterministic safety analyses, in PRAs even SC SSCs do not get

treated differently from typical industrial grade SSCs in release scenario characterization, with the exception of their estimated failure probabilities.

A conceptually different approach is needed for safety analysis of existing facilities, where an analysis of the safety of the 'facility as is' is performed. The primary objective of the analytical process must then turn to the identification of needed controls and their potential inadequacies, and the corresponding corrective or compensatory measures. Furthermore, for existing DOE facilities, DBAs are typically either non-existent or irrelevant, due to a variety of reasons, such as changes in the original mission or early design philosophies. Thus, this standard adopted the notion of derivative DBAs that for simplicity of notation were summarized as DBA in the text. But these DBAs are not, in general, the actual accident scenarios that formed some aspects of the basis for the facility design. For these existing facilities, safety assurance is provided through an aggressive approach based on a comprehensive analysis of all hazards leading to the release of radiological or toxicological material, and ensuring that the controls identified against each hazard are relevant, specific, and effective.

It is emphasized again that the value of 25 rem TEDE is not to be used as a 'hard' pass/fail level. Unmitigated releases should be compared against the EG to determine whether they challenge the EG, rather than exceed it. This is because consequence calculations are highly assumption driven and uncertain. There are uncertainties in initiating event intensity, plant SSC and personnel response, accident phenomenology, DRs, ARFs and RFs, and so on. The point here is that other factors may play a part in the decision, and the EG value guides the decision making process towards a level of uniformity that could not exist without some form of quantitative benchmark.

The EG is not used as any measure of acceptable or adequate safety. Rather, the EG is a tool intended to carry the application of hazard analyses one step further to gradation of hazard-based controls with tangible results on the operating floor. Specifically, Chapter 3 identifies two classifications of safety SSCs, SC and SS. Only two classifications of safety SSCs are used in order to support meaningful distinctions in the requirements imposed on safety SSCs.

It may be argued that in lieu of, or in addition to the EG, DOE should also promote the use of some form of risk acceptance criteria, so risk or safety analysts would know what is safe enough, or when the amount of analysis performed would be sufficient. However, DOE's experience with previous DSAs for existing facilities has shown that use of risk acceptance criteria of any kind has generally resulted in short cutting of the hazard analysis process, and inadequate identification and understanding of needed controls. Additionally good practice dictates that safety improvement should be made whenever practical, regardless of the level of existing safety. In other words, there is no such thing as 'safe enough' in an absolute sense.

The EG value is not release frequency dependent, since as mentioned earlier, the determination of need is solely driven by the bounding consequence potential. In addition, calculation of frequencies and consequences of various release scenarios involve accounting for large uncertainties on both scales. Limiting the EG to one value on the consequence scale alone reduces the impact of uncertainties on SC designation of SSCs with no loss of information on characterization of the needed controls because of

comprehensive hazard analysis. Generally, the availability of typical preventive or mitigative features, such as the ventilation and filtration system, given the occurrence of a DBA in DOE's non-reactor nuclear facilities will reduce potential public doses to well within a small fraction of the EG. Thus, an approach that also uses frequency of release, even if equally practical, would not generally result in different SSC classifications. Moreover, requiring frequency-based calculations would result in enlarging the paper process, thus undermining DOE's emphasis on comprehensive hazard analysis, without significant payback in safety assurance on the operating floor.

The protection of the public and workers during normal operations is governed by 10 CFR 835, Occupational Radiation Protection; unintended releases of sufficiently high frequency as considered a part of normal operations would also be governed by this regulation. This is not to imply, however, that safety SSCs should be identified based on compliance with 10 CFR 835. It is inherent in the hazard analysis process described in this standard that a comprehensive spectrum of accidents, including those that may have a higher likelihood, be identified, evaluated, and analyzed. Any accidents that have a significant consequence potential to the public or workers, independent of likelihood, must be thoroughly evaluated, including the identification of any appropriate safety SSCs or administrative controls.

Toxicological EGs are not specified. There is no industrial or regulatory precedent for SC designation of SSCs in facilities or processes with only toxicological hazards. SS designations, which are based on qualitative guidelines, can be triggered without distinction from both radiological and toxicological hazards. However, controls for toxicological releases, which trigger nuclear accidents or have nuclear impacts, are potential candidates for SC designation.

CONCLUDING MATERIAL

Review Activities:

DOE	Field Offices
DP	AL
EH	CH
EM	ID
ER	NV
FM	OR
LM	RFO
NE	RL
NS	SR
PR	SF
SA	Fernald

National Laboratories
ANL
BNL
INEL
LANL
LLNL
PNL
Sandia

Area Offices
Amarillo
Argonne
Brookhaven
Dayton
Golden
Kirkland
Los Alamos
Rocky Flats
Pinellas
Princeton

Preparing Activity:
DOE EH-22

Project Number:
SAFT-0105