TS

NOT MEASUREMENT SENSITIVE

DOE-STD-1189-2008
March 2008

DOE STANDARD

INTEGRATION OF SAFETY INTO THE DESIGN PROCESS

U.S. Department of Energy
Washington, DC 20585

AREA SAFT

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

This document is available on the Department of Energy
Technical Standards Program Web Page at
http://www.hss.energy.gov/nuclearsafety/techstds/

PREFACE

The U.S. Department of Energy (DOE) has approved this Standard for use by DOE and its contractors.

In a memorandum to DOE elements, dated December 5, 2005, on integration of Safety-in-Design, the Deputy Secretary of Energy stated, "I expect safety to be fully integrated into design early in the project. Specifically, by the start of the preliminary design, I expect a hazard analysis of alternatives to be complete and the safety requirements for the design to be established. I expect both the project management and safety directives to lead projects on the right path so that safety issues are identified and addressed adequately early in the project design."

DOE Standard 1189 has been developed to show how project management, engineering design, and safety analyses can interact to successfully implement the Deputy Secretary's expectations. These interactions are a fundamental element necessary in the integration of safety throughout the DOE Acquisition Management System. They are key to the timely identification, evaluation, and adjudication of Safety-in-Design issues early in project life.

This Standard provides the Department's expectations for incorporating safety into the design process for new or major modifications to DOE Hazard Category 1, 2, and 3 nuclear facilities, the intended purpose of which involves the handling of hazardous materials, both radiological and chemical, in a way that provides adequate protection for the public, workers, and the environment. The Standard describes the Safety-in-Design philosophies to be used with the project management requirements of DOE Order (O) 413.3A, Change (Chg) 1, *Program and Project Management for the Acquisition of Capital Assets*, and incorporates the facility safety criteria in DOE O 420.1B, *Facility Safety*, as a key foundation for Safety-in-Design determinations.

The requirements provided in the above DOE Orders and the expectations in this Standard provide for identification of hazards early in the project and the use of an integrated team approach to design safety into the facility. The basic Safety-in-Design precepts are as follows:

- appropriate and reasonably conservative safety structures, systems, and components are selected early in project designs;
- project cost estimates include these structures, systems, and components; and
- project risks associated with safety structures, systems, and components selections are specified for informed risk decision-making by the Project Approval Authorities.

The provisions of this Standard, when implemented in conjunction with DOE O 413.3A, Chg 1, and its guidance documents, are consistent with the core functions and guiding principles of Integrated Safety Management (ISM), as described in DOE P 450.4, *Integrated Safety Management Policy*.

The Standard provides guidance on a process of integration of Safety-in-Design intended to implement the applicable ISM core functions—define the work, analyze the hazards, establish the controls—necessary to provide protection of the public, workers, and the environment from harmful effects of radiation and other such toxic and hazardous aspects attendant to the work. Important ISM guiding principles involved in this process and addressed in this Standard are identification of safety standards and requirements and development of hazard controls tailored to the work to be performed. The process includes documentation and timely review of safety design evolution to ensure feedback and improvement, leading to design and construction that can lead to operations authorization.

The Standard does not instruct designers how to design nor instruct safety personnel how to perform safety analyses. Rather, the Standard provides guidance on how these two disciplines and project management can interface and work together to incorporate safety into design.

A project is expected to evolve over time, and the project safety design basis is also expected to evolve. The expectation is that within this evolution process, unanticipated issues will be minimized.

Some of the key concepts that are included in the Standard are the following.

1. The importance of the Integrated Project Teams (IPT), federal and contractor, including a contractor Safety Design Integration Team (SDIT), and effective coordination among these teams. The SDIT comprises both safety and design subject matter experts and is the heart of the safety and design integration effort.
2. The development of a Safety Design Strategy (SDS) that provides a roadmap for strategizing how important safety issues will be addressed in the design and in the tailoring in the development of key safety documentation. The SDS should be initiated based on a statement of DOE expectations for Safety-in-Design developed during the pre-conceptual stage and should be submitted during the conceptual design stage and updated and refined through the design process.
3. The development, in the conceptual design stage, of facility-level design basis accidents (DBA) that provide the necessary input to the identification and classification of important safety functions. These classifications (i.e., safety class, safety significant, seismic design basis) provide design expectations for safety structures, systems, and components (SSC).
4. The development of objective radiological criteria for safety and design classification of SSCs. These criteria relate to public and collocated worker-safety design considerations.
5. The identification and application of nuclear safety design criteria as provided by DOE O 420.1B and its associated guides.
6. The development of guidance for the preparation of a Conceptual Safety Design Report (CSDR), a Preliminary Safety Design Report (PSDR), and the Preliminary Documented Safety Analysis (PDSA). These reports are required by DOE O 413.3A, Chg 1, for Hazard Category 1, 2, and 3 nuclear facilities, and they must be approved by DOE as part of the project approvals to proceed to the next design or construction phase. The intent of these reports and their approval is to ensure that the directions and decisions made regarding project safety are explicitly identified and dealt with in early stages of design. The objective is to reduce the likelihood of costly late reversals of design decisions involving safety.

7. The definition, as needed, of a Risk and Opportunities Assessment that recognizes the risks of proceeding at early stages of design (especially conceptual design) on the basis of incomplete knowledge or assumptions regarding safety issues and the opportunities that may arise during preliminary and final design to reduce costs through alternative or refined design concepts or better knowledge regarding the uncertainties. This assessment is intended to be input to the Risk Management Plan assessments for a project.

These key elements of the Standard have several intersections and possible overlaps with the guides for the implementation of DOE O 413.3A, Chg 1. These guides should also be consulted for more complete information on the associated activities and documents. In addition, several directives and standards deal with some aspects of Safety-in-Design that are also addressed in this Standard, such as safety system classification and seismic design bases. For new facility design, these directives and standards are supplemented by this Standard. The directives and standards in this category are as follows:

- DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosive Safety Guide* for use with DOE O 420.1 Facility Safety;
- DOE G 420.1-2, *Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Nonnuclear Facilities*;
- DOE G 421-1-2, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*;
- DOE-STD-1020-2002, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*;
- DOE-STD-1021-93, *Natural Phenomena Hazards Performance Categorization Guidelines for Structures, Systems, and Components*; and
- DOE-STD-3009-94, Change Notice (CN) 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis*.

Nuclear safety design basis documents required by DOE O 413.3A, Chg 1 and by Title 10, *Code of Federal Regulations* (CFR) Part 830, *Nuclear Safety Management*, Subpart B, *Safety Basis Requirements*, for new projects and major modifications must be developed consistent with the expectations and guidance in this Standard.

There are a number of DOE Directives and Technical Standards specifically referenced in this Standard. Unless specifically prohibited or limited, successor documents may be used in place of the referenced directive or standard. Successor documents are subsequent revisions to the specified directives and standards issued through the DOE Directives System or DOE Technical Standards Program, as applicable, (for example, DOE O 420.1B would be a successor document to DOE O 420.1A) or the documents that replace them as defined within those programs (for example, a DOE directive may cancel all or part of a directive and replace those provisions with new provisions in a new directive). However, documents issued outside the Directives System and the Technical Standards Program are not considered to be successor documents to these directives and standards. Contracts and regulations may require that specific revisions be applied, particularly for individual projects (for example, 10 CFR Part 830 requires that hazard categorization be performed consistent with DOE-STD-1027-92, Change Notice 1, September

1997). The provisions of 10 CFR Part 830, Appendix A to Subpart B, Table 2, (known as the "safe harbor methodologies" for 10 CFR Part 830) specifically permit use of successor documents for the listed directives and standards.

SAFETY DESIGN GUIDING PRINCIPLES

1. DOE Order 420.1B, *Facility Safety*, is utilized and addressed in design activities, as applicable. Design teams should be able to clearly articulate strategies in the design that address DOE O 420.1B expectations and include them in the design/safety basis information.
2. Control selection strategy to address hazardous material release events is based on the following order of preference at all stages of design development.
    - Minimization of hazardous materials is the first priority.
    - Safety structures, systems, and components (SSCs) are preferred over Administrative Controls.
    - Passive SSCs are preferred over active SSCs.
    - Preventative controls are preferred over mitigative controls.
    - Facility safety SSCs are preferred over personal protective equipment.
    - Controls closest to the hazard may provide protection to the largest population of potential receptors, including workers and the public.
    - Controls that are effective for multiple hazards can be resource-effective.
3. Design codes and standards incorporated into the DOE O 420.1B guides are to be followed, unless specific exceptions are taken to those listed and approved by DOE.
4. The risk and opportunity assessment includes consideration of the Safety-in-Design approaches selected to address project cost contingencies and appropriate mitigation strategies for the risks/opportunities identified for the strategies selected.
5. Early project decisions on a technical approach are conservative in order to establish appropriate cost and schedule baselines for the project.
6. The Critical Decision (CD) packages portray safety-item selections, bases, and risks and opportunities, with proposed mitigation strategies and cost and contingencies, to enable informed risk decision-making by the project approval authorities regarding the project technical basis and cost.
7. The project team includes appropriate expertise and is established early in the project cycle.
8. Safety personnel are used from the onset of project planning to help ensure that appropriate hazards and techniques for hazard management are considered (e.g., material-at-risk [MAR] limitation, prevention techniques, and operationally effective design solutions).
9. Important safety functions, such as facility building confinement, confinement ventilation approach and systems, fire protection strategies and systems, security requirements, life-safety considerations, emergency power systems, and associated seismic design bases are addressed during conceptual design.
10. The safety design team ensures sufficient process definition is available, particularly at the conceptual and preliminary design stages, to enable major safety cost drivers to be included

in the design documentation, along with their associated safety functions and design criteria. The team also identifies the risks and opportunities associated with the selections identified and develops mitigation strategies that are included in the cost-estimate contingencies. Details may not be available in early project stages to identify all hazards and needed hazard controls.

11. All stakeholders are important to the process. Stakeholder issues are identified early and addressed.
12. To ensure that the project/facility configuration can be managed appropriately, the basis for decisions related to safety is clearly documented.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

ABBREVIATIONS AND ACRONYMS

AEGL	Acute Exposure Guideline Level
AHJ	Authority Having Jurisdiction
ALARA	As Low as Reasonably Achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
ARF	Airborne Release Fraction
ARR	Airborne Release Rate
ASME	American Society of Mechanical Engineers
BOD	Basis of Design
BPV	Boiler and Pressure Vessel Code
CD	Critical Decision
CDR	Conceptual Design Report
CFR	Code of Federal Regulation
CHG	Change
CIPT	Contractor Integrated Project Team
CN	Change Notice
COA	Condition of Approval
CSDR	Conceptual Safety Design Report
CSE	Criticality Safety Evaluation
CSP	Criticality Safety Program
CX	Categorical Exclusion
D&D	Decontamination and Decommissioning
DBA	Design Basis Accident
DBT	Design Basis Threat
DCF	Dose Conversion Factor
DID	Defense-in-Depth
DNFSB	Defense Nuclear Facilities Safety Board
DOE	U.S. Department of Energy
DR	Damage Ratio
DSA	Documented Safety Analysis
EEGL	Emergency Exposure Guidance Level

EMP	Emergency Management Program
EPA	U.S. Environmental Protection Agency
EPHA	Emergency Planning Hazard Assessment
ERPG	Emergency Response Planning Guideline
FONSI	Finding of No Significant Impact
FHA	Fire Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FW	Facility Worker
GFE	Government Furnished Equipment
HA	Hazards Analysis
HASP	Health and Safety Plan
HAZOP	Hazard and Operability Analysis
HCN	Health Code Number
HEPA	High Efficiency Particulate Air
HPR	Highly Protected Risk
IPT	Integrated Project Team
ISM	Integrated Safety Management
ITS	Important To Safety
MAR	Material-at-Risk
MC&A	Material Control and Accountability
N/A	Not Applicable
NCS	Nuclear Criticality Safety
NEPA	National Environmental Policy Act
NFPA	National Fire Protection Association
NPH	Natural Phenomena Hazard
O	Order
OECM	Office of Engineering and Construction Management
OMB	Office of Management and Budget
ORR	Operational Readiness Review
OSHA	Occupational Safety and Health Administration

P&ID	Piping and Instrumentation Diagram
PC	Performance Category
PDSA	Preliminary Documented Safety Analysis
PEP	Project Execution Plan
PFD	Process Flow Diagram
PHA	Preliminary Hazards Analysis
PSDR	Preliminary Safety Design Report
QA	Quality Assurance
RF	Respirable Fraction
ROD	Record of Decision
RMP	Risk Management Plan
SAC	Specific Administrative Control
SC	Safety Class
SCAPA	Subcommittee on Consequence Assessment and Protective Actions
SDIT	Safety Design Integration Team
SDC	Seismic Design Criteria
SDS	Safety Design Strategy
SE	System Engineer
SER	Safety Evaluation Report
SME	Subject Matter Expert
SMP	Safety Management Program
SNM	Special Nuclear Material
SPEGL	Short-Term Public Emergency Guidance Level
SRI	Safeguards Requirements Identification
SRID	Standards and Requirements Identification Document
SS	Safety Significant
SSC	Structure, System, and Component
STD	Standard
TEC	Total Estimated Cost
TEDE	Total Effective Dose Equivalent
TEEL	Temporary Emergency Exposure Limit
TPQ	Threshold Planning Quantity
TSR	Technical Safety Requirements

USQ	Unreviewed Safety Question

DEFINITIONS

Conceptual Safety Design Report (CSDR) – A Conceptual Safety Design Report is developed to:

a. document and establish a preliminary inventory of hazardous materials, including radioactive materials and chemicals;
b. document and establish the preliminary hazard categorization of the facility;
c. identify and analyze primary facility hazards and facility Design Basis Accidents;
d. provide an initial determination, based on preliminary hazard analysis, of Safety Class and safety significant structures, systems, and components (SSC);
e. include a preliminary assessment of the appropriate Seismic Design Category for the facility itself, as well as the safety significant structures, systems, and components;
f. evaluate the security hazards that can impact the facility safety basis (if applicable); and
g. include a commitment to the nuclear safety design criteria of DOE O 420.1 (or proposed alternative criteria).

Conceptual Safety Validation Report (CSVR) – The report prepared by DOE that documents the DOE review of the Conceptual Safety Design Report.

Documented Safety Analysis (DSA) – A documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety.

Fire Hazards Analysis (FHA) – A comprehensive assessment of the potential for a fire at any location to ensure that the possibility of injury to people or damage to buildings, equipment, or the environment is within acceptable limits (NFPA 801).

Hazards Analysis (HA) – This analysis supports PDSA development during Preliminary and Final Design and identifies the types and magnitudes of hazards that are anticipated in the facility. This level of hazard analysis expands the PHA to include evaluation of the process hazards.

Integrated Project Team (IPT) – An Integrated Project Team is a cross-functional group of individuals organized for the specific purpose of delivering a project to an external or internal customer. For the purposes of this Standard, this team may be composed of both Federal and contractor (or subcontractor) personnel, and it will support and report to the Federal Project Director. For complex or hazardous projects, a subordinate contractor IPT (CIPT) may be formed to support the Federal IPT and Project Director.

Major Modification – Modification to a DOE nuclear facility that is completed on or after April 9, 2001, that substantially changes the existing safety basis for the facility.

Preliminary Documented Safety Analysis Report (PDSA) – Documentation prepared in connection with the design and construction of a new DOE nuclear facility or a major modification to a DOE nuclear facility that provides a reasonable basis for the preliminary conclusion that the nuclear facility can be operated safely through the consideration of factors such as:

(1) the nuclear safety design criteria to be satisfied;
(2) a safety analysis that derives aspects of design that are necessary to satisfy the nuclear safety design criteria; and
(3) an initial listing of the safety management programs that must be developed to address operational safety considerations.

Preliminary Hazards Analysis (PHA) – This document provides a broad hazard-screening tool that includes a review of the types of operations that will be performed in the proposed facility and identifies the hazards associated with these types of operations and facilities. The results of the PHA are used to determine the need for additional, more detailed analysis; serve as a precursor where further analysis is deemed necessary; and serve as a baseline hazard analysis when further analysis is not indicated. The PHA is most applicable in the conceptual design stage, but it is also useful for existing facilities and equipment that have not had an adequate baseline hazard analysis.

Preliminary Safety Design Report (PSDR) – The report developed during Preliminary Design that updates and provides additional site and design details to those provided in the CSDR. The PSDR follows the format and content of the PDSA produced during final design.

Preliminary Safety Validation Report (PSVR) – The report prepared by DOE that documents the DOE review of the Preliminary Safety Design Report.

Safety Design Strategy (SDS) – The SDS, as part of the Project Execution Plan, provides a strategy for the early safety design basis development starting in the pre-conceptual design phase. The SDS documents all applicable Safety-in-Design expectations for the early project phases.

Safety-in-Design – The process of identifying and incorporating appropriate structures, systems, and components (SSCs) and their associated safety functions and design criteria into the project design to provide adequate protection for workers and the public.

Safety Design Integration Team (SDIT) – This contractor team, when established, supports the Federal or the Contractor Integrated Project Team (IPT) to ensure the integration of safety into the design process. The composition of the team is adjusted as necessary to ensure the proper technical representation commensurate with the analyzed hazards and the specific project phase. The SDIT ultimately supports decisions to be made by the Federal Project Director.

Safety Evaluation Report (SER) – The report prepared by DOE to document (1) the sufficiency of the documented safety analysis for a Hazard Category 1, 2, or 3 DOE nuclear facility; (2) the extent to which a contractor has satisfied the requirements of Subpart B of this part; and (3) the basis for approval by DOE of the safety basis for the facility, including any conditions for approval.

Safety Limits – The 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.

1.0 INTRODUCTION

1.1 Background

Federal Project Directors are accountable for the planning, programming, budgeting, and acquisition of capital assets. The principal goal of the Department of Energy (DOE) Acquisition Management System is to deliver capital assets on schedule, within budget, and fully capable of meeting mission performance and environment, safety, and health standards. DOE Federal Project Directors are responsible for managing capital asset projects with integrity and in compliance with applicable laws and contractual provisions. Major DOE objectives include obtaining quality products, ensuring timeliness of performance, controlling cost, and preventing or mitigating adverse events. To achieve these goals, Federal Project Directors assemble an integrated team that includes members from other DOE functional areas, such as budget, financial, legal, safety, and contracting, to assist them with the planning, programming, budgeting, and acquisition of capital assets.

DOE O 413.3A, Chg 1,, *Program and Project Management for the Acquisition of Capital Assets*, was developed to implement the DOE acquisition policy and Office of Management and Budget (OMB) Circulars[1] regarding planning, budgeting, and acquisition of capital assets; management accountability and control; financial management; and management of Federal information resources. The process, described in the Order and associated DOE directives and guidance[2] and implemented by DOE organizational elements, is referred to as the DOE Acquisition Management System.

A fundamental element that is necessary to achieve the DOE goal for capital asset acquisition is the integration of safety throughout the DOE Acquisition Management System. This Standard supports the DOE objective by providing guidance on those actions and processes important for integrating safety into the acquisition process for DOE Hazard Category 1, 2, and 3 nuclear facilities. Integrating safety into design is more than just developing safety documents that are accepted by the design function and organization: it requires that safety be understood by, and integrated into, all functions and processes of the project. Therefore, this Standard identifies interfaces, methodologies, and documentation strategies that might support proper integration. In addition, the Standard provides format and content guidance for the development of safety documentation required by DOE O 413.3A, Chg 1,[3] and 10 CFR 830, *Nuclear Safety Management*. These required documents include the Conceptual Safety Design Report (CSDR), the Preliminary Safety Design Report (PSDR), and the Preliminary Documented Safety Analysis (PDSA). The Standard provides information and the methodology for identifying and analyzing hazards, selecting and

[1] OMB Circulars A-11 (Part 7), A-123, A-127, and A-130.
[2] The DOE Office of Engineering and Construction Management (OECM) also publishes Project Management Practices that are available on the OECM web page: oecm.energy.gov.
[3] The application and use of any revision to DOE O 413.3A,Chg 1, will be determined by DOE for any ongoing project.

classifying appropriate safety structures, systems, and components (SSC), and integrating safety personnel at pertinent phases of project initiation, definition, and execution.

1.2 Roadmap to the Standard for Categories of Users

The Standard is written primarily for the use of the contractor(s) responsible for the design of a new facility. The processes described in the Standard, in addition to facilitating the integration of safety into design by the contractor, result in the development of several documents for input to the federal project team, the Federal Project Director and his Integrated Project Team (IPT). These documents include:

- the Safety Design Strategy (SDS), which supports the development of a Tailoring Strategy and the Project Execution Plan (PEP) required by DOE O 413.3A, Chg 1;
- a Risk and Opportunities Assessment, which supports the Risk Management Plan required by Order 413.3A, Chg 1; and
- three safety reports required by Order 413.3A, Chg 1, (Conceptual Safety Design Report, Preliminary Safety Design Report, and the Preliminary Documented Safety Analysis).

Chapter 2 of this Standard discusses the preparation, reviews, and approvals of these safety documents.

There are several categories of target audiences/users of the Standard. The parts of the Standard particularly relevant to all audiences are the Preface, including the key concepts and guiding principles upon which the Standard was developed, this Introduction (Chapter 1), Chapter 2, Project Integration and Planning, and Chapter 3, Safety Considerations for the Design Process, which provides an overall perspective of the Safety-in-Design process of this Standard.

Project management, both federal and contractor, will also find Chapter 7, *Safety Program and Other Important Project Interfaces*, Appendix E, *Safety Design Strategy*, and Appendix F, *Safety-in-Design Relationship with the Risk Management Plan* informative and useful to their responsibilities and functions.

Project safety personnel and DOE safety reviewers will find that Chapter 4, Hazard and Accident Analyses; Chapter 5, *Nuclear Safety Design Criteria*; Chapter 6, *Safety Reports*; Appendices A through D, which deal with safety SSC and seismic classifications; and Appendix G, *Hazards Analysis Table Development* are directed toward their functions and responsibilities. Appendix F, *Safety-in Design Relationship with the Risk Management Plan* is also important to safety personnel because they are the source of initial input to the Risk and Opportunities Assessment related to safety assumptions and uncertainties that can affect the project's cost and schedule.

Project design personnel should be familiar with Chapter 5, Nuclear Safety Design Criteria, Chapter 7, Safety Program and Other Important Project Interfaces, and Appendices A through D, which address safety design classifications for safety SSCs.

Appendices H and I, which are format and content guidance for the preparation of the CSDR, PSDR, and PDSA, are important to the project team members charged with the preparation of these documents and to the DOE reviewers of them.

For projects that are potential major modifications of existing facilities, Chapter 8, Additional Safety Integration Considerations for Projects, and Appendix J, Major Modification Determination Examples are especially relevant.

1.3 Applicability

This Standard applies to the design and construction of the following:

- new DOE Hazard Category 1, 2, and 3 nuclear facilities;
- major modifications to DOE Hazard Category 1, 2, and 3 nuclear facilities (as defined by 10 CFR 830); and
- other modifications to DOE Hazard Category 1, 2, and 3 nuclear facilities managed under the requirements of DOE O 413.3A, Chg 1.

The activities and processes in this Standard may be applied to new facilities and to modifications to those facilities not listed above.

DOE O 413.3A fundamentally establishes the roles, responsibilities, and requirements for the Department in the DOE Acquisition Management System. The Contractor Requirements Document (CRD) attached to that Order delineates requirements for contractors in the Project Management System. The tasks, deliverables, and suggested tools in this Standard are generally intended to be provisions primarily for DOE contractors, unless they are specifically identified as DOE actions. DOE responsibilities for review and approval of contractor submittals identified in this Standard are discussed in Chapter 2. DOE-STD-1104-2008, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents*, provides guidance for the review of safety design basis documents.

For DOE projects subject to regulation by the Nuclear Regulatory Commission (NRC), where requirements in this standard overlap or duplicate applicable NRC requirements for nuclear safety (including quality assurance), the NRC requirements apply to the design, construction, operation, and decommissioning of DOE facilities and will be used to satisfy redundant or duplicative requirements from this standard. This exclusion does not apply to requirements for which NRC defers to DOE or does not exercise regulatory authority.

1.4 Must and Should

The verbs "must" and "should" are used throughout this Standard. If this Standard is listed as a contract requirement, or otherwise directed by DOE for a facility or project, the DOE contractor or other organization required to meet this Standard must comply with all of the applicable provisions that include the word "must". Provisions that use the word "should" are not required, but they are recommended in order that the expectations of this Standard can be implemented, particularly for complex or hazardous activities.

The majority of "must" statements in this Standard are derived from DOE directives, primarily DOE O 413.3A, Chg 1, DOE O 420.1B, and 10 CFR 830. That is, they reflect required actions necessary to comply with one or more of these directives. Where an activity is required by a DOE directive but is not directly involved with the integration of safety with design, it is assumed to be carried out by the project and may be indicated by "is" or "are" rather than a "must".

In addition, this Standard includes "must" statements associated with the Key Concepts and Guiding Principles that work together in enabling effective Safety-in-Design. Their application is necessary for the effective integration of safety into a project or facility design. The Guiding Principles of the Standard are derived from O 420.1B and O 413.3A, Chg 1. The Key Concepts include features introduced in this Standard and are consistent with effective implementation of O 420.1B and O 413.3A, Chg 1, regarding integration of Safety-in-Design. Failure to apply one or more of these principles or concepts to a new project or major modification design results in an effort that cannot claim to have fully implemented this Standard.

Requirements specific to this Standard are defined only for objectively measurable parameters or conditions. Requirements are not defined when objective evidence of compliance is not achievable. Requirements unique to this Standard include the establishment of a Safety Design Strategy (SDS), which is in support of the tailoring strategy and Project Execution Plan (PEP) required by DOE O 413.3A, Chg 1; the Risk and Opportunities Assessment, which is in support of the Risk Management Plan required by DOE O 413.3A, Chg 1; and Appendix A, which specifies new safety design classification criteria. The remaining unique "must" statements are judged to be necessary to comply with the Safety-in-Design processes described in this Standard.

Specific elements of this Standard may appropriately be tailored to fit a specific project and the SDS should establish the tailoring strategy. However, the Key Concepts and Guiding Principles represent high-level expectations for Safety-in-Design and are therefore applicable independent of tailoring.

1.5 Supplementary Guidance Documents

DOE M 413.3-1, *Project Management for the Acquisition of Capital Assets*, and any guides developed in support of DOE O 413.3A, Chg 1, should be referred to and used in conjunction with this Standard to enhance safety integration into project management processes and decisions.

2.0 PROJECT INTEGRATION AND PLANNING

DOE O 413.3A , Chg 1, requires the formation of an Integrated Project Team (IPT), to be led by a Federal Project Director. Subgroups to the IPT may be chartered during the project, including a Contractor Integrated Project Team (CIPT) led by the Project Manager, as well as subgroups to the IPTs for specific tasks or deliverables. Further information on the roles, responsibilities, and functions of the IPT are provided in the Office of Engineering and Construction Management (OECM) Project Management Practices, *Integrated Project Teams* (see footnote 2).

The Federal Integrated Project Team (IPT) will comprise both DOE Federal staff and contractors, and the contractor Project Manager will be a key member of the Federal IPT. If a Contractor IPT is formed for certain complex or hazardous projects, interfaces between the two IPTs must be established to ensure synchronization of information and reviews for all disciplines and functions essential to the project. The interfaces and interactions necessary for effectively integrating safety into project design are addressed in this Standard. Contractor IPT activities and deliverables support the Federal IPT and project decisions that are made by DOE.

Similar to the roles and functions of the Federal IPT, Safety-in-Design roles and functions for each project should be specifically tailored for that project. The contractor should establish a Safety Design Integration Team (SDIT), especially for complex or hazardous projects. The SDIT would be the Safety-in-Design team support for the CIPT, if a CIPT is established, and would also be the key Safety-in-Design interface with the Federal IPT. For small or less-complex projects with a straightforward safety strategy, an SDIT may not be required, and any contractor Safety-in-Design input would go directly to the CIPT or Federal IPT through appropriate subject matter experts (SME). If an SDIT is formed, it should implement the Safety Design Strategy (SDS). The SDS and SDIT are discussed in sections 2.2 and 2.3.

DOE O 413.3A , Chg 1, requires the appointment of a Federal Project Director and formation of an Integrated Project Team (IPT) during the conceptual design phase. Based on the documentation required at CD-1, such as an acquisition strategy, Project Execution Plan (PEP), a design review, and preparation of a Conceptual Safety Design Report (CSDR), appointing a Federal Project Director and forming an IPT and the contractor SDIT should be among the first orders of business as soon as mission need is approved (CD-0), if not before.

2.1 Contractor Integrated Project Team

A CIPT may be formally established for complex or hazardous projects, with the Contractor Project Manager serving as the team leader.[4] If established, the CIPT

[4] It is recommended that a CIPT be considered for all Hazard Category 1 and 2 nuclear projects. If a Federal IPT is collocated with the contractor project team and has an active direct and dedicated management role for the project, a CIPT may not be warranted. The intent is to form a dedicated IPT, ultimately reporting to and supporting the Federal Project Director that will have active day-to-day roles and responsibilities on complex nuclear projects.

provides the overarching contractor focal point specifically charged with executing a project through interactions with and support to the IPT and Federal Project Director. As the team members are representative of all competencies that influence or affect the execution of the project, the CIPT provides an important forum where project issues can be openly discussed and resolved. As a project progresses from initiation to transition/closeout completion, the CIPT membership may change to incorporate the necessary skills and expertise. Although a core team is expected to provide direct support to the project, team membership may be either full-time or part-time, depending on the scope and complexity of the project.

The contractor safety lead should be a member of the CIPT and should be responsible for representing all safety issues before the team and for ensuring that project issues are appropriately shared with the SDIT.

2.2 Safety Design Integration Team

If established, the SDIT should include the key members of the contractor project team who implement Safety-in-Design for the project. The SDIT is expected to be a dynamic organization that will be made up of a limited core team comprising safety, design, and operations personnel, as well as SMEs, who will come together for short or extended periods of time to accomplish a task. Often these task-specific teams may consist of the same people each time, but they will have a targeted responsibility that requires their time and attention away from their normal activities. For example, the SDIT will be quite active, and the membership will increase, while performing a hazard analysis. As noted previously, the CIPT may fulfill the role of the core SDIT for small projects or projects with a simple, straightforward safety strategy. Team composition is critical for the SDIT to be successful. A multi-disciplinary team is needed to identify and analyze the hazards in the facility and to ensure that the designed controls:

- are adequate to perform the safety function;
- do not create an undue burden on operations;
- can be designed to fulfill the safety function; and
- fit within the project cost and schedule.

The SDIT (or the project safety lead if there is no SDIT) is responsible for drafting a SDS and also for preparing a Risk and Opportunity Assessment. The Risk and Opportunity Assessment is input to the project's Risk Management Plan and is summarized in that document.

Although the appropriate team composition will depend on the process or unit operation being developed, it should always include the core team and appropriate supporting specialists. The core SDIT should consist of safety personnel (CIPT safety lead), engineering and design personnel responsible for the process or facility, operations personnel, and the line management of the design organization. In addition to the core team, supporting specialists may be included as appropriate from the following areas:

- security (depending on the project, security may need to be a core team member);
- design, including appropriate disciplines (Civil, Structural, Electrical, Instrumentation, etc.);
- geotechnical/seismic;
- health physics and radiological protection (shielding, uptakes, or exposure to hazardous materials, etc.);
- safety, accident, or risk analysts with expertise needed by the team;
- criticality safety;
- research and development (process, equipment development specialists);
- process chemistry;
- industrial safety (Occupational Safety and Health Administration [OSHA] issues);
- fire protection;
- emergency preparedness;
- environmental protection and waste management;
- human factors; and
- interfacing system representatives.

The presence of specialists will vary according to the process or unit operation that will be designed or analyzed and with the phase of the project.

Communication within the CIPT and the SDIT is paramount to understanding the major issues and ensuring that the solutions put forward as design or planned operations are appropriate and fully meet the needs of design, construction, project constraints, facility operations, and safety. Timely and effective interactions between the CIPT and the Federal IPT are crucial for mission success.

2.3 Safety Design Strategy

A Safety Design Strategy (SDS) must be developed for all projects subject to this Standard. DOE expectations for execution of safety activities during design should be identified and documented to support the development of the statement of mission need. The documentation of the DOE expectations for execution of safety during design is developed by the DOE safety lead and should define high-level DOE expectations. The SDS should then be based on those DOE expectations and should be developed as early in the Conceptual Design Phase as practicable. These DOE expectations are used during the development of the project SDS in the conceptual design stage. The SDS is updated throughout the design process.

As the initial project safety management integration tool, the SDS provides the preliminary information to gauge the scope of significant hazards and the general strategy for addressing those hazards. The SDS is a tool to guide design, document the safety analysis approach, support the safety design basis documents to be developed during each project phase, and establish concurrence on major safety decisions related to project cost and schedule. It provides a single source for project safety policies, philosophies, major safety requirements, and safety goals to maintain alignment of safety with the design basis during project evolution.

The SDS should contain enough detail to guide design on overarching design criteria, establish major safety SSCs, and identify significant project risks associated with the proposed facility relative to safety. Specifically, the SDS should address the following four main attributes of safety integration as the project progresses through project planning and execution:

- The guiding philosophies or assumptions to be used to develop the design,
- The Safety-in-Design and safety goal considerations for the project,
- The approach to developing the overall safety design basis for the project, and
- Significant discipline interfaces impacting safety.

For projects that may not follow the traditional project cycle, the SDS provides a vehicle to describe how requirements for safety documentation will be tailored to that particular project approach while satisfying DOE O 413.3A, Chg 1.

For certain projects, safety assumptions and criteria may be known when DOE approves the mission need at CD-0 (e.g., the facility will be a Hazard Category 2 nuclear facility). These assumptions and criteria should be in the SDS and should be used for developing the conceptual design and CSDR.

The SDS is not intended to supplant or duplicate the required safety deliverables to or include information that should be contained in other project documentation (e.g., schedules, resource requirements).

The SDS, at the conceptual design phase, is prepared by the SDIT (or the contractor safety lead in the absence of an SDIT) as an evolution of the DOE expectation for the execution of safety activities during design. It is approved by DOE Safety Basis Approval Authority and the Federal Project Director, with the advice of the Chief of Nuclear Safety (CNS) or the Chief of Defense Nuclear Safety (CDNS), as appropriate.

Updates to the SDS should focus on those major safety decisions that influence project cost (e.g., seismic design criteria, confinement ventilation, safety functional classification, and strategy). Interim SDS updates can provide a means by which all parties are kept informed of important changes due to safety in design evolution between Critical Decision points.

This Standard anticipates that the eventual safety basis for the facility being constructed or modified will be based on the format and content of DOE-STD-3009-94, CN 3. If a different methodology is applicable to the project or modification (e.g. legacy facilities or departmental decontamination and decommissioning activities), the SDS should establish that expectation, and the format of the PSDR/PDSA as provided in this Standard should be modified as appropriate. However, the expectations for integration of safety into the design process and application of nuclear safety design criteria apply to all projects and modifications within the scope of this Standard.

The safety documentation for a major modification project must include an SDS and a PDSA. Modification projects that require a new or revised hazards/accident analysis or require new hazard controls must be evaluated using the Major Modification Evaluation Criteria to determine if the modification constitutes a “major modification” and requires a PDSA (see Table 8.1). This evaluation must be documented in the PEP, the SDS itself, or in another appropriate project authorization document.

Modification projects that do not involve a “substantial change to the safety basis” to an existing nuclear facility as defined in 10 CFR 830 are not considered “major modifications” and do not require a CSDR, PSDR or a PDSA. For modifications subject to DOE O 413.3A, Chg 1, the SDS should document the type and scope of the hazard/accident analysis, describe the supporting safety documentation and DSA amendment or revision to be prepared, and should explain the process to develop and review and approve these documents (see Section 2.4.4, “Tailoring of Requirements”). These modifications may represent a capital asset project other than a major modification that is subject to the acquisition processes in DOE O 413.3A, Chg 1. This Standard and the included Safety-in-Design approaches may be tailored for these modifications. As previously mentioned, in such cases the basis for determining that the modification is not a major modification must be documented. Guidance for determining whether a facility modification involves a “substantial change to the facility safety basis” and is considered to be a “major modification” under the requirements of 10 CFR 830, is provided in detail in Section 8.1.

Modifications not requiring a new or revised hazard analysis/accident analysis and not requiring new hazard controls are considered simple modifications. These modifications need not be subject to the safety integration provisions of this Standard.

The SDS is discussed in detail in Appendix E and the SDS role in each project phase is discussed in Chapter 3 of this Standard, along with the Safety-in-Design activities for that phase. Section 6.4 addresses the change control process that is applicable to safety documentation.

2.4 Safety Interface with Project Management

2.4.1 Relationship to Project Management

DOE O 413.3A, Chg 1, governs the execution of most DOE capital asset acquisition projects. The integration of the safety design development and approval processes into the execution cycle for DOE Hazard Category 1, 2, and 3 nuclear facilities is the focus of this Standard. This section defines how the project management requirements in DOE O 413.3A, Chg 1, relate to this Standard.

Many projects are executed as "design-bid-build" projects with defined conceptual, preliminary, and final design phases. This is the underlying acquisition model presumed in this Standard. However, many projects are executed using different acquisition models and strategies. Accordingly, it is incumbent upon the Federal Project Director and the IPT to examine the provisions in this Standard and apply its processes and guidance appropriately to the project. This appropriate application of the processes, guidance, and methodologies in this Standard to the relevant phases of a project is known as "tailoring". However, the project management requirements of DOE O 413.3A, Chg 1, will govern the timing and substance of critical DOE project decisions.

In accordance with DOE O 413.3A, Chg 1, contractors responsible for the design of DOE Hazard Category 1, 2, and 3 nuclear facilities must implement this Standard, including the safety criteria of Appendix A, and submit the following safety basis documents for DOE approval (unless otherwise agreed to).

- Conceptual Design Stage: Safety Design Strategy
- Conceptual Design Stage: Conceptual Safety Design Report (CSDR)
- Preliminary Design Stage: Preliminary Safety Design Report (PSDR)
- Final Design Stage: Preliminary Documented Safety Analysis (PDSA)
- Prior to Operations: Documented Safety Analysis and Technical Safety Requirements

The Federal Project Director is responsible for ensuring the implementation of the requirements of DOE O 413.3A, Chg 1, and does this through contract requirements and through support of DOE entities. As such, the Federal Project Director approves or concurs on the approval of all safety submittals of the project. The DOE Safety Basis Approval Authority approves of the CSDR, PDSR, and PDSA based on a review by a Safety Basis Review Team. Table 2-1 shows the entities responsible for preparation, review, and approval of these safety documents.

Table 2-1. Roles and Responsibilities

Product/ Document	Responsibility			Interface with Other Documents/Products
	Prepare	Review	Approve	
Safety Design Strategy (SDS)	Contractor SDIT or, in the absence of an SDIT, the contractor safety lead is responsible for the preparation of the SDS as early in the Conceptual Design phase as practicable. The SDS is updated, as necessary, throughout the design stages.	DOE Safety Basis Review Team and the Integrated Project Team	Federal Project Director and the Safety Basis Approval Authority.	Pre-conceptual planning activities will provide the starting point. The SDS is part of or can be referenced from the tailoring strategy part of Project Execution Plan.
Risk & Opportunity Assessment	Contractor SDIT or, in the absence of an SDIT, the contractor safety lead prepares the Risk and Opportunity Assessment. It is updated, as appropriate, throughout the design stages.	Federal Integrated Project Team and the DOE Safety Basis Review Team	Federal Project Director	The Risk and Opportunities Assessment is input to the Risk Management Plan. It is summarized in the Risk Management Plan.
Conceptual Safety Design Report (CSDR)	Contractor SDIT or, in the absence of an SDIT, the contractor safety lead is responsible for the preparation of the CSDR.	DOE Safety Basis Review Team and the Integrated Project Team	Approval is via approval of the CSVR.	The CSDR needs to be consistent with the Conceptual Design Report (CDR).
Conceptual Safety Validation Report (CSVR)	DOE Safety Basis Review Team. DOE-STD-1104 provides guidance for review of the CSDR and preparation of the CSVR.	Federal Integrated Project Team	Safety Basis Approval Authority approves with concurrence by the Federal Project Director	The CSVR results from the DOE review of the CSDR. It documents the findings of that review and is a prerequisite to Critical Decision-1 (CD-1).

Product/ Document	Responsibility			Interface with Other Documents/Products
	Prepare	Review	Approve	
Preliminary Safety Design Report (PSDR)	Contractor SDIT or, in the absence of an SDIT, the contractor safety lead is responsible for the preparation of the PSDR	DOE Safety Basis Review Team and the Integrated Project Team	Approval is via approval of the PSVR.	The PSDR needs to be consistent with the Preliminary Design, as documented for the Preliminary Design Review.
Preliminary Safety Validation Report (PSVR)	DOE Safety Basis Review Team. DOE-STD-1104 provides guidance for review of the PSDR and preparation of the PSVR.	Federal Integrated Project Team	Safety Basis Approval Authority approves with concurrence by the Federal Project Director	The PSVR results from the DOE review of the PSDR. It documents the findings of that review and is a prerequisite to Critical Decision-2 (CD-2).
Preliminary Documented Safety Analysis (PDSA)	Contractor SDIT or, in the absence of an SDIT, the contractor safety lead is responsible for the preparation of the PDSA.	DOE Safety Basis Review Team and the Integrated Project Team	Approval is via approval of the SER	The PDSA needs to be consistent with the Final Design that is presented as part of the Critical Decision-3 (CD-3).
Safety Evaluation Report (SER)	DOE Safety Basis Review Team. DOE-STD-1104 provides guidance for review of the PDSA and preparation of the SER.	Federal Integrated Project Team	Safety Basis Approval Authority approves with concurrence by the Federal Project Director	The SER results from the DOE review of the PDSA. It documents the findings of that review and is a prerequisite to Critical Decision-3 (CD-3).
Documented Safety Analysis (DSA) and Technical Safety Requirements (TSR)	Contractor SDIT or, in the absence of an SDIT, the contractor safety lead, augmented by an operations team are responsible for the preparation of the operational DSA and TSR.	DOE Safety Basis Review Team and the Integrated Project Team	Approval is via approval of the SER	The DSA is an evolution of the PDSA. Any changes need to be identified and justified. The TSR is developed, based on the DSA.

Product/ Document	Responsibility			Interface with Other Documents/Products
	Prepare	Review	Approve	
Safety Evaluation Report	DOE Safety Basis Review Team. DOE-STD-1104 provides guidance for review of the DSA and TSR and preparation of the SER.		Safety Basis Approval Authority	The SER results from the DOE review of the operational DSA and TSR. It documents the findings of that review and is a prerequisite to Critical Decision-4 (CD-4).

2.4.2 General Expectations

This Standard focuses on establishing the safety design for a nuclear facility in an incrementally progressive way to provide some assurance that the safety design basis will be demonstrated to be acceptable when the design is completed. Accordingly, early project decisions on the technical approach should be reasonably conservative in establishing appropriate cost and schedule baselines for the project. The project is expected to evolve over time; the project design and safety design basis are also expected to evolve. The expectation is that within this evolution process, unanticipated issues will be minimized.

To ensure that the project/facility configuration can be managed appropriately, the basis for decisions related to safety must be clearly documented. This includes, for example, controls selection, material-at-risk (MAR), process options, inputs, and assumptions. This documentation allows later decisions to modify the design or safety design basis based on knowledge of the original decision and not just on the current understanding of the issue.

The overarching philosophy and logic in this Standard is that a heightened degree of conservatism is demanded in the earlier phases of a project when the design details are not available. In this vein, a broader or more conservative set of SSCs that would be designated as safety systems might be provisionally selected for conceptual design than might actually be required when the design is completed. The degree of conservatism can be relaxed, and, accordingly, the provisional set of SSCs may be refined when justified by evolving information as design progresses. This strategy should minimize the need for significant safety and major cost revisions to the project in later design cycles.

2.4.3 Planning

The project management practices required by DOE O 413.3A, Chg 1, emphasize appropriate planning for the execution of projects. The development and approval of the safety design is an essential element of the project execution cycle and warrants appropriate planning. The overall planning for project execution, of which safety is an integral part, is documented and approved in the PEP. To the extent desired by the IPT, and as specified in the project's tailoring documentation, the SDS and other safety planning documentation may be included within the PEP, or be included in other required project management or safety documentation as described is subsection 2.4.4 below.

2.4.4 Tailoring of Requirements

DOE O 413.3A, Chg 1, allows tailoring of the CD process for projects based on “risk, size, and complexity.” The tailoring approach for the CD process is typically described in a “tailoring strategy” or as part of the PEP. Tailoring of the safety design basis development steps and documents for a project is also permitted based on the level of risk posed by the facility chemical and radiological hazards, the complexity of the processing operations, and the scope of the hazards analysis required for the project. Tailoring of the safety design basis steps and documents is described in Section 2.3. The tailoring approach for safety design basis documents must be:

- described in the SDS; and
- summarized in the PEP.

DOE O 413.3A, Chg 1, specifies what safety documentation is required as prerequisites to obtaining specified CDs. This Standard provides guidance on the format and content of the safety documentation. As established in the tailoring strategy for the project, the information and approvals for documentation, as required by this Standard, can be sequenced, organized, and bundled as the project team desires to meet the safety performance measures in this Standard. For example, this option allows the project team to satisfy requirements often associated with separate documents or documents that are produced sequentially to be delivered in a manner that is effective and efficient for project team decisions. This Standard does not specify how a project would be phased or how the project supports its CDs. Instead, it specifies the safety expectations for a project during the project’s execution cycle. The mapping of when CDs are sought, what information requirements pertain to the CDs, and how the project will be executed will be specified in the tailoring strategy or, if desired, in the PEP. Should a significant change in the safety strategy occur, such changes may be documented by a revision to the SDS. Neither the PEP nor the applicable approved safety document (e.g., CSDR) need be revised to address the change. The safety documentation can be updated at the next CD safety document submittal (e.g., PSDR for the CSDR example above).

2.4.5 Safety Interface Requirements

The following are the requirements for the safety interface.

- In the process of selecting early, design-phase safety SSCs using reasonably conservative principles, it is recognized that project and design progression might cause the SSC designation to evolve. Significant impacts on the cost and schedule for potential changes in SSC designation are captured in the evolving cost and schedule baseline projections for the project, either explicitly (as part of projections for the evolving baseline design) or as an explicit contingency on those projections, if they are not included in the baseline design.

- The methods and criteria by which SSCs are designated (either safety class, safety significant, or defense-in-depth) during project phases must be justified and documented.
- The IPT must include applicable expertise to advise the Federal Project Director on matters relating to nuclear safety. DOE O 413.3A, Chg 1, requires the Chief, Defense Nuclear Safety (CDNS) and the Chief of Nuclear Safety (CNS) to validate that Federal personnel assigned to the Integrated Project Team as nuclear safety experts are appropriately qualified.

3.0 SAFETY CONSIDERATIONS FOR THE DESIGN PROCESS

This chapter discusses general concepts for fostering integration of safety considerations into design activities (Safety-in-Design) during the pre-conceptual, conceptual, preliminary, and final design stages.

As a project design progresses, the design organization determines the appropriate safety features to be incorporated into a project, and obtains concurrence by the Integrated Project Team (IPT). The design organization and IPT should identify and reach agreement on these features as early in the process as it is possible and practical to do so. The goal is to make decisions at as early a point as possible, recognizing that as design progresses, these decisions may need to be revisited. In particular, it is important that the design decisions be transparent and visible to all stakeholders and that any related issues regarding them are recognized and included in the Risk Management Plan (RMP), as discussed in Appendix F.

The design process for a complex facility is highly interactive and iterative. Therefore, coordination and communication among the activities and the individuals performing them is vital to the overall success of these activities. Because the design is evolving as the hazards and safety analyses are performed, it is essential that the IPT and Safety Design Integration Team (SDIT) are aware of the current state of the design at all times and that design staff are current on the status of the hazards/safety analyses work. Mechanisms must be established to ensure these communications.

Failure to incorporate safety considerations early in the design process can result in prohibitively expensive changes later in the design process if they are recognized only at the Preliminary Documented Safety Analysis (PDSA) development stage (i.e., during final design). To document safety design features early in the design process, DOE O 413.3A, Chg 1, prescribes reports at both the conceptual design phase (Conceptual Safety Design Report or CSDR), and the preliminary design phase (Preliminary Safety Design Report or PSDR), in addition to the required PDSA before the start of construction. The content and detail of these reports should be tailored to the safety information and maturity of the design as appropriate for the specific project.

This chapter discusses the Safety-in-Design considerations and activities to be performed during the initiation (pre-conceptual planning), conceptual design, preliminary design, and final design phases. The chapter also depicts the typical flow and interrelationships among project management, design development, and safety design basis development activities for these four phases. The design process for a specific project may vary considerably, commensurate with the tailoring of a project. The tailored design process is identified in the Project Execution Plan (PEP), which also evolves with the project activities. The Safety Design Strategy (see Section 2.3 and Appendix E) is developed consistent with, and works in conjunction with, the PEP and guides project design and safety documentation development.

The four figures in this Chapter graphically portray the processes supporting each of the primary design phases of a typical project. These processes are associated with one or more of the marked divisions that represent Program and Project Management, Project Engineering, or Safety Design Basis activities. Within each marked division, activities may be shown as grouped together within a dashed box. These activities are so closely associated that they are elements of a larger effort. In turn, these boxes may be shown joined with double-headed arrows, representing the integration needed to support the individual efforts and the fact that these activities may iterate. In reality, there is no two-dimensional depiction of these processes that is complete and yet effective in illustrating all of the relationships involved.

3.1. Pre-Conceptual Phase

During the pre-conceptual phase, the program identifies any gap between its current and required capabilities and compares the gap to the strategic plan. This gap analysis is translated into a Mission Needs Statement, which serves as the vehicle for formally establishing a project to close the identified performance gap.

Safety-in-Design efforts must begin during the pre-conceptual phase of a potential design and construction project when initial planning activities occur. The project team must consider the Safety Design Guiding Principles and key concepts of this Standard in the development of the project requirements to support the Mission Needs package. To ensure these principles are incorporated at this phase, a safety lead should be designated as early as practical as a key member to be assigned to the IPT when it is formed. The safety lead will be responsible for providing safety input to guide early project planning consistent with the Guiding Principles and key concepts.

DOE expectations for execution of safety activities during design should be clearly communicated commensurate with the hazard and control selection information available at this early stage in the potential project. Safety-in-Design goals should be identified; expectations for adherence to the design requirements of DOE O 420.1B, and any special safety requirements or expectations (e.g., active confinement) for the project should be included. These DOE Expectations for Safety-in-Design efforts should be formally documented.

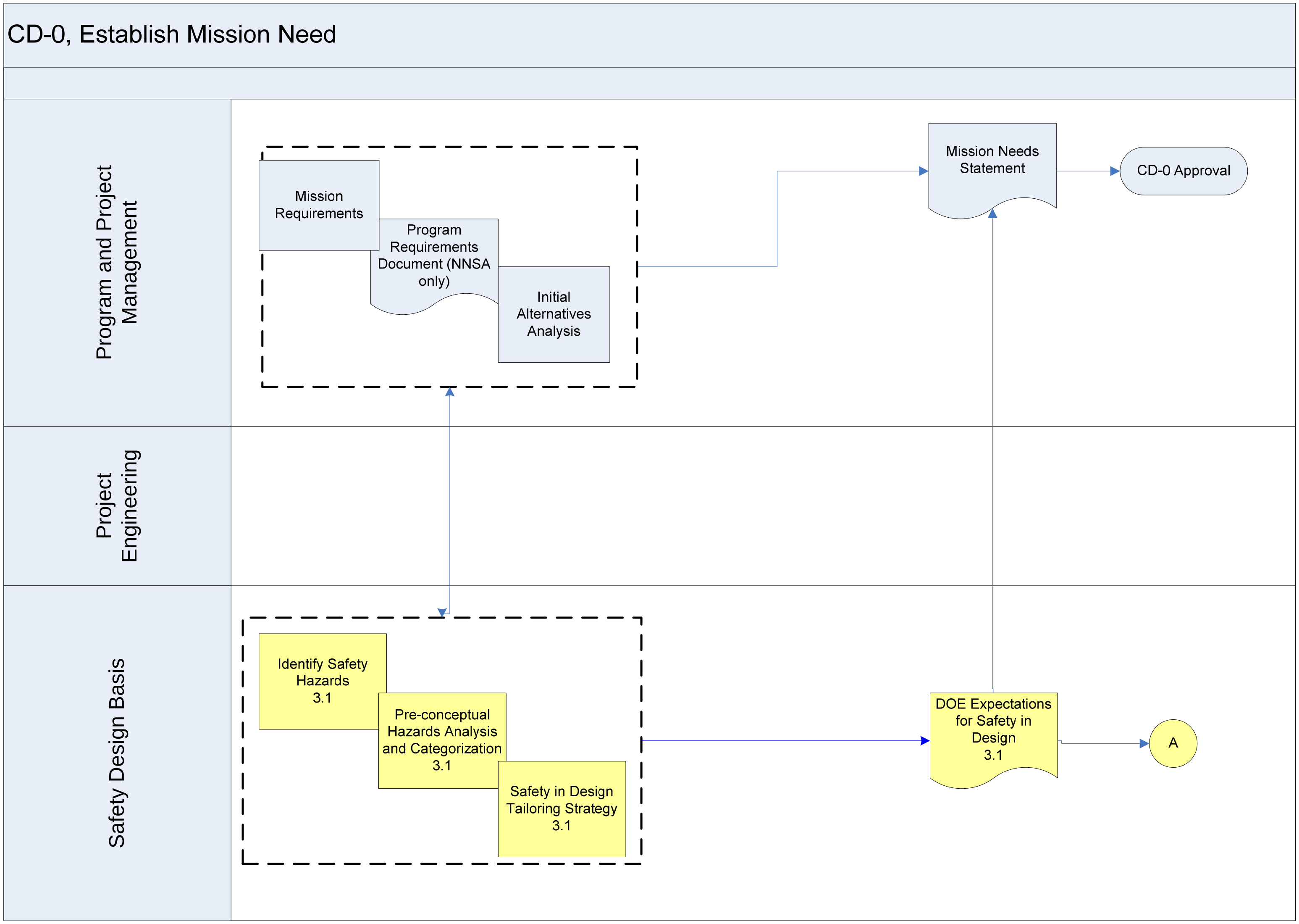
An initial alternative analysis is performed during the pre-conceptual planning phase to determine if a new facility or a modification to an existing facility would best satisfy the mission need. The analyst needs to have some understanding of the process technology that could be used for the facility to perform this analysis. In some cases, separate alternative analyses may be required to select the best process technology to achieve the facility mission. The material inputs and outputs, together with the process technology options, must be identified to provide the minimum amount of information needed for an initial assessment of the hazards posed by each proposed process. Detailed alternatives analyses will be completed later during the conceptual design phase.

Upper-level facility functions and performance requirements may also be developed in this phase. The physical form and quantities of the nuclear materials to be generated and received, and the waste materials to be produced, should be identified. This is important to ensure that the initial material release analyses can provide meaningful information. Generally, a simple process model that shows the material inputs and outputs will satisfy this purpose.

The hazard analysis at the pre-conceptual phase involves a qualitative high-level consideration of the facility/process risks performed in conjunction with the facility and initial technology selection alternative reviews. See Section 4.1 for guidance on hazard analysis for this phase of the project.

Figure 3-1 illustrates the interactions of project management and safety design basis development activities during the pre-conceptual design phase.

Figure 3-1. Pre-Conceptual Phase



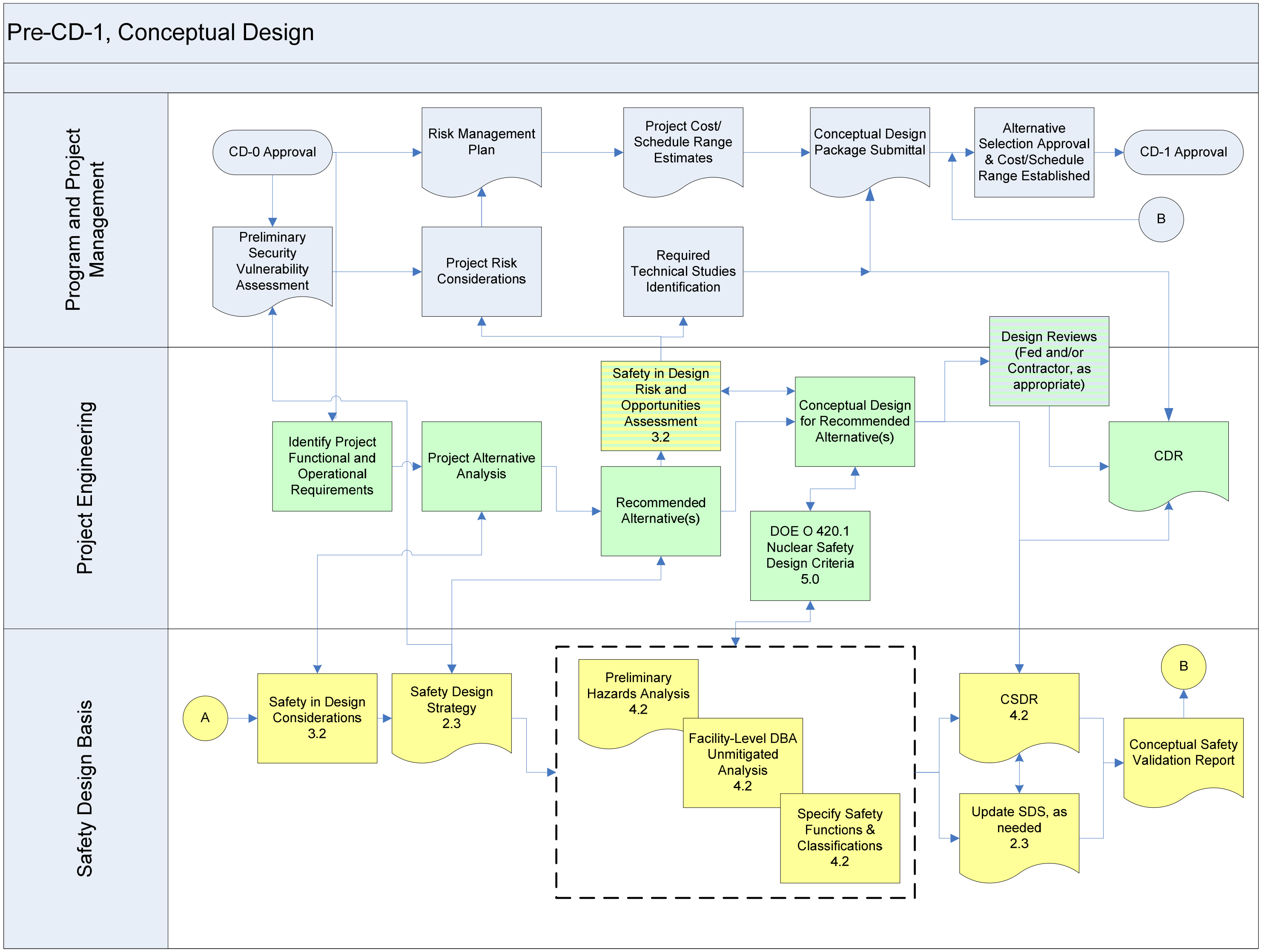
3.2 Conceptual Design Phase

The overall goal for Safety-in-Design at the conceptual design phase is to evaluate alternative design concepts, to prepare a Safety Design Strategy (SDS), and to provide a conservative safety design basis for a preferred concept to proceed into preliminary design. The intent is to perform sufficient analyses to make sound safety decisions during conceptual design and to document any risks and opportunities associated with selections and the associated project cost range and schedule impacts.

A Quality Assurance Program (QAP), compliant with 10 CFR 830, Subpart A, and DOE O 414.1C is established early in the project. The QAP describes the planned quality-related activities, surveillances, and assessments and is developed in the project conceptual phase and updated as the project matures. Section 8.9 of this Standard addresses the QAP in more detail.

The conceptual design phase presents a key opportunity for the safety analysis to influence the design. Figure 3-2 illustrates the interactions of project management, design development, and safety design basis development activities during the conceptual design phase. As can be seen in the figure, there are many activities that rely upon each other and that, in some cases, are iterative.

Figure 3-2. Conceptual Design Phase



The earlier in the project life cycle that requirements are identified and defined, the more effectively and efficiently the project will progress through the various phases and will meet project baselines, agreements, and commitments. As a project progresses from identification of the mission need through concept exploration, development, and design, the process of identifying, analyzing, and refining requirements is continual and is always ultimately traceable to specifications and designs. Once approved, the requirements document becomes part of the baseline requirements and is to be controlled through the change control process described in the PEP.

When design requirements are established, alternatives are evaluated to establish a process approach, and facility and equipment arrangements are determined. The configuration alternatives are evaluated against technical, safety, cost, and schedule criteria.

As design requirements are established for each alternative, engineering and safety personnel will begin to identify alternative facility layout and processing configurations. The DOE Expectations for Safety-in-Design and the Safety Design Guiding Principles and key concepts (see the Preface of this Standard) must be applied to these efforts to ensure that the design requirements and the selection of the preferred processing and facility arrangement alternatives are performed in a way that will result in a safe design. To ensure optimum Safety-in-Design considerations, a safety analyst must be involved as part of the evaluation of the processes for each of the various alternatives.

The SDS, at the conceptual design phase, is prepared by the SDIT (or the project safety lead in the absence of an SDIT) based on the DOE Expectations for Safety-in-Design. It is approved by DOE Safety Basis Approval Authority and the Federal Project Director, with the advice of the Chief of Nuclear Safety (CNS) or the Chief of Defense Nuclear Safety (CDNS), as appropriate.

As the processing approach and facility arrangements are being developed, alternatives are evaluated to select the design architecture; that is, the structures, systems and components (SSC). During the alternative analysis process, the IPT and SDIT ensure that the relative hazards, as well as the costs and uncertainties associated with the hazard controls that may be required to address these hazards, are considered for each alternative. The IPT and SDIT should also consider alternative facility locations that minimize the exposure of the public and collocated workers to facility releases or that minimize the threat of external events associated with nearby facilities.

Due to the need to develop an integrated process which assures that both the security and safety requirements are met, it is important to specify physical security needs early in the conceptual design process. This allows security and safety professionals to identify and resolve any potential conflicts and/or identify risks that will be incorporated into the risk and opportunities assessment. Recommendations from the initial security Vulnerability Assessment should be identified, including the need for new technologies, or incorporation of new technologies, and factored into the preliminary hazards analysis. To aid in this integration, the strategy for security design should be documented and incorporated, as appropriate, into the SDS.

Once the alternatives have been evaluated and a selected alternative designated, the design and safety work to identify and describe the SSCs to satisfy the facility performance requirements and to perform the facility processing operations is initiated. Safety design requirements and considerations in DOE O 420.1B, must be addressed in the developing design. To the extent that the design maturity will support in this conceptual phase, the Conceptual Safety Design Report (CSDR) includes a listing of applicable 420.1B design criteria and a brief summary of the implementation approach proposed for each applicable criterion. See Chapter 5 of this standard for further guidance on nuclear design criteria and Appendix H for documentation in the CSDR.

The SDIT should formally recognize this point in the conceptual design phase as a point where refocusing of efforts from alternatives comparisons and selection to the goal of producing a conceptual design that integrates safety into the design is needed.

The focus of safety work at this point in conceptual design is to (1) document and establish a preliminary inventory of hazardous materials; (2) document and establish the preliminary hazard categorization of the facility; (3) identify and analyze primary facility hazards and facility-level design basis accidents; and (4) provide an initial determination, based on the PHA, of safety class and safety significant SSCs. See Section 4.2 of this standard for guidance on hazard analysis for this project phase.

As a result of the requirements analysis and the alternatives analyses, a general process block-flow diagram or description of the process operations based on the selected technology and a general description of the more significant hazard controls should be developed for the project.

A Safety-in-Design Risk and Opportunity Assessment for the conceptual design is used to evaluate the overall safety design basis risks and opportunities associated with the project. The risks include the uncertainties related to the possibility that there may be additional costs and schedule impacts that are not yet identified because the design is still immature or there are uncertainties associated with the viability of the design and programmatic strategies selected. Opportunities refer to the potential opportunities to reduce the costs or improve the schedules as the design matures and to select proposed hazard controls or other cost and schedule drivers that are identified as not being necessary after all.

The Risks and Opportunities Assessment associated with the safety strategies that are selected is essential to a robust assessment for the project. Appendix F provides information to ensure a complete Risk and Opportunities Assessment is performed for the project.

In the conceptual design phase, the studies that still need to be completed to verify key safety strategy assumptions, make technology selections, or better understand the process operations or safety implications must be identified and should be documented in the SDS, CSDR, and CDR. Corresponding risks associated with possible outcomes of the studies identified should be included in the Safety-in-Design Risk and Opportunity Assessment.

The following major safety activities take place during the conceptual design phase.

- The requirements analysis from the pre-conceptual phase is further developed to include safety functions and SSC requirements and is documented in the project technical requirements documents and in the CDR.
- Alternative design concepts are analyzed and a preferred alternative is selected.
- An SDS is developed to guide design including description of strategies to address major hazards, commitment to appropriate safety design criteria and security issues as applicable.
- A Preliminary Hazards Analysis (PHA) is performed to provide the basis for facility preliminary hazard categorization. (Appendix G provides guidance on the information requirements for the PHA.)
- A preliminary Fire Hazards Analysis is performed that identifies and assesses fire risk and defines levels of Safety-in-Design that do not necessarily come from the PHA.
- A preliminary security Vulnerability Assessment is completed and factored into the PHA.
- A facility-level DBA Analysis is performed to identify the major facility safety functions needed.
- SSCs and their safety classifications are proposed for the major safety functions. (Appendices A, B, C, and D provide guidance on safety classifications.)
- The initial Safety-in-Design Risk and Opportunities Assessment is developed based on assumptions that may have been necessary and on uncertainties in safety and design considerations. (This assessment is input to the project Risk Management Plan and assessment.)
- The CDR is developed to document the final conceptual design architecture.
- The CSDR is developed to document the bases for the safety design aspects of the facility. (Appendix H provides guidance on the development and format and content of a CSDR.)
- Required technical studies necessary to resolve risks and opportunities are identified.
- The initial baseline range estimates are identified.
- DOE reviews the CSDR and prepares a Conceptual Safety Validation Report (CSVR).

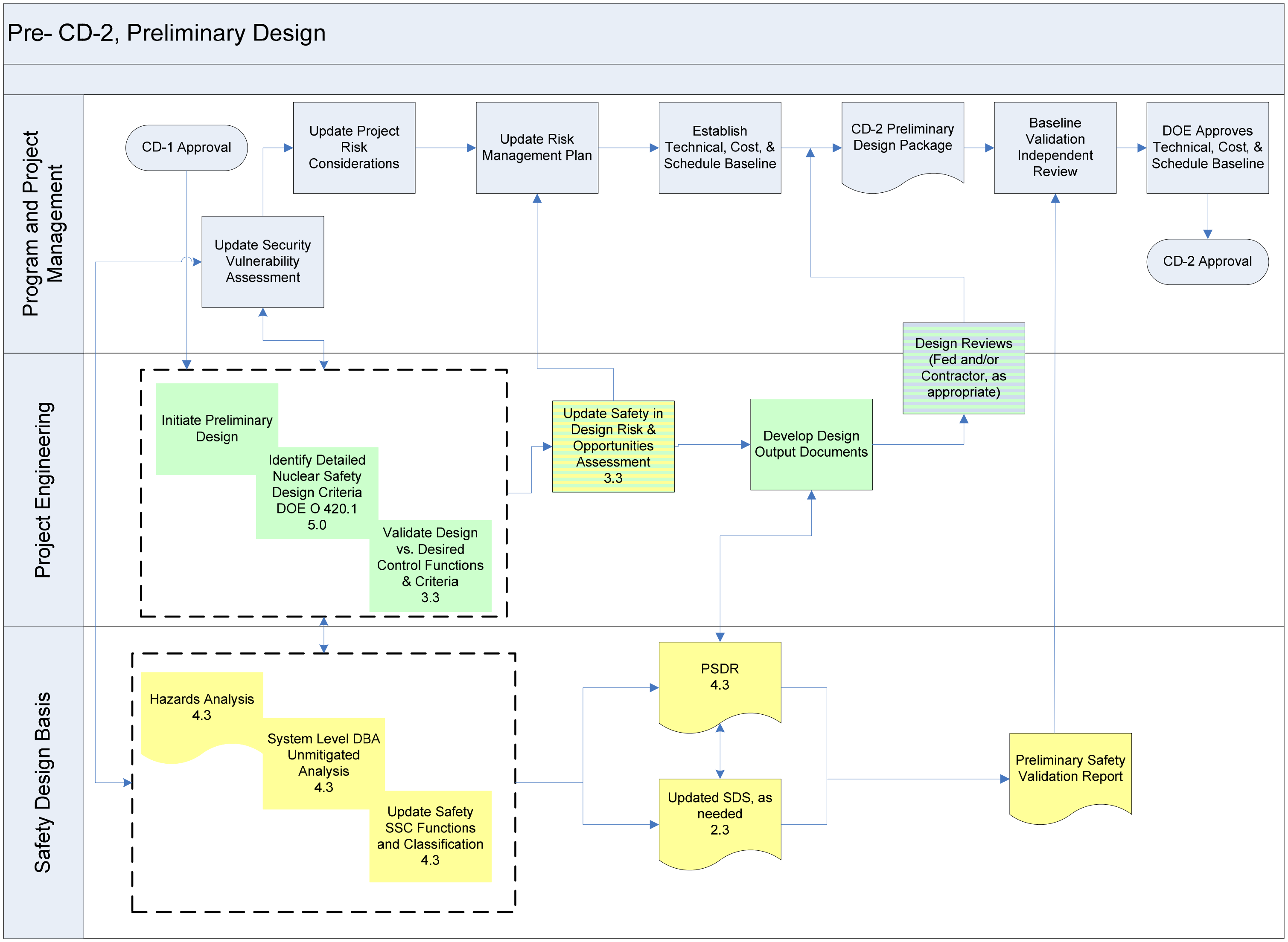
3.3 Preliminary Design Phase

Safety-in-design efforts during the preliminary design phase are intended to be incremental rather than a complete reevaluation of the conceptual design. The hazard analysis (HA) will evolve from a facility-level analysis to a system level hazard analysis as design detail becomes available. As the HA is refined, the selection of controls, safety functions, and classifications developed during the conceptual design phase must be revisited to ensure they are still appropriate.

Decisions made during the preliminary design phase provide the basis for the approach to detailed design and construction. Decisions that are reversed after this phase, for whatever reason, can have significant impacts on overall project cost and schedule. It is essential that contractor and DOE safety personnel are totally engaged and fully participate in design reviews during this phase, so their views and advice can be considered in the evolving design in a timely fashion.

Figure 3-3 depicts the workflow for the preliminary design phase.

Figure 3-3. Preliminary Design Phase



The project technical design requirements for the preliminary design phase include initial technical requirements for the project and embody many of the deliverables indicated in DOE O 413.3A, Chg 1, for the preliminary design phase, including the design requirements document(s) containing the information available at this phase These technical requirements include those derived from the safety analysis.

Because the design is still evolving at this point in the process, adequate Safety-in-Design for the preliminary design phase is based primarily on identifying viable engineering resolutions to nuclear safety design requirements and specifying an adequate set of more detailed safety design requirements that are based on safety analyses. During this phase a more complete assessment of hazard controls, based on hazards analyses at the process level, is developed, including those intended for in-facility worker protection. Section 4.3 of this Standard provides an expanded discussion of hazards analysis, hazard control selection, and safety classification of these controls.

The security Vulnerability Assessment should be updated based upon the developing design of the facility proposed security features. During this phase, security strategies may be refined, security system performance requirements are defined, and other infrastructure requirements are identified. Physical, information, personnel, and cyber security are all considered in the analysis.

The approach for demonstrating how the preliminary design will satisfy the nuclear safety design criteria of DOE O 420.1B or proposed alternative criteria must be developed during this phase if it was not done earlier. Because the design is still evolving at this point in the process, adequate Safety-in-Design for the preliminary design phase is based primarily on identifying viable engineering resolutions to nuclear safety design requirements and specifying an adequate set of more detailed safety design requirements that are based on safety analyses. Chapter 5 of this Standard provides guidance on the nuclear safety design criteria of DOE O 420.1B and Appendix I for documentation in the PSDR.

The Safety-in-Design Risk and Opportunity Assessment developed in the conceptual design phase must be updated during the preliminary design phase to reflect the results of any technical studies, design modifications, or other developmental work that impact the risk assessment. The results must be documented in the Risk Management Plan to provide information for the development of the project baseline cost, as described in DOE O 413.3A and its guidance.

Additional information regarding the aspects to be considered in the Safety-in-Design Risk and Opportunity Assessment is provided in Appendix F, "Safety-in-Design Relationship with the Risk Management Plan".

Any remaining studies that need to be performed to address specific details in the facility final design must be delineated in the preliminary design phase. These studies may include assumption validation studies, any remaining equipment selection studies (e.g., trade studies), and design optimization studies. Studies that could affect the safety design basis developed for the preliminary design should be highlighted in the safety strategy section of the PDR and in the PSDR. Corresponding risks associated with possible outcomes of the studies identified are included in the updated Risk and Opportunity Assessment.

Safety-in-Design documentation also evolves during the preliminary design phase as follows:

- PHA is revised and updated to an HA (see Chapter 4 and Appendix G);
- FHA is updated;
- The security Vulnerability Assessment is updated;
- PDSR is developed, building on the information in the CSDR (see Chapter 6);
- SDS is updated to reflect the evolution in the design and safety design bases (see Chapter 2 and Appendix E;
- Safety-in-design Risk and Opportunity Assessment is updated and should reflect changes that were made to take advantage of opportunities or address identified risks (see Appendix F); and
- By the end of design, the final National Environmental Policy Act (NEPA) documentation is completed to support the selected site.

3.4 Final Design Phase

During this phase, details for procurement in support of construction activities are developed. Typically, about 30 to 40 percent of the design activity is completed during the preliminary design phase, and the remainder of the design is completed during the final design phase.

By the final design phase, both the preliminary design and the PSDR will have been reviewed and approved. These reviews may prompt changes to the conclusions and approaches taken for safety and design in the preliminary phase. Similarly, evolution of the design from preliminary to final may prompt the design approaches and commitments captured in the PSDR to be revised based on improved knowledge and process optimization.

The security Vulnerability Assessment should be updated based upon the final design of the facility proposed security features. During this phase, security strategies, security system performance requirements, and other infrastructure requirements are finalized.

During this phase a final set of hazard controls is developed, based on hazards and accident analysis of the final design. The safety analyses in the final design phase, including mitigated analyses, must encompass the scope of the design and demonstrate that the designated safety SSCs are adequately designed to reliably perform their intended safety functions. Appendix G provides guidance on documenting the hazard analysis results.

The design adequacy of safety SSCs must be demonstrated. This is fundamental to the integration of Safety-in-Design activities. The burden of proof is on the design organization to demonstrate that the design and functional requirements derived from the safety analysis process are satisfied. The designed SSC should be evaluated to validate they can provide the desired safety function from the safety analysis, that they can be implemented, and are cost effective. Section 4.4 of this Standard provides an expanded discussion of hazards analysis, hazard control selection, and safety classification of these controls.

The PDSA addresses the broad range of issues necessary to demonstrate compliance with DOE O 420.1B and its guides; specifically, DOE G 420.1-1, -2, and -3, where applicable. Many of the design criteria are qualitative in nature and require an analysis to show how they are applied to a particular SSC. System and component design must satisfy national codes and standards (code[s] of record where applicable) identified in DOE G 420.1-1. Compliance with the requirements of these standards will be reviewed during acceptance of the safety documentation and during readiness activities in support of the CD-4 milestone. Appendix I discusses how the PDSA evolves from the PSDR. Both documents have the same format to simplify the evolution process.

The Safety-in-Design Risk and Opportunity Assessment from the preliminary design phase must be updated to reflect the results of any technical studies, design modifications, or other developmental work that affects the risk assessment. The Risk Management Plan is updated as necessary.

Design reviews at the final design phase should ensure that the safety analysis is current with respect to the design. The configuration management process at the final design stage should be well defined and able to track changes to the design and initiate conforming changes to analyses and documentation as changes are made. Section 6.4 of this Standard discusses expectations with respect to configuration management.

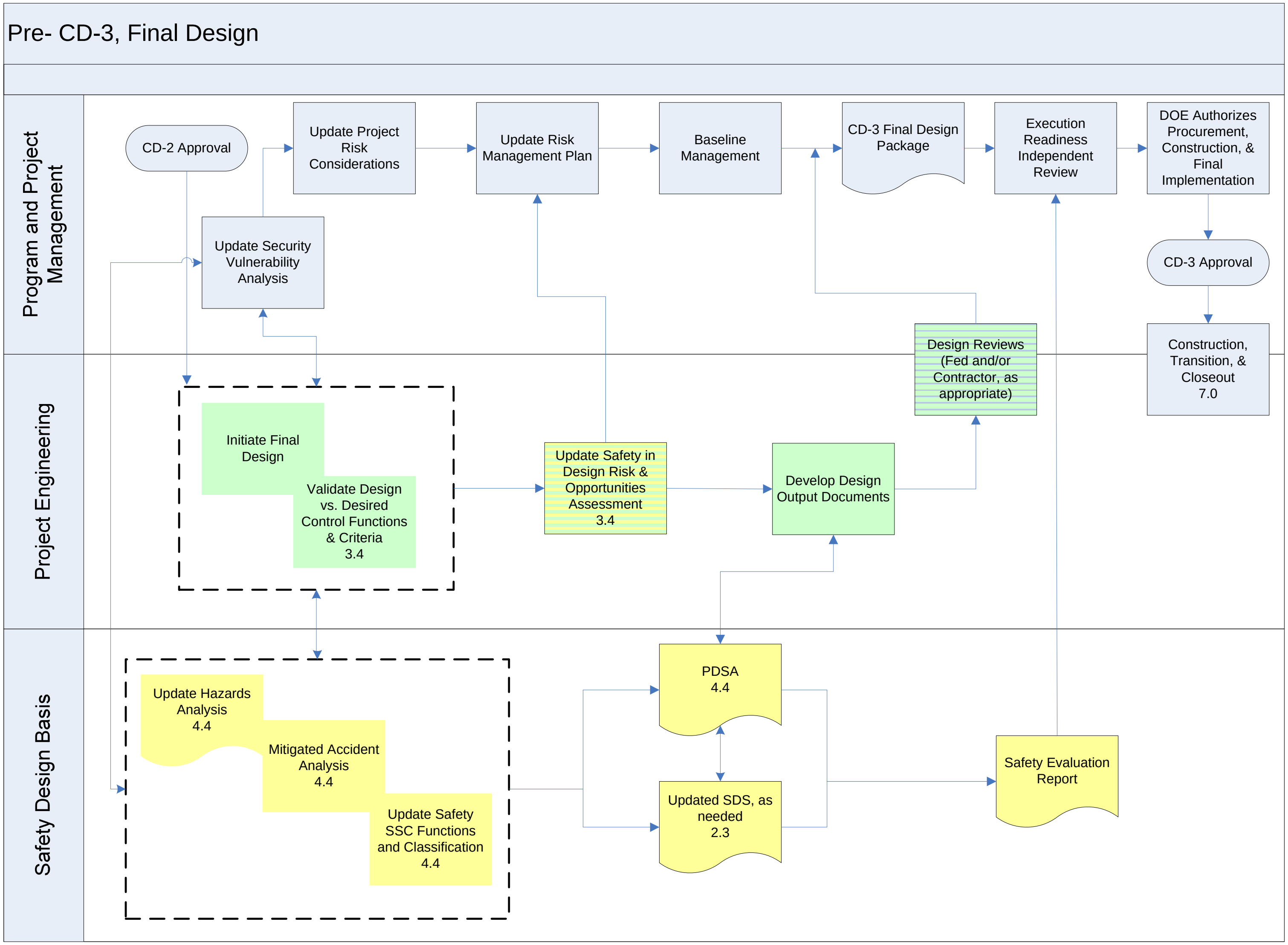
In addition, Section 3.9 of DOE-STD-1073, *Configuration Management*, provides guidance on turnover of configuration management from design to construction. As stated, these efforts should be begun well before turnover to ensure a smooth transition.

The following safety activities are typically performed during the final design phase:

- update SDS as necessary;
- update hazard and accident analysis;
- update the security Vulnerability Assessment
- update the design requirements document(s)
- update Safety-in-Design Risk and Opportunity Assessment; and
- prepare a PDSA.

Figure 3-4 depicts the workflow for the Final Design Phase.

Figure 3-4. Final Design Phase



3.5 Construction, Transition, and Closeout

3.5.1 Introduction

This section describes those safety-basis-related activities that are accomplished after the final design and Preliminary Documented Safety Analysis (PDSA) are approved and before approval to operate is granted. The primary project activities that can occur in this project interval include construction and transition to operations. The primary safety basis activities include preparing the Documented Safety Analysis (DSA) and Technical Safety Requirements (TSR), review and approval of these by DOE, implementation of the commitments in the DSA and TSR, and verification that those requirements are met before normal operations begin. If not previously approved, a facility Unreviewed Safety Question (USQ) procedure is also prepared and submitted for DOE approval.

3.5.2 Construction

Construction of the project design requires close coordination and integration of the various physical, contractual, technical, financial, and organizational interfaces. Numerous changes to the "final" design can occur during construction, some of which may affect the assumptions, commitments, or results of the safety analysis. Therefore, rigorous configuration management of the design and the safety analysis documentation is important to understand whether a design change can affect the approval basis for the PDSA, and to maintain consistency between the as-built facility and the safety basis documentation (DSA and TSR). Section 6.4 provides guidance on managing changes that affect the PDSA. In some cases, pre-existing SSCs or "government furnished equipment" (GFE) are provided to the project for use in the facility, creating the potential for additional challenges. Section 8.3 contains guidance and recommendations on the use of GFE.

3.5.3 Development of Safety Basis

Development of the DSA and the TSR (or revisions as appropriate for a major modification) begins in this phase. The DSA evolves from the PDSA with the addition of the final analysis of operational hazards and any upset conditions that were not considered previously. Safety Management Programs (SMPs) are detailed in this document, and elements of those programs that are needed in hazards analyses and other upset events are defined in the appropriate hazards analyses. Guidance for development of an operational TSR is contained in DOE G 423.1-1.

The DSA for a new facility documents a design, and its associated safety design basis, that has been approved by DOE as part of the Conceptual Safety Design Report (CSDR), Preliminary Safety Design Report (PSDR), and PDSA approval process. The DSA also documents any changes that were necessary during the construction phase for future operational reference and review and for approval of annual updates.

Additional analysis tasks that may be needed to prepare the DSA include evaluation of equipment that was not part of the preliminary and final design, such as government furnished equipment (GFE) or specialty equipment designs that were performed in separate design activities not fully addressed in the PDSA, and detailed operational analysis for those activities that did not need to be considered for development of the design. In addition, hazards analyses that were completed as part of the PDSA must be reviewed to ensure that they remain accurate and that changes are made as necessary. Note that, ideally, GFE should be included in the early hazard and accident analysis activities and should be treated in the hazard and accident analysis as though it were part of the design. Otherwise, the design interfaces (and potentially acceptability of the GFE) may not be found in a timely fashion. This additional task would be a final check on interfacing facilities or systems that are not under the direct control of the project.

To complete the operational hazards analyses and analyze other upset conditions that were not developed in the PDSA, the hazards analysis process should engage the operations staff. Detailed operational concepts should be developed by the operations staff in conjunction with the safety analysis efforts and should include GFE that may be used in these operations.

The DSA cannot be completed until there is a high degree of certainty that facility configuration matches the design documentation, safety design basis documentation, and the operating procedures for that configuration. Final verification that the DSA information is consistent with the as-built configuration is necessary before sending the DSA and TSR to DOE for approval. A rigorous configuration management program (including change control) will help in this regard.

The final development of the DSA and TSR should provide for implementation planning. The initial planning for these activities should be included in the Transition Plan, which should be baselined during final design. The Transition Plan provides the concepts that support when and how many operations staff are brought into the project to support transition and defines (to the extent known at the time) the activities that need to be performed, including those needed to implement the commitments expected to be in the DSA and TSR. Many of the details of activities needed to implement the DSA and TSR are based on limited information available in the preliminary design. Consequently, the detailed strategy and activities needed to implement the DSA and TSR need to be addressed and compared to the baseline in the Transition Plan such that appropriate adjustments can be made.

Additional adjustments may be required based on the DOE Safety Evaluation Report (SER) for the facility operational safety basis and other transition activities.

3.5.4 Checkout/Acceptance, Testing and Commissioning

The final stages of the project process involve acceptance and turnover of the SSCs from the construction effort to the operating organization. Acceptance is generally predicated on appropriate checkout/acceptance, testing, and commissioning. Planning for these activities should occur at early stages of the project and be coordinated with the operating organization to facilitate an efficient, timely turnover to ensure functionality of the safety SSCs.

Testing serves to verify that the components, systems, and facilities meet or exceed design requirements and performance parameters and helps to train operating personnel in the operation of the equipment, systems, and other components of the completed project. Key activities include the preparation and approval of test procedures, and the organization of test teams. Procedures are prepared by personnel who are or will be part of the test teams. Staff from the operator organization is also part of the test teams. The project organization works closely with the user in developing and presenting specific process and facility related training, and continues to provide support to the operations and maintenance staff throughout transition and turnover.

Early turnover and transition activities include facility walkdowns to identify and correct physical, process, safety, quality, or environmental deficiencies; and planning, preparation, performance, and documentation of equipment and systems testing and operation. Checkout and test planning and preparation typically begin at the equipment (item) level, progress to the system level, and culminate at the facility level. Test planning begins during design to ensure that the physical features needed to support testing are provided.

3.5.5 Readiness Reviews

Readiness reviews are performed to ensure that contractor programs, equipment, and personnel are ready to safely start up and operate the facility. DOE Order 425.1C, *Startup and Restart of DOE Nuclear Facilities*, defines the requirements for conducting either an Operational Readiness Review (ORR) or a Readiness Assessment (RA) for nuclear facilities. Readiness reviews may also be performed for non-nuclear facilities at the discretion of DOE.

3.5.6 Project Closeout

When construction, testing, and turnover are complete and the operational capability has been attained, the project is ready for Critical Decision-4, Approve Start of Operations or Project Closeout. A key part of obtaining Critical Decision-4 is the delivery of appropriate project related documentation to support the initiation of operations. The key discriminator in the turnover is the operational organization's readiness for assuming operational responsibility and the government acceptance of the asset.

4.0 HAZARD AND ACCIDENT ANALYSES

This chapter provides guidance on hazards and accident analyses as the design process progresses from scoping analyses in pre-conceptual design to the PHA and DBAs in conceptual design, system and process-level hazards analyses in preliminary and final design and the related identification of needed safety functions, and the selection and classification of safety structures, systems, and components (SSC).

4.1 Pre-conceptual Planning Phase

A scoping analysis of potential hazards should be performed during the pre-conceptual planning phase to plan for the conceptual design phase. The scoping analysis is important for the development of DOE expectations for Safety-in-Design.

There may be a wide range of maturity with respect to the definition of potential projects. In some cases, information available or developed may have target cost ranges identified and scope defined. In other cases, only rudimentary information on project plans and mission may be available. Knowledge of hazards will be dependent on maturity of the potential project.

Scoping hazard analysis during pre-conceptual planning involves a qualitative assessment of the facility/process risks in conjunction with any facility and initial technology selection alternative reviews performed. During and after the facility and technology selection process, project technical staff, in conjunction with nuclear safety project personnel, should evaluate the need for safety functions and associated hazard controls that may be required given the nature of the hazards. The initial determination of hazard controls that may be required is based on the qualitative assessment of the facility hazards and a preliminary determination of the approach to be taken to satisfy the defense-in-depth requirements of DOE O 420.1B. At this phase, only the major hazard controls that will have a significant influence on the facility design and cost need to be identified. The results of the initial hazards assessment, including a discussion of the overall major Safety-in-Design strategies and DOE safety expectations, are documented in support of the Mission Need Statement, commensurate with the level of detail available during pre-conceptual planning.

4.2 Conceptual Design Phase

A formal, disciplined evaluation of the potential facility hazards must be performed during the conceptual design phase. The design information available at this phase will be limited and may involve several design alternatives, but this effort is needed to perform a preliminary identification of the required safety functions, as well as to identify a preliminary set of Safety SSCs. The hazards analyses performed in this phase include a PHA and identification of events warranting designation as design basis accident analyses (DBA).

Early identification of safety SSCs (particularly those that could have high cost or schedule impacts) is a major contributor to developing an accurate estimate of facility and project costs. The hazards analyses establish the foundation for identifying the safety SSCs. At the conceptual design stage, this is achieved through hazards identification, hazards evaluation, and identification of major safety functions necessary to provide adequate protection, primarily for accident conditions. Safety SSCs are then chosen that will satisfy those safety functions for the preferred alternative. Identifying and classifying the safety SSCs (safety class and safety significant SSCs) is a fundamental part of the Safety-in-Design process.

Safety-in-design considerations for safety SSCs and defense-in-depth or important to safety SSCs (SSCs that perform a safety function but are not classified as Safety Class or Safety Significant, see DOE G 421.1-2 section 5.3., Hierarchy and Selection of Control Items) should be communicated to the design staff in a timely fashion. Similarly, the Integrated Project Team (IPT) and Safety Design Integration Team (SDIT) need to be cognizant of the design concept as it evolves to ensure that safety considerations are factored into each design decision.

Control strategies for DBAs must also be clearly identified in the hazards analysis, including the following:

- required safety functions and classifications;
- SSCs required to perform these functions; and
- natural phenomena hazard (NPH) performance categories (non seismic NPH) and seismic design bases for major SSCs.

Because preliminary cost and schedule baseline ranges being developed are strongly influenced by the selection of the hazard controls (and by NPH design requirements), the hazards analysis process used to arrive at these controls needs to be thorough and based on sound safety principles. To ensure that the baseline range estimates are conservative, the hazards analysis process and the criteria for selection of safety SSCs must also be conservative.

After the preliminary process flow diagrams are prepared, the facility design should further evolve before the formal hazards analysis documentation in the PHA is completed. Ideally, the project decisions and design documentation that should be drafted during the conceptual design phase and that are necessary for the formal hazards analyses during the conceptual design phase are as follows:

- facility site/location selection;
- general arrangement drawings;
- MAR estimates or assumptions and material flow balances;
- sizing of major process system containers, tanks, piping, and similar items;

- process block flow diagrams or equivalent documentation of the required major process flow steps and their sequence;
- preliminary one-line diagrams for ventilation, electrical power and distribution, special mechanical handling, and instrumentation and control system architecture;
- summary process design description and sequence of major operation; and
- confinement strategy.

Making the decision on the facility location will simplify the analysis process; however, the hazards analysis might also be a factor in site selection. If the site has not been selected around the time of inception of conceptual design, the analyst should either use bounding conditions or worst-case assumptions or perform a parametric comparison of the hazards involved at each potential facility site location. Such analyses increase the uncertainties in the Risk and Opportunities Assessment.

The hazardous material release events must be evaluated more formally in a PHA and facility-level DBAs for the selected alternative design. Development of the PHA during the conceptual design phase is an iterative process, and the PHA should evolve to include consideration of more refined design details as they become available. A strong PHA developed during this phase is the foundation for an effective Safety-in-Design approach for the project.

The PHA must be based on the following:

- project decisions and documentation described in this section;
- material-at-risk (MAR) quantities; and
- key project assumptions and strategies identified in the project SDS.

During the conceptual design phase, an objective of hazards analyses is to identify high-cost safety functions and design requirements (including those for NPH protection) for the SSCs that will be included in the project. Examples include the following:

- building structure;
- building and process confinement;
- power systems, including those associated with single failure criteria for safety class SSCs;
- fire protection provisions; and
- special mechanical equipment (e.g., gloveboxes).

The PHA must establish a suite of facility DBAs to define f functional and performance requirements for the facility design. This is facilitated by grouping the hazardous release events according to the nature of the postulated initiating events. One such grouping is shown below.

- **Internally Initiated Events**
  - **Fire –** Consequences are typically due to inhalation or ingestion of released hazardous material.
  - **Explosion –** Consequences are typically due to inhalation or ingestion of released hazardous material.
  - **Loss of Containment/Confinement –** Consequences are typically due to inhalation or ingestion of released hazardous material.
  - **Process Upsets –** Consequences are typically due to inhalation or ingestion of released hazardous material.
  - **Inadvertent Nuclear Criticality –** Consequences are typically due to direct external exposure from the event with potential for additional direct exposure from, or inhalation of, fission products.
- **Externally Initiated Events –** Consequences are typically due to inhalation or ingestion of released hazardous material. Depending on the specific event, direct exposure may also be applicable.
- **Natural Phenomena Hazards Initiated Events –** Consequences are typically due to inhalation or ingestion of released hazardous material. Depending on the specific event, direct exposure may also be applicable.

The categories of hazardous release events identified in these groupings essentially form the foundation for the facility level DBAs. The DBAs considered in the hazard analysis represent the range of potential accidents for the facility processes, and the results of that analysis must be used to identify the controls needed to protect against these accidents, considering both the public and collocated workers. All accident conditions (energy sources, intermediate process hazards, and similar conditions) must be considered.

The DBA analysis must ultimately address applicable accident environmental conditions for which the safety SSCs need to be designed to withstand and perform their safety function. These design basis conditions, together with the bounding consequences of an unmitigated release, provide the basis for selecting safety class and safety significant SSCs and their functional and performance requirements. (See Appendix A, “Safety System Design Criteria,” and Appendix B, “Chemical Hazard Evaluation.”)

Once the safety SSC functions are identified in the PHA (including the set of DBAs), the design team translates them into conceptual designs (e.g., drawings and initial system design descriptions). These conceptual designs are then the basis for cost estimates for the project.

In the conceptual design phase, the hazardous release event evaluations are based on facility-level events and are not a complete listing of all events possible in the facility. At the conceptual design stage, facility-level DBA are characterized by locations and quantities of MAR and gross descriptions of events that could result in a release of MAR (fires, explosions, spills, NPH events). The purpose of these facility-level

DBA, at this stage is primarily to classify safety functions, Performance Categories, and Seismic Design Categories for safety features that could provide those functions. The events evaluated should be chosen by the SDIT to ensure that the hazards considered and the safety features selected provide a reasonably conservative perspective of the high-risk/high-cost design requirements for the project. It is critical that the full SDIT be involved in the development of the PHA to ensure complete consideration of accidents and events, as well as design features to prevent or mitigate releases, to the degree practicable at this phase. (See Chapter 2, "Project Integration and Planning," for additional details on team involvement expectations.)

Due to the critical nature of the PHA process in defining the MAR release events and associated safety systems, it is important that certain key information is developed and described for each event postulated for use by the project team. Appendix G, "Hazard Analysis Table Development," provides detailed guidance on what should be discussed for each MAR release event postulated by the IPT.

Although many process details will not be available to perform a PHA during the conceptual design phase high-level events, such as fires, explosions, deflagrations, and NPH events, should be evaluated commensurate with the available process definition of MAR locations. From these evaluations, reasonably conservative prevention and mitigation strategies, along with the appropriate functional classifications and safety functional requirements, should be developed.

For those events with consequences that do not lead to selection of safety class or safety significant controls, the analysis should also identify the controls that are appropriate for collocated worker and public defense-in-depth protection. Hazard controls other than safety class or safety significant are identified in the conceptual design phase to the extent necessary to identify cost-dominant SSCs. These controls may be included to meet requirements defined by safety management programs and other administrative programs. Appendix A of this Standard provides criteria for classification of SSCs for radiological hazards. Additionally, prevention/mitigation strategies must be identified for chemical hazards. Guidance for chemical hazards is provided in Appendix B of this Standard.

Information from the PHA, as well as any uncertainties related to necessary hazard controls, is considered in the Risk and Opportunity Assessment so that appropriate cost contingencies and mitigation strategies for the items can be presented in the final Conceptual Design Report (CDR) and in the Conceptual Safety Design Report (CSDR).

A project design review occurs during the conceptual design phase. The results of the PHA are included in the conceptual design and must be included in this review. For example, before selecting alternatives, the PHA should identify top-level safety requirements, provide a basis for the classification (unmitigated consequence analysis to help define whether safety class SSCs are needed), and identify uncertainties such as those associated with multiple sites.

The events postulated and the safety strategies selected in the PHA provide the foundation for the development of the CSDR. The PHA also provides the foundation for performing the HA for future design phases of the project.

4.3 Preliminary Design Phase

Hazard analysis effort during the preliminary design phase includes the following:

- updating the facility hazard categorization (if needed);
- updating the analysis of the DBAs analyzed in conceptual design to confirm the selection of facility-level hazard controls and their functional classifications;
- developing a system-level HA and selecting and classifying hazard controls for the in-facility worker; and
- considering beyond-DBA events.

The objective for hazard analyses during the preliminary design phase is to confirm and add detail to the conceptual design stage analyses, including developing functional requirements and performance criteria for safety SSCs for in-facility worker hazards and identifying Specific Administrative Controls (SAC) (See DOE-STD-1186-2004). SACs should only be selected if engineered controls cannot be identified or are not practical.

The hazard analysis performed during the preliminary design phase is the system-level HA.

Prerequisites for the HA include developing or updating the information from the PHA during conceptual design, including the following:

- facility general layout drawings;
- Process and Instrumentation Diagrams (P&IDs);
- updated process flow sheets;
- electrical one-line diagrams; and
- updated listing and locations of material at risk.

The HA must:

- address the spectrum of accidents that may impact design and which may be initiated by facility operations, natural phenomena, and external man-induced events;
- evaluate potential accident consequences to the public and workers; and
- identify and assess associated preventive and mitigative features, including classification (i.e., safety class, safety significant, and SACs based on the significance of possible consequences).

The results of the HA provide an appropriate comprehensive evaluation of the complete facility hazardous event scenarios and accident spectra necessary to define the design. *Guidelines for Hazard Evaluation Procedures*, *Second Edition with Worked Examples* provides examples of some of the techniques that can be used to produce a well-reasoned and clear assessment of facility hazards and their associated controls. The HA considers the complete accident spectrum. However, at this design stage the HA only provides a preliminary definition of accident sequences and assumptions. The results of the HA are documented using the format and content guidance in Appendix G “Hazards Analysis Table Development”.

A graded approach should be used for the HA based on the magnitude and complexity of the hazards of the facility. The graded approach should also be used to select techniques for hazard analysis. The technique selected will be sufficiently sophisticated or detailed to provide an appropriately comprehensive examination of the hazards associated with the facility given the complexity of the operation and degree of design maturity. *Guidelines for Hazard Evaluation Procedures*, *Second Edition with Worked Examples* contains guidance on some of the techniques that may be appropriate for HAs specific to the application and process.

On the basis of the HA and the updated DBA analyses, a suite of SSCs must be selected and classified as safety class, safety significant, defense in depth or important to safety SSCs for the protection of in-facility workers, collocated workers, and the public. The DBA analysis also provides accident environmental conditions that safety SSCs need to be designed to withstand and continue to perform their safety function. Accident analyses are inherently graded in terms of the degree of physical modeling and engineering analysis needed to quantify accident consequences. The analysis to determine accident environmental conditions is generally included as part of the design process and may be documented as calculations separate from the safety documentation. Design details for safety SSCs must be developed that incorporate design requirements derived from the HA, the updated DBA analysis, and DOE O 420.1B.

The hazard analysis must also indicate whether a facility contains significant chemical hazard(s) that necessitate DBA analysis for consideration of SSCs for safety significant classification (see Appendix B).

The safety basis provisions of 10 CFR 830 require considering the need for analysis of accidents that may be beyond the design basis of the facility to provide a perspective of the residual risk associated with the operation of the facility. It is prudent to examine beyond DBAs at the preliminary design phase to provide insight into the possibility of additional facility features that could prevent or reduce severe beyond DBA consequences. They also serve as the bases for cost-benefit considerations for additional safety design provisions related to these postulated accidents. No lower limit of frequency for examination is provided for beyond DBAs. However, as frequencies become very low, little or no meaningful insight is attained. Beyond DBAs are not expected to be analyzed to the same level of detail as DBAs, and are not evaluated for man-made external events.

4.4 Final Design

During this phase, the DBAs are revised to reflect any changes that are design dependent (such as a change in the planned location of a structure resulting in different potential impacts from collocated facilities). In addition, during this phase analyses that support final classification of safety significant SSCs and demonstrate the adequacy of the control suite (engineered features with necessary SACs) are finalized.

The major new safety analysis activity in this phase is completion of the safety analysis. The completed safety analysis demonstrates the adequacy of the design from the safety prospective. As with the design, it is not necessary to show the progression of the design that led to the final choices, only the final choices, and the justification for their adequacy. The Preliminary Documented Safety Analysis (PDSA) guidance in Appendix I discusses how this information is applied to support the completion and documentation of the safety analysis.

At the final design phase, the safety analyses must encompass the scope of the design and demonstrate that the designated safety SSCs are adequately designed to reliably perform their intended safety functions. For system and component design, adherence to national codes and standards, in accordance with DOE G 420.1-1, -2, and -3 must be used to demonstrate that the design criteria have been met. Many of the design criteria are qualitative in nature and require an analysis to show how they are applied to a particular SSC. Demonstrating compliance with the requirements of these standards will be an important review consideration during acceptance of the safety documentation and during readiness activities in support of the CD-4 milestone.

If the requirements of applicable standards were tailored, a justification that demonstrates the adequacy of the final design with the tailored requirements must be documented. A System Design Description may be used to capture and maintain such information.[5] As the design progresses, design reviews should be used to validate the selection of criteria, application of codes and standards, deviations, and design output.

To provide a baseline understanding of the adequacy of controls, the accident analysis in the PDSA must describe how the selected controls adequately prevent and mitigate the accidents, including how the controls provide defense-in-depth. The discussion puts the effectiveness of hazard controls into accident context and provides the baseline safety analysis for the evaluation of changes, for example, under the Unreviewed Safety Question (USQ) process, for the operational period.

The development of safety design analysis information is important to the design progression. In many instances, the results will define design requirements for the procurement of safety materials or components. These design requirements represent

[5] See DOE STD 3024-98, *Content of System Design Descriptions*.

important quality assurance attributes that must be objectively demonstrated and should be tied to the procurement specifications. For example, a process control system may be selected as a safety system during the safety-design evolution. Once selected, the control system must be demonstrated to be capable of performing its safety function under all postulated process upsets or accidents as credited in the accident analysis.

Example

A process control system may be selected as a safety system during the safety-design evolution. Once selected, the control system must be demonstrated to be capable of performing its safety function under all postulated process upsets or accidents as credited in the accident analysis.

Specifically, the design of a control system based on pressure instrumentation for some specified system transient must factor instrument uncertainty into the system response. If the system must operate following a postulated pipe break in its physical area, the instrumentation must be shown to be able to withstand the pipe break consequences, typically by qualification testing.

Calculations are required to define the conditions for such testing. If the control system is deemed safety class and required to satisfy single failure criteria, Failure Modes and Effects Analyses (FMEA) or fault trees may be needed to ensure active single failures do not affect system function under postulated system faults. If the control system is required to function during and/or following a seismic event, not only must the system and its active components be demonstrated capable of withstanding the acceleration forces, but any SSCs not part of the system must be evaluated to ensure their failure cannot endanger the control system (target-source interaction analysis).

In this case, instrument uncertainty, environmental qualification parameters, single failure, and seismic target-source interaction, must be considered in the selection of the actual components for installation, and these requirements must be translated to the procurement specifications.

Typically, the final design concepts necessary to develop the PDSA are completed before the final design phase, but changes may arise during final design that result in the need to revise the PDSA. It should be recognized that the commitments and descriptions in the PDSA may change and adequate change controls will need to be established to accommodate this possibility.

Not all design issues related to safety may be resolved by the final design phase. Consequently, it may be necessary to identify where these issues remain open and describe the safety implications associated with them. This is particularly applicable for equipment, such as government furnished equipment (GFE) that will be procured by others in a later phase of the project. This ultimately translates to a project risk issue as well as a safety issue. These risks must be documented in the Risk and Opportunity Assessment.

5.0 NUCLEAR SAFETY DESIGN CRITERIA

As discussed in Chapter 4, the results of the Preliminary Hazard Assessment (PHA), the Design Basis Accident (DBA) Analysis and the identification of Safety structures, systems, and components (SSC) must be considered in the design process. After the appropriate facility location and processing alternatives have been selected, other safety design requirements and considerations must be specifically addressed during design development. These requirements and considerations are in DOE O 4201.1B in the following chapters:

- Nuclear and Explosives Safety Design Criteria (Chapter 1);
- Fire Protection (Chapter 2);
- Nuclear Criticality Safety (Chapter 3); and
- Natural Phenomena Hazards Mitigation (Chapter 4)

In addition, specific criteria or guidance for implementing these requirements are contained in the following:

- DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety*;
- DOE G 420.1-3, *Fire Protection and Emergency Services Program*;
- DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*; and
- DOE G 420.1-2, *Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Nonnuclear Facilities*.

Alternative safety design criteria may be proposed by the design contractor, as described in 10 CFR 830.206, but the alternative criteria must be approved by DOE.

The SDIT (or its functional equivalent) should review DOE O 420.1B, as well as its implementation guides and their referenced Standards, and should compile a listing of the applicable safety design requirements and associated guidance relative to each of the safety topics addressed in the above-listed chapters of the Order. These safety design requirements and criteria must be placed under design control with an expectation to demonstrate implementation at project end. As the design evolves, requirements will become more specific. The intent of engineering design control is to ensure safety design requirements and criteria are controlled throughout the design process and changed only with appropriate review, approval, and flow down of the change into the design and documentation. Control of safety requirements is a fundamental responsibility of the SDIT. Where no SDIT is formed, control of these requirements is the responsibility of the project safety lead. The project change control process must provide for concurrence by the Federal Project Director for changes to criteria invoked in the SDS. Derived requirements which implement these criteria are controlled wholly within the design control process.

The Conceptual Safety Design Report (CSDR), the Preliminary Safety Design Report (PSDR), the Preliminary Documented Safety Analysis (PDSA), and the Documented Safety

Analysis (DSA) must address, to the appropriate degree of design maturity, each of the safety design requirements and considerations in DOE O 420.1B (unless an alternate set of requirements has been approved by DOE) and identify the extent to which the design incorporates them. Where the design does not fully satisfy one of these requirements, the rationale must be provided.

Specific SSCs will have been identified in the conceptual design phase along with applicable DOE O 420.1B criteria. As design evolves, specific design codes and standards to be used for the design of the safety SSCs will typically be identified during Preliminary Design. Guidance for mapping between the safety functions and the selected safety SSCs and applicable design codes and standards is provided in the guidance documents listed above for DOE O 420.1B. The linkage between safety requirements and the design codes and standards should be provided at a high level in the safety documentation (see H.2 6. and I.2 Appendix B).

If the codes and standards chosen for the safety functions and safety SSCs differ from those identified in the DOE requirements cited in this section, the rationale for the selection of alternate codes and standards must be provided. The PSDR is generally the first place where a linkage to the specifics of the alternative selection and rationale in a document such as the Design Criteria Document is provided. The PSDR should summarize and reference the document that contains this information.

Demonstrating compliance with the requirements in DOE O 420.1B generally involves a design analysis or series of analyses. For example, some safety SSCs are required to be designed to withstand common cause effects and adverse interactions from natural phenomena hazard (NPH) events. The design analyses must demonstrate that those safety SSCs that are required to function before, during, or after the NPH event will continue to do so. This may entail evaluation of a number of nearby or overhead SSCs that perform no direct safety function. Design documentation to demonstrate this requirement for "source SSCs" may involve design criteria for the facility or system and calculations demonstrating acceptable seismic design. Each applicable analysis for a project should be considered as important technical basis information that is to be maintained in support of the safety basis for the life of the facility.

During design, material in Type B containers with current certificates of compliance may be excluded from the inventory for final hazard categorization, when safety analyses demonstrate that containers can withstand all accident conditions.

6.0 SAFETY REPORTS

6.1 Safety Input to the Conceptual Design Report

DOE O 413.3A, Chg 1, requires developing a Conceptual Design Report (CDR) during the conceptual design phase. The CDR is intended to provide the Approval Authority with integrated information sufficient to understand the overall project scope and cost, the risk and opportunities, and the cost range for the selected conceptual design. The CDR for the selected conceptual design must incorporate an effective Safety-in-Design approach to address potential material-at-risk (MAR) release events. DOE O 413.3A, Chg 1, and its guidance establish the minimum content for the CDR, which summarizes the project requirements and the proposed design solution. The CDR is a necessary element in decision-making because it documents the following:

- project design requirements;
- alternatives evaluated and selected for facility and the process configurations;
- design architecture (major structures, systems and components [SSCs]) selected to satisfy the design requirements, consistent with the selected alternatives; and
- safety design basis for the proposed facility.

Both the CDR and the Conceptual Safety Design Report (CSDR) provide the following:

- risk-informed decision making information for the DOE approval authorities; and
- equipment safety classifications and design requirements, as well as a corresponding cost range that reflects the Safety-in-Design decisions made during the conceptual design phase.

The CDR provides an integrated discussion of the key results of the hazards analysis including the following:

- facility hazard category determination;
- selected safety functions and controls;
- SSC functional classifications, performance categories, and seismic design criteria for natural phenomena hazard (NPH) protection;
- design criteria for the safety SSCs; and
- approach to be taken to further develop and document the safety basis through the remaining project phases.

In addition, the SDS must also describe any uncertainties with respect to the safety design basis assumptions and selected hazard controls, and explain how the risks associated with these uncertainties will be managed.

6.2 Conceptual Safety Design Report

DOE O 413.3A, Chg 1, requires a CSDR as a part of the approval package for CD-1. The purpose of the CSDR is to summarize the hazards analysis efforts and Safety-in-Design decisions incorporated into the conceptual design along with any identified project risks associated with the selected strategies. Appendix H provides specific guidance for preparing the CSDR.

DOE must review the CSDR and document the review in a Safety Validation Report to confirm that the preliminary safety positions adopted during conceptual design constitute an appropriately conservative basis to proceed to preliminary design. These positions include the following:

- selection of the preliminary hazard categorization (HC-1, 2, or 3) of the facility;
- preliminary identification of facility Design Basis Accidents (DBA);
- assessment (based on the analyses of DBAs) of the need for safety class and safety significant facility-level hazards controls;
- preliminary assessment of the appropriate seismic design criteria for the facility; and
- position(s) taken with respect to compliance with the safety design criteria of DOE O 420.1B or any alternate criteria proposed.

6.3 Preliminary Safety Design Report (and PDSA)

The key Safety-in-Design documents developed during the preliminary design phase are the Hazards Analysis (HA) and the Preliminary Safety Design Report (PSDR). The format and content of the PSDR are designed to be built upon to produce the Preliminary Documented Safety Analysis (PDSA) during the final design phase. The format and content guidance for the PDSR are provided in Appendix I of this Standard. The PSDR addresses the following Safety-in-Design aspects for the Preliminary Design Phase:

- site information of the type that can affect Safety-in-Design (e.g., location of nearby facilities and external hazards, meteorological information for dispersion analyses, seismic and other natural phenomena information);
- facility and process descriptions, including facility structure types and layout, process description and flow sheet, and summary system descriptions for safety SSCs, consistent with the level of design;

- summary of the HA, including process hazards evaluation, selected DBAs; FHA, selected safety SSCs and their safety function; functional classification; and required seismic and other natural phenomena design criteria, including their bases;
- for safety class and safety significant SSCs and Specific Administrative Controls (SAC), the functional requirements and performance criteria (including applicable design requirements from DOE G 420.1-1 and DOE G 420.1-2);
- information regarding aspects of the preliminary design that are required to support the prevention of inadvertent criticality;
- roadmap of project documentation addressing design aspects related to the effective implementation of safety management programs; and
- documentation of how the safety design criteria of DOE O 420.1B are met, including any exceptions or alternate approaches, which may include analyses performed to meet the safety analysis expectations.

Based on the design maturity in preliminary design, the PSDR will demonstrate the adequacy of the hazards analyses and the selection and classification of the hazard controls, including consideration of the application of the principles associated with the hierarchy of controls. If the commitments made in the PSDR and design documents are met, the result should be a final design and a constructed facility that could be approved for operation without major modifications. The PDSA at the final design stage is an evolution of the PSDR.

6.4 Change Control for Safety Reports as Affected by Safety-in-Design Activities

A clearly defined project configuration should be established at the conclusion of each phase of the design. DOE-STD-1073-2003, *Configuration Management*, states: "The objective of change control is to maintain consistency among design requirements, the physical configuration, and the related facility documentation, even as changes are made." At the conceptual design stage, change control should be implemented within the design organization to maintain consistency among the various concepts and their supporting documentation. The CSDR issued at the completion of the conceptual design must reflect the project configuration as described in the conceptual design. Critical relationships between safety and the concept that progresses to the final design are established in the CSDR.

As the conceptual design evolves to the preliminary design, it is documented in a PSDR. The PSDR must specifically identify any changes to Safety-in-Design decisions and commitments that were described in the CSDR and must provide explanations for the changes. Similar identification of changes and explanations must be provided between the PSDR and the PDSA.

As the preliminary design progresses to the final design, the PSDR evolves into the PDSA with its attendant supporting safety analyses, which have been formalized relative to earlier evaluations. The approved PDSA constitutes the basis upon which DOE agrees that procurement and construction may begin.

PDSA configuration baseline documents should be identified within the project baseline. The PDSA configuration baseline is the basis for determining if PDSA revision is needed, and formally establishing and maintaining the PDSA configuration baseline provides the means to ensure that the Department can continue to rely on the information in the PDSA.

Not every change in the PDSA configuration baseline will necessitate a PDSA revision. The following criteria are suggested to determine whether a PDSA revision is needed because of post-PDSA approval design changes.

- The change alters a safety function for a safety SSC identified in the current PDSA.
- The change results in a change in the functional classification, reliability, or rigor of the design standard for an SSC previously specified in the PDSA configuration baseline.
- The change requires implementation of new or changed safety SSC or proposed Technical Safety Requirement (TSR) controls.
- The change significantly alters the process design or its bases, such as increased material at risk, changes to seismic spectra, major changes to process control software logic, new tanks, new piping, new pumps, or different process chemistry.

7.0 SAFETY PROGRAM AND OTHER IMPORTANT PROJECT INTERFACES

There are multiple interfaces with required programs and project evolution steps that link with the Safety-in-Design process. The intent of this chapter is to highlight the links where these areas, particularly Safety Management Programs (SMP), which are required to be addressed in sections 6 through 17 of the Documented Safety Analysis (DSA), directly interface with the design process; specifically, where they link to the development of safety design bases. This chapter is not intended to provide comprehensive explanations because the subject matter is addressed in detail in other DOE documentation. Table 7-1 shows the typical activities associated with these SMPs for each project phase.

For new facilities that will be built at existing DOE sites where SMPs have been established, much of the interface with the DSA will be similar to that for existing facilities. Exceptions may occur where new classes of hazards are introduced. For new sites, the development of SMPs should be a focus of management attention early in the project life cycle, and these programs should mature as the facility heads toward operational capability.

Most of the sections in this chapter involve aspects important to design, and consideration of them should be integrated into the design effort as early as it is practical to do so. Among these are emergency preparedness, radiological protection, nuclear criticality safety, fire protection, human factors, and security. Further discussion on this integration is provided in the following sections, and Table 8-1 shows actions relating to them as a function of design stage.

7.1 Quality Assurance

The quality assurance (QA) requirements of 10 CFR 830 and DOE O 414.1C apply to DOE nuclear facilities and activities. The scope of the QA rule is defined in 10 CFR 830.120 as follows:

> This subpart [Subpart A of 10 CFR 830] establishes quality assurance requirements for contractors conducting activities, including providing items or services, that affect, or may affect, nuclear safety of DOE nuclear facilities.

This wording was specifically chosen to include activities in the design and construction phases before completion of the facility and introduction of nuclear material. That is because the quality of the design and construction is integral to the safe operation of the facility.

Furthermore the inclusion of a robust QA program in the design and construction phases can greatly strengthen the ability to achieve the goals of Safety-in-Design, namely to identify and correct problems early in the design and construction phases when it is more cost-effective to make corrections. With respect to the activities defined in this Standard, QA should be viewed as an important tool. The successful completion of many nuclear facilities has occurred simply because of the quick response to QA findings during design and construction.

In particular, the following QA activities can help keep the design process on track.

- Establishing and using formal work processes such as design reviews, document control, verification processes, and configuration management.
- Training of design and review staff on applicable standards, requirements, and work processes.
- Performing periodic assessments of the documentation, including drawing reviews, to ensure that the drawings, design calculations, and other documents are in agreement. Key design and construction personnel should be involved in these reviews.
- Performing independent design verifications, validations, assessments and design outputs by qualified persons to keep design and analysis errors to a minimum.
- Identifying problems that occur in the design process, determining the root cause and taking timely corrective actions, both immediate and long term.
- Developing and using approved vendor lists to ensure quality products.
- Periodically evaluating the approved vendors to ensure their quality has not degraded; and, if it has, examining the products already supplied to ensure they are adequate.
- Controlling documents and drawings, as well as changes to them, to approved processes.
- Ensuring the quality of safety software used for design activities.
- Identifying and controlling design interfaces.
- Periodically meeting with vendors to ensure safety components can in fact be constructed and function consistent with design specifications without unconsidered exceptions.

Ultimately, the safety documentation must be validated against approved design outputs. The iterative nature of the safety and design processes demands a more flexible change control process at this stage, but ultimately design outputs must be controlled under the applicable configuration management plan. DOE-STD-1073-2003, *Configuration Management*, Section 3.9, discusses activities that should be initiated during design to ensure a smooth turnover from design to construction.

DOE O 413.3A, Chg 1, requires that quality assurance begins at project inception and continues throughout the project's life cycle. Consistent with that requirement, DOE O 413.3A, Chg 1, also requires that a quality assurance program (QAP) (compliant with 10 CFR 830, Subpart A, and DOE O 414.1C) is approved in CD-1 and updated and continuously applied throughout the project's life cycle. The QAP describes the planned quality related activities, surveillances, and assessments and should be developed in the project conceptual phase and updated as the project matures.

DOE and commercial nuclear industry QA experience highlight the need to specifically consider:

- tracking and verification of assumptions from the safety analysis or design to operational acceptance;
- appropriate translation of inspection and test requirements for installation verification or safety SSCs;
- use of subcontractors with recent experience with nuclear QA; and
- documentation of safety SSC inspections and tests.

The project Quality Assurance Program (QAP), established at the project's inception, will guide QA activities for the project. Appropriate assessments of the safety analysis and design process are planned and completed consistent with the project QAP.

DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830, Subpart A*, and DOE O 414.1C are of special relevance with regard to design activities.

7.2 10 CFR 851 Worker Safety and Health Program

The focus of the Worker Safety and Health Program Rule (i.e., 10 CFR 851) is as follows:

- provide a place of employment that is free from recognized hazards that are causing or have the potential to cause death or serious physical harm to workers; and
- ensure that work is performed in accordance with (i) all applicable requirements of this rule; and (ii) with the worker safety and health program for that workplace.

This commitment to providing a workplace that is free of recognized hazards adds a layer of attention to the hazard analysis and facility controls that goes beyond that required for the Preliminary Documented Safety Analysis (PDSA).

The 10 CFR 851 rule requires establishing a worker safety and health program that is approved by the Department. Two required areas of this rule that are of particular relevance to Safety-in-Design are fire protection and pressure safety. The rule invokes National Fire Protection Association (NFPA) requirements for fire protection and American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel code (BPV). These consensus standards are also typically invoked by DOE G 420.1-1 for safety-significant and safety-class systems and components, as well as DOE G 420.1-3 for all fire protection systems, regardless of safety designation. These standards represent design input into any new construction and potentially to major modifications.

Applicability of worker safety-related national consensus codes and standards should be recognized at the earliest stages of conceptual design and captured in appropriate requirements documents. As the design evolves into preliminary and detailed design, these codes and standards will drive certain areas of design.

The worker safety and health program should ultimately be reflected in the SMP chapters of the DSA. Worker safety programs specifically described in the DSA are Hazardous Materials Program, Occupational Safety (which includes fire protection), Emergency Preparedness, Management, Organization, and Industrial Safety Provisions. These areas are discussed in more detail below.

7.3 Fire Protection

A key interface during the early design phases is identifying the potential fire hazards and scenarios that can drive safety functional classification of fire protection SSCs (e.g., detection and suppression). Fire protection design includes the following elements: reliable water supply, noncombustible construction, fire-related barriers, detection systems, building contents, ventilation control, and automatic suppression systems. Design is developed through a competent and thorough FHA and interactions between the design team and fire protection SMEs. Design guidance for fire protection can be found in DOE G 420.1-3 and in DOE-STD-1066-99. Safety fire protection SSCs can represent a significant cost to the overall project and present special interface challenges between fire protection SMEs and safety analysis disciplines. A full understanding of the implications of fire protection selection is necessary to effectively implement such a strategy during detailed design. For example, selecting a confinement ventilation system that uses HEPA filtration necessitates considering potential particulate loading of the filters due to fire scenarios.

An FHA is required for all nuclear facilities or facilities that present unique or significant fire risks. An FHA requires a comprehensive evaluation of fire hazards, including postulation of fire accident scenarios and estimates of potential consequences (i.e., maximum credible fire loss). DOE O 420.1B requires the conclusions of the FHA to be integrated into the DSA. DOE G-420.1-1 encourages the initiation of the FHA early in the design process and suggests that this effort be closely coordinated with the safety analysis effort. The preliminary FHA and its conclusions should be addressed in the facility CSDR and PSDR in a manner that reflects all relevant fire safety objectives that could affect the facility safety basis. The FHA is typically coordinated and integrated through teaming of fire safety personnel with hazard/accident analysts, and any conflicts related to the FHA and DSA should be resolved as early in the design process as practicable. DOE-HDBK-1163-2003, *Integration of Multiple Hazard Analysis Requirements and Activities*, provides additional guidance.

The FHA provides fire protection strategy and protection schemes necessary to control or mitigate fire hazards to workers and the general public. Each stage of the project life cycle as indicated in Table 8-1 demonstrates how the FHA supports the design process. In the conceptual design, a preliminary FHA provides fire protection strategy alternatives for control or mitigation of accident consequences. Fire protection strategies will dictate design requirements. These design requirements will be evaluated as part of preliminary design. System-level hazard controls and classification are also developed and further refined. This includes other protection requirements, such as property protection and building code requirements.

Another important facet of fire protection is the code-based requirement for an Authority Having Jurisdiction (AHJ). For designs that do not comply with appropriate NFPA Standards, AHJ review and acceptance of design outputs relevant to fire protection and life safety are required. Appropriate interfaces with the AHJ should be anticipated and planned.

7.4 Infrastructure

Infrastructure considerations are critical to a project. It is important to identify infrastructure needs and existing capabilities or constraints as early as practicable in the design process. In this discussion, infrastructure includes all existing facilities and utilities that will interface or that may coexist with the new facility or modification to an existing facility. The infrastructure considerations include, but are not limited to the following:

- supporting utilities (e.g., water, steam, power, industrial gases);
- surrounding or collocated facilities;
- supporting organizations and SMPs; and
- interfacing facility (modifications).

Of particular interest is the identification of any constraints that may hinder project planning and execution. Equipment compatibility (e.g., electrical) constraints can arise when interfaces with an aged infrastructure are possible. Gas systems should be investigated to fully understand interconnections with surrounding facilities and for features relevant to the hazard analysis. Utility interfaces should be identified in both pre-conceptual and conceptual design. An important consideration is the ability of the utilities to support SC and SS systems such as fire sprinkler systems. In preliminary design, specific needs should be reconciled with the existing systems capabilities and capacities to support baseline cost estimation.

Surrounding or collocated facilities need to be considered in the early stages of the hazard analysis for conceptual design. Nearby facilities may present hazards (e.g., toxic or explosive gases) that must be considered in the hazard analysis as an external hazard. Provisions may be required within the planned facility to mitigate the effect of such events on personnel within the new facility. An analysis of the effects of nearby facilities should be completed in support of the Preliminary Safety Design Report (PSDR).

7.5 Nuclear Criticality Safety

Nuclear criticality safety (NCS) represents a specialized safety discipline. Given the significance of an inadvertent nuclear criticality, the presence of quantities of fissionable materials sufficient to sustain a critical reaction can determine the facility hazard categorization. Where there is sufficient fissionable material present, NCS controls can also result in safety significant functional classification of SSCs and, potentially, TSR controls. As a result, the NCS function must be represented on the project team and closely linked to the safety analysis effort from the earliest stages of project development. Criticality safety evaluations (CSE) must be integrated with the traditional safety analysis techniques to provide a comprehensive safety analysis. DOE has promulgated guidance for performing and documenting criticality safety evaluations in DOE-STD-3007-2007.

To support design development, it is important to develop fundamental design criteria to address typical criticality safety concerns (e.g., safe geometry) and to incorporate these criteria early in the design process. The purpose of these criteria is to avoid the use of cumbersome and inherently less reliable administrative controls. An example set of design criteria is provided in Table 7-2.

One of the most important criticality safety design features is to prevent, by design, natural phenomena initiators for criticality accidents (e.g. seismic and wind). In addition, the fire protection program at design will also drive criticality safety design requirements. The building code, Life Safety Code, national fire codes, and DOE directives almost always require automatic sprinkler protection and firefighting hose capability as well as suitable drainage for nuclear facilities. Unless exemptions and variances have been approved for automatic and manual fire suppression, the criticality calculations must take this moderator into account. For example, in a facility where sprinklers are planned, the criticality safety evaluations must consider the effects of introduction of water due to sprinkler activation. The presence of sprinklers will also tend to drive engineered controls for criticality safety to prevent water ingress to fissionable material containers, both in process containers and in storage. Criticality concerns could also result in a change from water-based sprinklers to an alternative gaseous suppression system, which could affect cost estimates. Therefore, there is a need for close cooperation between fire protection/fire hazards analysis and criticality safety early in design.

Criticality safety includes human interaction with the potential criticality hazard. Addressing human interaction issues typically results in administrative controls. Minimizing use of administrative controls in lieu of more reliable engineered controls should be a focal point for design. This also points to the need to identify criticality safety issues early in the design process and design the facility in such a way as to preclude criticality problems (e.g., provide storage appropriate for the types of materials, design systems that can be used by the operator in a way that ensures criticality safety, consider criticality potential when designing sprinkler systems and other fire protection). One specific aspect of NCS operations requiring early project definition is emergency response to criticality accidents.

Designs should strive to make a criticality accident a beyond extremely unlikely event. If that is not practical, the Double Contingency Principle requires control of two independent parameters (see DOE-STD-3007-2007). Deviations from the Double Contingency Principle must be specifically approved by DOE and typically results in layers of administrative controls. A singular focus of criticality Safety-in-Design should be to avoid the need for single parameter control in all processes where a criticality accident is credible.

7.6 Radiological Protection

Radiological controls to achieve As Low as Reasonably Achievable (ALARA) represent a fundamental design philosophy that is used at the earliest stages of design and which is a requirement of 10 CFR 835. Subpart K of 10 CFR 835 “Design and Control and Facility Design and Modifications,” provides key inputs into the design process. DOE G 441.1-1B, *Radiation Protection Programs Guide*, provides additional guidance for design, in Section 7.4 of that guide.

Radiological hazards will generally be considered as candidates for confinement or shielding strategies to minimize worker exposure. These strategies will evolve to design requirements through the project life cycle. In addition, detection or monitoring equipment is generally required to protect workers, the public, and the environment.

7.7 Human Factors

In the context of safety bases development, DOE-STD-3009-94, CN 3, defines human factors to consist of the following:

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

These two factors apply to the design in (1) the layout and design of SSCs for operation, construction, maintenance, and testing or surveillance; and (2) in the evaluation of failure probability of human relied upon actions. In some instances, these factors overlap (e.g., control room operator action).

The connection to the safety analysis is, in many cases, indirect in that, by including this philosophy, inadvertent human errors can be minimized. This is specifically important to ensure that administrative controls can be implemented within the facility.

Within the project life cycle, the human potential for error is effectively addressed through the hazards analysis process and industrial or programmatic safety programs that identify other opportunities to avoid error potential. This is a normal part of design evolution and should be factored into the design process as those human factors reviews occur over the life cycle (particularly through preliminary and detailed design stages).

Human factors for design should be established as a design philosophy early in the conceptual design phase. This philosophy should evolve to consider standard human interface issues. Many codes and standards reflect this approach, and it is inherent in the standards. It is also important to include operator input and reviews by maintenance and test personnel to ensure access for maintainability and testability.

7.8 Security

Some measure of security is required to be addressed for most DOE facilities. However, for a limited number of facilities, security drivers for the design and operations are a key consideration for the project. In these limited cases, security requirements can represent a significant cost driver. Security protection schemes may involve one or more of the following: designed structural protection for key resources or materials; adversary deterrence and delay; intrusion detection systems; and protective force resources. Aspects of the security scheme must be coordinated with the design as it relates to safety in a two key areas: (1) structural design and (2) inadvertent or accidental discharge of weapons or weapon systems.

The interaction between the project team and security personnel is needed to develop an integrated implementation involving both safety basis and security allowing achievement of the Design Basis Threat (DBT) objectives while ensuring safety is appropriately considered.

Where significant structural protective measures are warranted (e.g., special nuclear material storage or processing), Natural Phenomena Hazards (NPH) design and security measures may be used in a complementary manner; that is, major structural components may be designed to serve both functions and result in efficient use of resources. The key factor is obtaining the security requirements early in the project to coordinate with the NPH design.

Accidental discharges of security systems could initiate accidents such as hazardous material releases, fires, nuclear criticality, or damage to safety SSCs or process systems. As an initiator for an event, accidental or unintended discharge of weapons or deterrent systems could present a hazard to workers and the public, and must be addressed in the hazard analysis. These events could be caused by human error, faulty security system design, or internal or external hazards. There is also the potential for common cause effects on security systems that must be considered in the safety analysis. Some accident initiators that could actuate the security system and exacerbate accident consequences include facility events, such as fires, and seismic and other NPH events.

Given the rapid evolution of security requirements, security modifications in existing facilities could be candidates for consideration as a major modification. In that case, preparation of a PDSA and application of the nuclear safety design criteria of DOE O 420.1B will be required.

As safeguards and security has an independent set of directives that are implemented and the safety and security disciplines often use similar terms, it is important to clearly define the areas for which these two do not interface, as well as areas where interaction is needed. From the Safety-in-Design perspective, it is critical to address the interfaces and to clearly define when the protective measures implemented by the security system to meet the applicable requirements must be addressed by appropriate safety measures to ensure the safety and health of workers, public, and the environment. Interfaces with Safeguards and Security that are important to safety basis development include the development of Safeguards Requirements Identification (SRI), a Vulnerability Assessment (VA), and participation in the hazard analysis efforts.

There are no requirements to document security strategies within the DSA. However, security plans and vulnerability assessments are required in the security domain and these documents may be influenced by safety-driven interaction through the process.

7.9 Environmental Protection

The DOE National Environmental Policy Act (NEPA) process is a Federal process conducted in accordance with 10 CFR 1021, for identifying environmental impacts to support decision-making about a proposed action. The Integrated Project Team (IPT) needs to support this process. DOE O 451.1B, Chg 1, *National Environmental Policy Act Compliance Program*, establishes DOE internal requirements and responsibilities for implementing the National Environmental Policy Act (NEPA) of 1969, the Council of Environmental Quality Regulations implementing the Procedures Provisions of NEPA (40 CFR 1500-1508) and the DOE implementing procedures of 10 CFR 1021. The project should coordinate with the DOE Site and Operations Office NEPA compliance officers during the project initiation phase to ensure that the NEPA process is fully executed. NEPA documentation, consistent with design, should be developed as early as possible in the project acquisition process. In accordance with O 413.3A, Chg 1, the NEPA strategy and analysis are prepared during conceptual design. Final NEPA documents, including public involvement (if necessary) and resulting Record of Decision (ROD) or Finding of No Significant Impact (FONSI), must be issued prior start of final design.

The Project Team needs to identify all applicable environmental regulatory requirements. These include regulations issued by the Environmental Protection Agency and by delegated states pursuant to statutes such as the Clean Air Act, the Clean Water Act, and the Resource Conservation and Recovery Act (RCRA). Other requirements (relating, for example, to protection of endangered species, protection of historic and cultural resources, and others) may also be applicable. Permits may be required under some of these regulations, and planning for these permits needs to be incorporated in the project schedule. Most permits are applicable to facility operation, but some may be required prior to start of construction.

DOE O 450.1, Administrative Chg 1, *Environmental Protection Program*, and associated guides provide further information relative to environmental protection practices by which the DOE implements sound stewardship that is protective of the air, water, land, and other cultural resources impacted by DOE operations and by which DOE cost-effectively meets or exceeds compliance with applicable environmental, public health, and resource protection laws. DOE sites are required to implement environmental management systems, as part of their integrated safety management systems. The environmental aspects of the project should be reflected in the site's environmental management system prior to operation.

7.10 Hazardous Material

Similar to radiological hazards, DOE requirements invoke an ALARA concept for the protection of workers from hazardous materials. Design should support the primary objective of reducing the frequency, severity, and cost of incidents involving hazardous material, as well as the cost of hazardous operations. Prevention practices, such as substitution of less hazardous materials in a project or design of a process to reduce generation of hazardous waste, should be examined prior to consideration of protection strategies. Protection strategies will generally involve confinement strategies, such as gloveboxes, piped systems, and tanks, as well as administrative controls. The approach will typically be driven by the magnitude of the hazard and inventory.

Major hazardous materials, typically associated with process requirements, should be identified and considered within the safety strategy. The process design will identify and refine inventory or maximum anticipated quantities to support structure, system, and component (SSC) functional classification. Codes and standards to be applied should be specified for application in detailed design. Provisions for facility monitoring and protection instrumentation for worker protection need to be considered.

Further guidance is available in the DOE-HDBK-1139/2-2006, *Chemical Management* (Volume 2 of 3), "Chemical Safety and Lifecycle Management."

DSA Chapter 8, "Hazardous Material Protection," must incorporate the ALARA approach, the elements to provide hazardous material exposure control, and facility protection instrumentation.

7.11 Radiological and Hazardous Waste Management

Most processing facilities will generate waste. DOE-O-420.1B requires that facility process systems be designed to minimize waste production and mixing of radioactive and nonradioactive waste. Hazardous waste streams, including types, sources, and quantities should be identified early in the design and prevention practices, such as substitution of less hazardous materials in a project or design of a process to reduce generation of hazardous waste, should be examined to reduce management costs of these waste streams. Management strategies for these waste streams including storage and treatment and disposal systems must be described in the DSA. Any potential for accidental releases from waste handling and treatment systems should be addressed during the hazard analysis process in the preliminary and detailed design processes.

7.12 Emergency Preparedness

DOE O 151.1C and its accompanying guidance set, the DOE G 151.1-series, establish specific requirements and methods for the Emergency Management Program (EMP). Early integration of EMP considerations into the safety design process can provide opportunities to minimize the hazardous nature of operations and to improve the ability to respond if an emergency occurs.

There is much that can be gained in project integration between the EMP and the hazard analyses conducted for the safety analysis.

At the early stages in the project, only major hazards are likely to be known. EMP SMEs, designers, and safety analysts can work together to identify options that may be less hazardous. Incorporating instrumentation, hardware, and related requirements into the design can improve the ability to detect emergency situations during operations. Early recognition of an event is essential to enable potentially affected workers and the public to take actions to prevent or limit their exposure to hazardous materials. Provisions in the design may be appropriate to support recovery and re-entry.

The Emergency Planning Hazards Assessment (EPHA) for the EMP starts from the hazards analyses that support the safety design basis. The EPHA must include accident sequences where safety controls fail, as well as accidents that are beyond the design basis for a facility. DOE-HDBK-1163-2003 provides guidance for features of the EPHA that go beyond the scope of the hazards analyses that support design. EMP SMEs and project safety analysts should work together to define and analyze these scenarios.

7.13 External Reviews

The safety documentation development effort should anticipate and prepare for external interfaces and reviews. Periodic reviews are required by DOE project oversight. In addition, external reviews are conducted by DOE pursuant to nuclear safety rules (i.e., 10 CFR 830, 835). The principal DOE external safety design basis reviews and approvals will be of the Conceptual Safety Design Report (CSDR), Preliminary Safety Design Report (PSDR), and PDSA, and, of course, review and approval of the operational DSA and Technical Safety Requirements (TSR).

Periodic formal project reviews, particularly those at the major project approval stages, are required by DOE O 413.3A, Chg 1. The safety documentation development team should anticipate supporting these reviews. The team should expect focused reviews on safety functional classification determinations in relation to potential cost drivers for the project.

The Defense Nuclear Facility Safety Board (DNFSB) is an independent oversight agency with purview of nuclear safety at DOE defense nuclear facilities. The DNFSB evaluates the effectiveness of DOE regulatory oversight activities and the safety of defense nuclear facility design, construction, operations, and decommissioning. Various DOE defense nuclear sites have resident DNFSB staff located with the DOE Site Operations Offices. The resident staff can, and typically will, participate in reviews of the project at any stage. Additionally the DNFSB conducts their own review of the proposed facility design, including the safety design basis development and construction, when determining the adequacy of project nuclear safety and the effectiveness of DOE oversight.

Other external regulatory reviews performed for the purpose of permitting activities are conducted by independent agencies (local, state, and Federal) pursuant to environmental regulations such as the Resource Conservation and Recovery Act, Clean Air Act, and Clean Water Act. Typically, these permits or site permit modifications are approved before formally declaring facility readiness. In certain situations, the state may establish limiting criteria on design (e.g., zero release criteria) that may be more limiting on the design and operation than the requirements derived from safety design basis development.

The project manager should anticipate and identify all stakeholders that could affect the development of the safety design case. Once identified, regular interaction with these key oversight groups should be planned to minimize unanticipated issues at critical review steps.

7.14 System Engineer Program

DOE O 420.1B requires application of a System Engineer (SE) program to “active safety class and safety significant SSCs as defined in the facility’s DOE-approved safety basis, as well as to other active systems that perform important defense-in-depth functions, as designated by facility line management.” An objective of the program is to ensure operational readiness of systems within scope. This objective translates into ensuring proper configuration management of the systems and associated documentation and requirements. SE program requirements are also aimed at supporting operations and maintenance.

In preparation for the operational phase, it will be important to identify SEs and involve them in the design and hazard analysis process. Ideally, this should begin in the final design phase so that they may become familiarized with the design in preparation for more direct involvement in the construction phase. SEs should be involved in the planning for and conduct of system testing to allow detailed operational understanding. The SEs should also have a fundamental understanding of the safety function and performance requirements for their assigned system, as well as for the associated design and safety documentation. Proper SE preparation will help facilitate a smooth transition to routine operation and maintenance following approval for operations.

7.15 Procedures, Training and Qualification

A systematic approach to operations involves the development of operating procedures based on the design and identified hazard controls to operate SSCs within their design and DOE authorized limits through the TSRs. In turn, operators are trained on applicable process and hazard fundamentals, SSC operations and functions, and specific operating procedures. Operators are expected to understand important safety system features and any specific administrative controls, as well as the operator's role in the safety of the facility.

In order to satisfy expectations, the results of the safety and design process must be incorporated into the procedures and training programs. This includes nuclear criticality safety-derived requirements as well. System operating and test procedure development should begin in the detailed design phase. System description documents should be used as a tool to capture both operating intent and safety design information for use by the safety analysts and procedure writers. Draft qualification requirements should begin in parallel with detailed design and should be completed early in the construction phase. Training will ensue in the construction phase.

Table 7-1. Typical Actions Associated with Project Life-Cycle Stages

Actions Authorized by Critical Decision Approval						
Phase / Interface	**Mission Need**	**Conceptual Design**	**Preliminary Design**	**Detailed Design**	**Construction**	**Resource Requirements and Guidance**
QA	• QA strategy	• Update QA Plan • Conduct assessments	• Assessments	• Assessments	• Input to DSA Ch. 14	• 10 CFR 830 • DOE-O-414.1C
Fire Protection	• Identify major fire scenarios and special fire considerations for input to likely safety SSC designation	• Develop Preliminary FHA • Separation of SSCs • Life Safety – Egress considerations (approach) • Identify Fire Areas • Preliminary Functional classification • Define design codes and standards	• FHA update • Design Basis Fire defined • Fire barrier design and fire areas finalized • AHJ review of building layout	• FHA update • Support PDSA development	• Final FHA • Prepare DSA Ch. 11	• DOE-O-420.1B • DOE-O-440.1 • DOE-STD-1066 • 10 CFR 851 • DOE G 420.1-3

Actions Authorized by Critical Decision Approval						
Phase / Interface	Mission Need	Conceptual Design	Preliminary Design	Detailed Design	Construction	Resource Requirements and Guidance
Criticality Safety	• Determine criticality potential • Input to Hazard Categorization	• Criticality Control Philosophy • Criticality guidance for Design	• Preliminary CSEs • Updated criticality safety design requirements	• Updated preliminary CSEs • Re-assess criticality limits and controls based on design and operating the process/facility • CSE input to PDSA (Hazard Analysis and TSR derivation)	• Update and issue CSEs • TSRs and operating procedures will incorporate criticality controls, as developed under the guidance of DOE-STD-3007 and DOE G 423.1-1. • Validate NCS controls in field\ • Prepare DSA Ch. 6	• DOE-O-420.1B • DOE-STD-3007-2007 • DOE-G-421.1-1
• **Radiological Protection**		• ALARA strategy	• ALARA Review • Preliminary Shielding Analysis (Facility Layout and Material Location and Quantity) • ALARA Considerations in Design • Contamination Control • Zoning	• Final Shielding Analysis • ALARA review • Monitoring (area and personnel)	• Input to DSA Ch. 7	• 10 CFR 835 • DOE G 441.1-1B

Actions Authorized by Critical Decision Approval						
Phase / Interface	Mission Need	Conceptual Design	Preliminary Design	Detailed Design	Construction	Resource Requirements and Guidance
Human Factors		• Define HF strategy and goals	• HF Engineering Plan HF Preliminary Review	• HF Review	• Prepare DSA Ch. 13	• DOE-HDBK-1140-2001
Security	• Draft Safeguards Requirements Identification (SRI)	• SRI	• Design reviews	• Design Review	• Security Plans	• DOE-O-470.3 • DOE-O-470.4
Environmental Protection	• EPA • State Environmental Agency	• NEPA Strategy and Analysis • EPA • State Environmental Agency	• Draft NEPA Documents	• Final NEPA Documents		• 10 CFR 1021 • DOE O 451.1B • DOE O 450
Hazardous Materials		ALARA strategy	• Toxicological Material Hazards Analysis • Contamination Control • Refine inventories • Codes and Standards defined • Zoning • ALARA review	• ALARA reviews • Codes and Standards Implementation • Monitoring (area and personnel) requirements	• Prepare DSA Ch. 8	• DOE-O-440.1A

Actions Authorized by Critical Decision Approval						
Phase / Interface	**Mission Need**	**Conceptual Design**	**Preliminary Design**	**Detailed Design**	**Construction**	**Resource Requirements and Guidance**
Radiological and Hazardous Waste Management		• Identify major waste streams • Fundamental approach defined		• Develop waste handling designs	• Prepare DSA Section 9	• 10 CFR 830 • DOE-O-420.1B • 10 CFR 850 • DOE O 435.1
Emergency Preparedness	• Emergency Preparedness Hazard Survey and Screen	• Update Emergency Preparedness Hazard Survey and Screen	• Coordinate hazard evaluations • Preliminary EPHA	• Update EPHA	• EPHA updated and finalized • ERP updated and finalized • Prepare DSA Ch. 15	• 29 CFR 1910.119 • 40 CFR 68 • DOE-O-151.1C
External Reviews	• DNSFB • Project Review • SDS review	• DNFSB • CSDR Review • Project Review	• DNFSB • PSDR Review • Project Review	• DNFSB • PDSA Review • Project Review	• DNFSB • DSA/TSR Review • ORR/RA (as applicable)	• DOE-O-226.1
System Engineer Program			• Define systems requiring SE	• Identify SEs • SEs participate in Final Design	• SEs support testing	• DOE-O-420.1B

Actions Authorized by Critical Decision Approval						
Phase / Interface	**Mission Need**	**Conceptual Design**	**Preliminary Design**	**Detailed Design**	**Construction**	**Resource Requirements and Guidance**
Procedures, Training and Qualification				• Identify training and qualification needs • Develop draft operating and maintenance procedures • Define operator qualification requirements	• Complete procedures • Develop and conduct training • Input to DSA Ch. 12	• DOE O 5480.20A

Table 7-2. Example Nuclear Criticality Safety Design Criteria

Attribute	Criteria
Geometrically safe designs	1. Storage tanks, process piping, containers, etc. shall be designed for conservative enrichment or optimal concentration and reflection for all anticipated nuclides. 2. Designs shall be based on worst-case fire suppression actuation or local pipe breaks. 3. Leaks from solution areas should be anticipated and flooring designed to be compatible with solutions and provide collection capability (prevent long-term migration of fissionable material into sub-flooring materials). 4. Fissionable containing piping shall be spaced to preclude neutron interaction.
Layout processes to support material flow	1. Fissionable solution piping shall be arranged to minimize or eliminate manual transfers. 2. Transfers from safe to non-geometrically safe geometry shall be provided with engineered controls. 3. Avoid any favorable to unfavorable geometry solution transfers. If such need to be made, active design features should be installed to mitigate the potential for a criticality accident due to transfer of fissionable solution to an unfavorable geometry vessel.
System design for holdup minimization	1. Employ vertical tanks to facilitate particulate collection and monitoring. 2. Provide methods to facilitate holdup verification/assay. 3. Locate filtration on exhaust systems as close to main processing loop as possible.
Maximize use of passive design features	1. Utilize positive isolation techniques to prevent unmonitored backflow potential (e.g., air breaks). 2. Avoid common ties between fissionable and non-fissionable systems. 3. Designs must eliminate potential for water ingress into fissionable material processes and containers in the event of fire.
Standardize Equipment	1. Storage racks shall be modular and prevent relocation of fissionable material up to the seismic DBA. 2. Gloveboxes shall be designed to address concerns associated with spills or in-leakage of moderators. 3. All process equipment must withstand the facility seismic DBA.

8.0 ADDITIONAL SAFETY INTEGRATION CONSIDERATIONS FOR PROJECTS

8.1 Integration of Safety into Facility Modifications

The purpose of the process described in this section is to provide a means whereby a proposed facility modification can be determined to be a major modification (or not), within the definition of 10 CFR 830. All proposed modifications must undergo the Unreviewed Safety Question (USQ) process as required by 10 CFR 830 for Hazard Category 1, 2, and 3 nuclear facilities.

The process for integration of safety into the design of facility modifications is similar to that for new facilities, but it is tailored to the scope, magnitude, and complexity of the modification. Figure 9-1 presents an overview of a conceptual process for facility modifications that involves two assessments. The first is whether the modification is so simple that it does not involve a substantive change in the facility safety basis and also does not come under the requirements of DOE O 413.3A, Chg 1. This should be a straightforward assessment to eliminate from major modification consideration those modifications that do not require a new or revised hazard or accident analysis, new or revised hazard controls, and involve safety basis changes that are descriptive only. These simple modifications may be processed under the normal change control processes necessary to support the engineering and USQ processes.

The second assessment is more subjective and involves a determination of whether the modification is a major modification requiring a PDSA under 10 CFR 830. Table 8-1 presents criteria to aid in making this judgment. If a facility modification is not a major modification but is subject to DOE O 413.3A, Chg 1, a Safety Design Strategy (SDS) that describes the tailoring of the modification project and the supporting safety documentation to be developed is necessary. Note that preliminary safety documentation, including the Conceptual Safety Design Report (CSDR), the Preliminary Safety Design Report (PSDR), and the Preliminary Documented Safety Analysis Report (PDSA), is not required for modifications that are not major modifications.

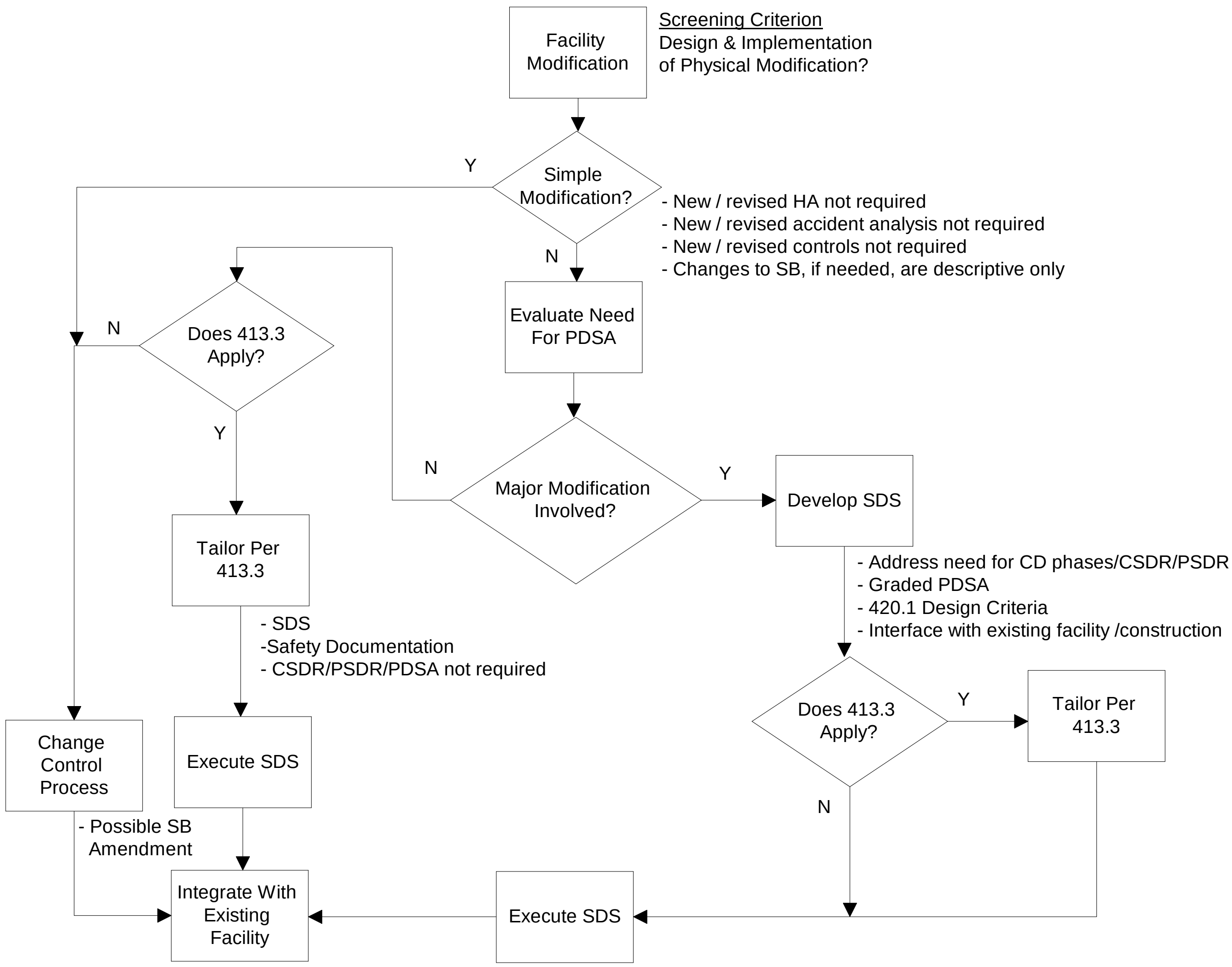
The degree to which a facility may have to be modified to accommodate new or existing missions may range over a continuous spectrum from minor changes up to those involving the addition or upgrade of multiple safety systems and highly hazardous processes. The latter type of modification may be a capital project and require nearly all of the design phases and processes necessary to design and construct a new facility.

If a facility modification represents a "substantial change to the existing safety basis," it is considered a "major modification"; that is, one in which the design criteria of DOE O 420.1B and its Guides apply to new or upgraded structures, systems, and components (SSC) and for which a PDSA is required to support the design process.

The interface of the facility modification with the facility being modified and its ongoing activities presents a challenge. The change control processes of the existing facility should be coordinated with the construction, installation, and testing activities supporting the modification. Frequently, the organization responsible for executing the modification is different from the one operating the facility; therefore, a disciplined process for controlling and coordinating construction activities is necessary.

This chapter summarizes the integration of safety into the design and execution of facility modifications.

Figure 8-1. Facility Modification Process



8.1.1 Review of Existing Hazard Analysis

The first step in determining how to handle a proposed facility modification is to review the existing hazards analysis in the facility DSA. Review of the existing hazard analysis may determine that it is adequate for the modification, that the hazard controls adequately address the modification and associated activities, and that implementing the existing change control processes, such as the USQ and configuration management processes, procedure changes, and training programs is adequate to support the proposed change. These are generally simple modifications that may require a change to the description of the facility or its activities but do not represent a substantial change to the safety basis.

The review may also indicate that a new or revised hazard analysis is required to support a proposed facility modification or associated activities. For modifications to existing processes, the hazard analysis revision may involve identifying additional hazards and updating an existing hazards analysis. A new hazard analysis may be performed for new discrete activities or for processes that were not previously evaluated. In this case, the hazards analysis should identify potential hazards, necessary hazard controls, and impacts to the existing safety basis. The intent of the hazards analysis is to identify safety functions and safety basis functional requirements as early as practical in the conceptual phase of the modification to ensure that they are integrated into the project design in a timely and cost-effective manner.

The new or revised hazards analysis may identify a number of safety functions and safety SSCs that are different than those previously considered. There are a number of reasons that a reassessment of facility hazards and identification of hazard controls is necessary at the conceptual phase, all of them associated with minimizing project risk, including the following:

- to ensure that the safety functions and safety SSCs are integrated into the design at the earliest and most effective phase;
- to allow a proactive assessment of potential impacts of the modification to the safety basis of the existing facility; and
- to enable a more realistic cost and schedule estimate for the modification.

The hazards analysis may address only the end-state (operational) risks associated with the modification project and not the interim risks encountered during construction or equipment installation activities. In this case, (1) the interim risks must be identified, and (2) necessary hazard controls must be implemented, as part of the facility work control process and the associated hazard analysis (e.g., job hazards analysis) and considered under the facility’s USQ process.

8.1.2 Major Modifications

As defined by 10 CFR 830, major modifications are those that "substantially change the existing safety basis for the facility." A major modification requires the development of a PDSA (Section 830.206) and its approval by DOE (Section 830.207).

As provided by Section 830.206 of the rule, the PDSA is required to document the nuclear safety design criteria used for the modification, and DOE approval is required (with limited exceptions) before commencing procurement and construction activities.

While modifications to a nuclear facility occur almost constantly throughout its life cycle, not all may involve a "substantial change to the facility safety basis" and are not considered to be major modifications. Major modifications involve significant project liability such that the rigor of a PDSA and attendant DOE review and approval are established to reduce overall project risk. This approach ensures formal DOE concurrence in the establishment and implementation of nuclear safety design criteria and selection of hazard controls as early as possible in the modification process.

8.1.3 Determining a Major Modification

It is important to determine the need for a PDSA as early as feasible in planning for a modification so that actions to revise the existing safety basis documentation or develop the PDSA document may begin early in the design process. At the same time, the design should be mature enough to define the scope of the modification to allow a meaningful recommendation. This should occur before submittal of the conceptual design report or at a similar phase for modifications not subject to the critical decision process described in DOE O 413.3A, Chg 1.

In many situations, the need for a PDSA may be readily discernible with little or no detailed evaluation required. For example, a project that does not involve a design effort and the implementation of a physical modification (e.g., facility procedure upgrade project, facility maintenance or overhaul project) is not a major modification and does not require a PDSA. Any safety implications for such projects can be adequately addressed through the existing requirements related to safety basis management (such as the USQ process) or Integrated Safety Management without the need for a PDSA. However, situations will arise where this determination is not clear and a more rigorous evaluation is required. Table 8-1 provides recommended criteria for evaluating the need for a PDSA, and, therefore, the existence of a major modification. Each criterion addresses a key project characteristic relevant to the purposes of a PDSA.

In applying the PDSA evaluation criteria in Table 8-1, the intent is that each criterion should be assessed individually and then an integrated evaluation should be performed based on the collective set of individual results. In performing this evaluation, the focus should be on the nature of the modification and its associated impact on the existing facility safety basis. Examples of the application of the PDSA evaluation criteria are included in Appendix J, "Major Modification Determination Examples," to provide additional guidance.

Where a major modification is found to exist, an SDS must be developed that addresses (1) the need for a CSDR or PSDR (as well as the required PDSA) to support project phases, (2) the graded content of the PDSA necessary to support the design and modification, (3) the application of nuclear safety design criteria, and (4) the interface with the existing facility, its operations, and construction activities.

A facility modification that does not qualify as a major modification, but does involve a positive USQD, requires a safety analysis in support of a request for approval from DOE to proceed with the modification. A positive USQD at this step also provides DOE with an opportunity to check the validity of the initial finding (see Figure 8.1) of a simple modification.

Table 8-1. Major Modification Evaluation Criteria

Major Modification Evaluation Criteria		
Evaluation Criterion No.	**Evaluation Criteria**	**Discussion**
1	Add a new building or facility with a material inventory ≥ Hazard Category 3 (HC 3) limits or increase the HC of an existing facility?	A new building may be a structure within an existing facility segment. That structure may or may not have direct process ties to the remainder of the segment/process. The requirements of DOE-STD-1027-92, Change Notice 1, September 1997, are used in evaluating Hazard Categorization impacts.
2	Change the footprint of an existing HC 1, 2 or 3 facility with the potential to adversely affect any safety class (SC) or safety significant (SS) safety function or associated structure, system and component (SSC)?	A change in the footprint of an existing facility requires the identification and evaluation of any potential adverse impacts on SC or SS safety functions or associated SSC (e.g., structural qualification, evacuation egress path, fire suppression spray pattern) or safety analysis assumptions. Changes that may involve adverse impacts require careful attention to maintaining adherence to applicable engineering standards and nuclear safety design criteria.
3	Change an existing process or add a new process resulting in the need for a safety basis change requiring DOE approval?	A change to an existing process may negatively affect the efficacy of an approved set of hazard controls for a given event or accident. Likewise, potential safety concerns associated with a new process may not be adequately addressed by the existing approved control sets. In this case, it is assumed that the existing analyses addressed the hazards associated with the new or revised process, but the specified control set(s) may no longer be valid. The evaluation of any new hazards introduced by the revised or new process should be addressed via Criterion 6
4	Utilize new technology or government furnished equipment (GFE) not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	This assessment should include consideration of the impact that the use of new technology (including technology scale-up issues) or GFE may have on the ability to specify the applicable nuclear safety design criteria with a high degree of certainty in the early stages of the project. Additionally, refer to GFE discussion in Section 8**.3**. GFE may have a technical baseline that is not directly and fully supportive of the project functional and performance requirements. An example would be employing a new technology for removal of certain nuclides from a waste stream.

Major Modification Evaluation Criteria		
Evaluation Criterion No.	**Evaluation Criteria**	**Discussion**
5	Create the need for new or revised safety SSCs?	Consideration should be given to the relative complexity of the controls and the ease with which the controls can be implemented. The use of a complicated multi-channel Safety Class seismically qualified instrumented system to provide multiple interlock and alarm functions would typically pose a higher risk to the project than the use of a safety significant passive design feature. The degree of design and regulatory uncertainty should be addressed for this criterion for the development, review, and approval of new or revised safety analysis and attendant controls (e.g., presence of multiple regulatory/technical agencies on a single project).
6	Involve a hazard not previously evaluated in the Documented Safety Analysis (DSA)?	Hazards can include the introduction of an accident or failure mode of a different type from that previously analyzed in addition to radiological or toxicological hazards. The need to address a new hazard early in the design process may lead to some degree of uncertainty related to the proper specification of applicable nuclear safety design criteria. In such cases, this uncertainty should be addressed within this evaluation.

8.2 Construction Projects within Operating Facilities

For major modifications or other projects that are being incorporated into or added onto existing nuclear facilities, it is necessary to ensure that the requirements of the approved and implemented safety basis for the facility being modified are observed and protected throughout the construction and testing processes. Construction or interim hazards and risks may be significant drivers for the design activity, such as introduction of unacceptable fire sources during construction, and may require a different design approach. It is important that these types of issues not be delayed for consideration solely under work control processes for installing the modification.

During the work planning process, it is necessary to determine the methods and processes by which the modifications will be constructed or installed. These documents need to consider impacts to the existing facility features and design bases that may include the following:

- effect of additional wall penetrations;
- increased or decreased loading on existing SSCs;
- capability of existing support systems to carry additional load demand (e.g., electrical, steam, air); and
- effects of startup testing of new components in conjunction with existing facility systems.

It is necessary to ensure that all proposed project activities are reviewed against the existing safety basis using the USQ process. If the result of the USQ determination is that DOE approval is necessary, the contractor may need to establish alternate or supplemental safety basis documentation activities, such as a specific amendment to existing and implemented safety basis or a standalone interim safety basis covering construction activities, to support construction and installation.

8.3 Government Furnished Equipment

DOE occasionally provides pre-existing SSCs, hereafter referred to as government furnished equipment (GFE), for use in a new project or a modification to an existing facility. Experience has shown that the use of GFE can lead to the identification of significant safety issues after substantial project work has been completed if the GFE technical baseline, performance and operational characteristics, and associated hazards are not fully understood and accounted for in the project design. The failure to fully integrate the use of GFE into the project baseline documentation in a timely manner can result in significant project cost and schedule impact that can ultimately lead to project cancellation. The approach to GFE interfaces must be addressed in the SDS.

Guidance is provided in the following sections to ensure that GFE is properly and fully integrated into the project effort.

Also in the class of activity is equipment that was not part of the preliminary and final design process discussed previously. This situation is frequently encountered in science and technology efforts where the building and the equipment it houses are developed on different schedules. In such cases, interfaces are typically defined in the design process, and the development of the equipment conforms to those interfaces. However, hazardous operations and safety design requirements for to-be-installed equipment may not be fully defined in the final design. In such cases, the Documented Safety Analysis (DSA) should address the design issues along with the risk and opportunity assessments conducted during all project phases. The SDS should define the appropriate approach for ensuring DOE agreement with the safety of the equipment.

Discussions that follow for GFE provider and end-user responsibilities may be tailored to support equipment designs that are developed after the designs for the building to house the equipment are approved through final design. This guidance is intended to promote a thorough consideration of the necessary information and evaluations that need to be supplied, performed, or otherwise developed if GFE is to be safely and effectively used in a project. This involves a mutually collaborative effort on the part of the GFE supplier and end user that can foster the timely integration of the necessary information into project planning and execution activities.

8.3.1 GFE-Provider Responsibilities

The project team should establish appropriate requirements for the provider of the GFE to supply in a documentation package that defines the technical baseline, performance and operational characteristics and the associated hazards of the GFE. This documentation is typically in the form of specifications, drawings, calculations, technical reports, test reports, operating manuals, operating procedures, hazard analyses, and similar documents. This collection of information should be sufficient to allow the original GFE technical basis to be readily and well understood by the end user (i.e., the project) and should define the following:

- codes and standards used in design, fabrication, assembly, inspection, and testing;
- materials of construction;
- key interface parameters (e.g., footprint dimensions, weights, anchor details, heat loads);
- key interface utility requirements (e.g., air, steam, electricity, cooling water);

- instrumentation and control provisions/needs and interface requirements (including local indication and alarms provisions, as well as remote analog/digital indication, alarm, and interlock process parameter input capabilities);
- structural loads included in the design (e.g., deadweight, thermal, pressure, vibration, dynamic, seismic, tornado, wind, missile, snow, flood) along with associated functional capability under these loads;
- environmental qualification and capabilities, including effects from the process medium as well as ambient conditions;
- potential failure modes and hazards (preferably from an Failure Modes and Effects Analysis [FMEA] or HA, if performed);
- performance and operating information, including normal process parameters (e.g., flows, pressures, temperatures, levels);
- upset conditions and associated parameters;
- design parameters;
- operating manuals and procedures for both normal and upset conditions;
- maintenance manuals, including specification of recommended spare parts;
- test reports; and
- operating and usage history.

In addition to providing the foregoing information, the GFE provider should also make all supporting QA documentation available to the end user. Such information may include material certification and test reports, certificates of compliance, nondestructive examination reports, and hydrostatic test reports. The intent is to provide the end user with auditable, objective evidence that all applicable code and standard QA requirements have been satisfied.

The lack of complete technical, performance, operational, and QA documentation as outlined above may result in concluding that the GFE baseline or history is indeterminate. Providing this information to the end user as early as possible in the project will minimize project impact should an indeterminate state render the GFE unusable or should the project have to pursue a baseline reconstruction effort.

8.3.2 GFE End User Responsibilities

After reviewing or reconstructing the necessary technical, performance, operational, and QA documentation, the end user will be in a position to assess the adequacy of the GFE relative to the needs of the project (i.e., the project functional and performance criteria). This assessment may identify gaps, including those related to the project safety design basis, which the project will have to address should the GFE be used. Safety design basis-related gaps may be document-related or hardware-related with the recognition that documentation gaps could result in downstream hardware impacts. The risk for such safety design basis noncompliance underscores the need to integrate the GFE information into the project safety design basis development effort as early as possible to minimize downstream impacts.

An example of a document gap would be the absence of FMEA or HA information. This would result in the project having to perform the necessary analyses to identify potential GFE failure modes and hazards, which then need to be integrated into the project safety design basis work. The inclusion of this information may result in identifying the need for new or revised control sets that may not have been previously anticipated by the project. An example of a hardware gap would be a discrepancy between the GFE "as provided" condition and that required by the project safety design basis (e.g., not seismically qualified with the appropriate attendant functionality). This may require a modification of the GFE to achieve the required level of performance with respect to structural capability, environmental compatibility, reliability, inspectability, testability, accuracy, and similar processes. Note that the need for such modifications may be derived indirectly through safety design basis-supporting evaluations (e.g., ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System Hardware, and Software Requirements*.)

APPENDIX A

SAFETY SYSTEM DESIGN CRITERIA

This appendix provides guidance and criteria for specification of the seismic design basis and the safety classifications of structures, systems, and components (SSC). These criteria relate to radiological hazards only. Treatment of chemical hazards for safety significant classification purposes is discussed in Appendix B.

During conceptual design, when a conservative estimate of the total facility inventory of hazardous material can be made and facility-level Design Basis Accidents (DBA) are defined and analyzed, a preliminary assessment of safety design aspects for the facility can be formulated. This appendix specifies the methodologies to be applied to the major preventative and mitigative SSCs that are selected from the analyses of the DBAs. Classifications resulting from this guidance provide information that can be used to prepare a preliminary list of functional safety requirements for these safety SSCs. It is intended that this information be used to develop conservative cost estimates for the conceptual design. Note that support systems that are essential for a safety class (SC) or safety significant (SS) SSC to perform its safety function must also be classified at the same level as their supported SSC.

A.1 Seismic Design Basis

This section specifies how to apply two recently published national standards for seismic design of DOE non-reactor nuclear facilities. The standards were developed at the initiative of DOE and provide methods, guidelines, requirements, and criteria for the seismic design of SSCs. The standards are as follows:

- ANSI/ANS 2.26-2004, *Categorization of Nuclear Facility Structures, Systems and Components for Seismic Design*; and
- ASCE/SEI 43-05, *Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities*.

These national standards were developed by the American Nuclear Society (ANS) and the American Society of Civil Engineers (ASCE). The standards working groups that developed these standards included DOE, the Nuclear Regulatory Commission (NRC), the Defense Nuclear Facility Safety Board (DNFSB), and industrial representation. To a large degree, these national standards are based on DOE experience with application of seismic requirements in the following DOE natural phenomena hazards (NPH) standards:

- DOE-STD-1020-2002, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*; and
- DOE-STD-1021-93, *Natural Phenomena Hazards Performance Categorization Criteria for Structures, Systems, and Components*.

ANS Standard 2.26, as interpreted in this appendix was adopted by DOE for the purposes of seismic design basis specification. The seismic design classifications of ANS 2.26 are to be used in association with DOE radiological criteria provided in this appendix. It is intended that the requirements of Section 5 of ANS Standard 2.26 and the guidance in Appendix A of that Standard be used for selection of the appropriate Limit States (LS) for SSCs performing the safety functions specified. The resulting combination of Seismic Design Category (SDC) and LS selection provides the seismic design basis for SSCs to be implemented in design through ASCE/SEI 43-05, *Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities*.

For DOE purposes, the criteria for selecting an SDC are to be based on the following methodologies and criteria.

- DOE implementation of ANS Standard 2.26 relies on conservative bases for unmitigated accident analysis.
- A worker, in the ANS Standard 2.26, is interpreted to mean a collocated worker at a distance of 100 m from a facility (building perimeter) or estimated release point.
- For criteria associated with the public, the methodology of assessment to be followed is that of Appendix A of DOE-STD-3009-94, CN 3.
- Criteria doses are Total Effective Dose Equivalent (TEDE)[6].
- In conceptual design, if there are no bases for defining seismic related DBAs, Hazard Category 2 facility structural designs must default to ANSI/ANS 2.26 SDC-3, Limit State D. If the hazards analysis conducted during subsequent stages of design shows that unmitigated consequences are less than the threshold criteria for SDC-3 shown in Table A-1 below, then this may be reflected in the evolving design stages.
- Until ANS 2.27 and ANS 2.29, which are referenced in ANS 2.26, are formally issued by ANS and adopted by DOE, DOE Standards 1022 and 1023 should continue to be used in seismic design. Note that for other natural phenomena hazards (NPH), DOE Standards 1020, 1021, 1022, and 1023 are applicable.

[6] The concept of TEDE was introduced as a construct to represent the summation of Direct Exposure and Committed Dose from retained radionuclides from other pathways. This construct has also been referred as Total Effective Dose (TED) and Annual Effective Dose (AED) (when considering exposures received or committed to in a single year). Currently the ICRP supports the concept of TED, although this terminology is not present within ICRP 60, 68, or 71.

Table A-1. Guidance for SDC Based on Unmitigated Consequences of SSC Failures in a Seismic Event

	Unmitigated Consequence of SSC Failure from a Seismic Event	
Category	Collocated Worker	Public
SDC-1	Dose < 5 rem	Not applicable (1)
SDC-2	5 rem < dose < 100 rem	5 rem < Dose < 25 rem
SDC-3	100 rem < dose	25 rem < dose

(1) A Hazard Category 1, 2, or 3 nuclear facility with consequences to a collocated worker from failure of an SSC in a seismic event will require that SSC to be classified as SDC-1 at a minimum. Therefore, a public criterion for SDC-1 is not needed.

(2) As noted in ANS 2.26, the SDCs used in the Standard and in this table are not the same as the SDCs referred to in the International Building Code (IBC).

This table, in comparison with criteria in ANS Standard 2.26, is truncated at SDC-3 on the following bases.

- No higher designations than safety significant or SDC-3 design requirements are judged to be necessary for collocated worker protection because (in addition to design features) site training and site emergency procedures provide for adequate protection for workers. Only in the case of an in-facility worker who must remain in the facility for safe shutdown or other safety-related purpose should SDC-3 be considered for SSCs required for protection of that worker. In that case, the mitigative effects of personal protective equipment may also be considered. Design effort should give priority to engineered design features over PPE in such a circumstance.
- It is likely that DOE will build only high-hazard, non-reactor nuclear facilities at large sites, where it is more likely that the collocated worker criterion would be controlling for seismic design purposes. In such cases, it would be unlikely that the qualitative radiological criteria suggested by ANS Standard 2.26 for the public for SDC-4 would be exceeded. If the quantitative public criterion for SDC-3 of Table A-1 is exceeded significantly for any project (between one and two orders of magnitude), then the possibility that SDC-4 should be invoked must be considered on a case-by-case basis.

In performing the unmitigated accident analyses specified by ANS 2.26, material-at-risk (MAR) should be conservatively estimated. The source term quantities used should be derived, as appropriate to the situation, to consider damage ratio (DR) and airborne release fraction (ARF) for the DBAs, in accordance with the unmitigated accident analysis source term guidance of Appendix A, Section A.3.2, of DOE-STD-3009-94, CN 3, and DOE G 420.1-1. A leakpath factor of 1.0 must be used. Dose conversion factors consistent with ICRP Publications 68 and 72 must be used.

For the purposes of this Standard, a χ/Q value at 100 m of 3.5E-3 sec/m3 must be used for the dispersion calculation. This value is based upon NUREG 1140 (no buoyancy, F-stability, 1.0 m/sec wind speed at 100 m, small building size [10 m x 25 m], and 1 cm/sec deposition velocity). Dispersion analyses for public dose calculations should be done according to the guidance of DOE-STD-3009-94, CN 3, Appendix A.

The following supplemental guidance to ANS 2.26 should be used when selecting SDCs and Limit States:

(a) To ensure that the SSC Limit State selected for determining the permissible maximum stress, strain, deformation, or displacement is consistent with the safety function(s) of the SSC as determined from hazard and accident analyses, the safety analyst (responsible for hazard and accident analyses), the Seismic Design Engineer (responsible for seismic design, and for coordinating the selection of SSC Limit State and SSC Seismic Design Category), and the Equipment Expert (responsible for the mechanical or electrical design of the equipment) should work together and evaluate the functional requirements of the SSC and its subcomponents in relation to their modes of failure.

(b) If the safety functions of an SSC include confinement and leak tightness, irrespective of the Seismic Design Category (SDC) of the SSC, following the intent of Section 5 of ANS 2.26, a Limit State C or D must be selected, unless the SSC functional requirements can be described as given in Limit State B column for the SSC Type “confinement barriers and…” in ANS 2.26, Appendix B. An SDC-1 or SDC-2 SSC having safety functions requiring Limit States A, B, C or D are to be designed as follows:

SDC	Limit State			
	A	B	C	D
1	**ASCE 7-05 Occupancy Category I or II (I=1.0) (1)** **R_a = R(1)**	**ASCE 7-05 Occupancy Category I or II (I=1.0) (1)** **R_a =0.80R(1)** **But $R_a \geq 1.0$**	**ASCE 7-05 Occupancy Category I or II (I=1.0) (1)** **R_a =0.67R(1)** **But $R_a \geq 1.0$**	**ASCE 7-05 Occupancy Category I or II (I=1.0) (1)** **Use R_a (1) = 1.0**
2	**ASCE 7-05 Occupancy Category III or IV(2)** **R_a = R(1)**	**ASCE 7-05 Occupancy Category III or IV(2)** **R_a =0.80R(1)** **But $R_a \geq 1.0$**	**ASCE 7-05 Occupancy Category III or IV(2)** **R_a =0.67R(1)** **But $R_a \geq 1.0$**	**ASCE 7-05 Occupancy Category III or IV(2)** **Use R_a (1) = 1.0**

Note (1): I = Importance Factor (see Table 11.5-1 of ASCE 7-05)

R = Response Modification Coefficient given in ASCE 7-05(see Tables 12.2-1 and 15.4-2 of ASCE 7-05).

R_a = Actual (reduced) Response Modification Coefficient to be used in the design

Note (2): ASCE 7-05 Occupancy Category IV (I = 1.5) shall be used if there is a radiological release consequence of concern to the public or the environment resulting from an unmitigated failure of the SSC.

A.2 Safety Classification of SSCs

A.2.1 Public Protection Criteria

The guidance of DOE G 421.1-2 and DOE-STD-3009-94, CN 3, Appendix A, should be used in classifying SSCs as Safety Class (SC) for radiological protection. The words “challenging” or “in the rem range” in those documents should be interpreted as radiological doses equal to or greater than 5 rem TEDE, but less than 25 rem TEDE. In this range, SC designation should be considered, and the rationale for the decision to classify an SSC as SC or not should be explained and justified. SSCs designated as Safety Class based on seismic hazards must also be designated as SDC-3 for seismic design, at a minimum.

A.2.2 Collocated Worker Protection Criteria

A conservatively calculated unmitigated dose of 100 rem TEDE has been chosen as the threshold for designation of facility-level Safety SSCs as safety significant (SS), for the purpose of collocated worker protection. The radiological source term quantities used should be derived, as appropriate to the situation, to consider damage ratio (DR) and airborne release fraction (ARF) for the DBAs, and should be reasonably conservative. A leakpath factor of 1.0 must be used. For the purposes of this Standard, a χ/Q value at 100 m of 3.5E-3 sec/m3 must be used for the dispersion calculation. This value is based upon NUREG 1140 (no buoyancy, F-stability, 1.0 m/sec wind speed at 100 m, small building size [10 m x 25 m], and 1 cm/sec deposition velocity).

A.3 Existing Facilities and Major Modifications of Existing Facilities

The seismic design classification and collocated worker safety significant criteria of this appendix should not be applied in a backfit sense to existing facilities that are not undergoing modifications.

For major modifications of existing facilities, these criteria should be used with the following caveats. Backfit analyses should examine (1) the need to upgrade interfacing structures, systems, and components in accordance with these criteria; and (2) whether there should be relief for the modification from the design requirements that application of these criteria in design would imply.

APPENDIX B
CHEMICAL HAZARD EVALUATION

Consistent with practice in nonnuclear hazardous facility design, DOE is not invoking classification of safety class structures, systems, and components (SSC) or specifying nuclear design requirements based on chemical hazards alone. This appendix, however, provides guidance for consideration of safety significant designation for SSCs, in terms of guidance for chemical exposures. The guidance provides a sense of scale as to what is meant by a “significant exposure” in the criterion for classifying SSCs as safety significant. The guidance is based on a process of (1) screening chemicals (hazardous chemical materials) to determine those that may have the potential to immediately threaten or endanger onsite (collocated) workers or the public and (2) evaluating the severity of potential exposures against advisory classification criteria for collocated workers and the public. Evaluation of chemical hazards for potential significant facility worker hazards is addressed in Appendix C, “Facility Worker Hazard Evaluation”.

B.1 Screening of Hazardous Chemical Materials

The hazardous chemical material screening process identifies all hazardous chemical materials in the facility/activity that require further evaluation. All chemicals with known or suspected toxic properties must be subjected to the screening process.

Chemicals that may be excluded from further analysis for functional classification and the identification of attendant design criteria include the following.

- Chemicals with no known or suspected toxic properties.
- Materials used in the same form, quantity, and concentration as a product packaged for distribution and use by the general public.
- Chemicals in a quantity that can be “easily and safely manipulated by one person.” Quantities of hazardous chemical materials considered to be easily and safely manipulated by one person can be locally determined in accordance with the provisions of 29 CFR 1910.1450(b).
- Materials that have a health hazard rating of 0, 1, or 2, based on National Fire Protection Association (NFPA) 704.
- Solid or liquid materials that, because of their physical form or other factors (e.g., plausible dispersal mechanisms), do not present an airborne exposure hazard.
- Chemicals that can be defined as a Standard Industrial Hazard for which national consensus codes and standards provide for safe design and operation. The consensus code or standard needs to be identified and must be applicable to the use of the chemical in the facility that is to be screened from further evaluation.

Hazardous chemical materials that require further analysis include the following:

- chemicals with an assigned health hazard rating of 3 or 4 based on NFPA 704 in quantities greater than a quantity that can be "easily and safely manipulated by one person" [see 29 CFR 1910.1450(b)]; and
- chemicals without an assigned health hazard rating which require further analysis if in quantities greater than a quantity that can be "easily and safely manipulated by one person" [see 29 CFR 1910.1450(b)].

DOE O 151.1C, *Comprehensive Emergency Management System*, also has a screening process for hazardous materials. While this screening process is for different purposes (identification of materials which if released could meet the definition for an operational emergency), it is worthwhile to read and consider this process during the design stage so that the facility can be designed to preclude these releases.

B.2 Public and Collocated Worker Protection Criteria

Potential exposures to the public and collocated workers are estimated as described in Section B.3. These exposures can be compared to the following threshold levels for consideration of SSC classification as safety significant in facility design to prevent or mitigate these exposures.

- Public: Exposure > AEGL-2/ERPG-2/TEEL-2; and
- Collocated Worker: Exposure > AEGL-3/ERPG-3/TEEL-3.

The order of preference for evaluating a chemical is as follows: (1) Acute Exposure Guideline Levels (AEGL) promulgated by the Environmental Protection Agency (EPA) (60 minute AEGL); (2) Emergency Response Planning Guidelines (ERPG) published by the American Industrial Hygiene Association; and (3) Temporary Emergency Exposure Limits (TEEL) developed by DOE. In the event that a TEEL value cannot be obtained, users may select from one of the sets of chemical exposure guidelines issued by other agencies that are sometimes used as emergency planning criteria. These include the short-term public emergency guidance levels (SPEGL) and emergency exposure guidance levels (EEGL) developed by the National Research Council, and the levels of concern (LOC) published jointly by the EPA, Federal Emergency Management Agency (FEMA), and Department of Transportation (DOT).

B.3 Estimating Exposures to Collocated Workers and the Public

Exposures are chemical concentrations at the receptor location and depend primarily on the concentration of the chemical released, the rate of release, and the dispersion (dilution) that occurs between the release location and the receptor.

Toxicological consequences of a release are based on the peak air concentration at the receptor location that occurs any time during the duration of the release.

Unmitigated chemical consequence analysis should use reasonably conservative values for the parameters related to material release, dispersal in the environment, and health consequences. In many instances, the data available to support these analyses are not prototypic of the situation being analyzed or there is large and poorly characterized uncertainty. Hence, judgment needs to be used in selecting reasonably conservative values for the parameters of concern. For hazardous material aerosols and gases with a density near that of air, standard Gaussian atmospheric dispersion can be used. If the toxic material is released at some average rate over some period of time, the peak concentration at the receptor is obtained directly from the definition of the steady state χ/Q'

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

Where:

C = peak concentration (mg/m^3)

Q' = toxic material release rate (mg/s)

χ/Q' = steady state 1-hr dispersion coefficient (s/m^3).

The toxic material release rates (*Q')* can be determined in a manner similar to that used to determine radiological source terms (*Q*) divided by the release duration (*t*).

The peak 15-minute, time-weighted average (TWA) chemical concentration should be compared to the suggested threshold values for safety significant designation. There should be no adjustment of the suggested threshold value or the calculated concentration to account for differences between the recommended 15-minute exposure time and the exposure time implicit in the definition of the concentration-limit parameter.

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

Some consequence assessment dispersion codes will calculate the desired maximum 15-minute average concentration directly by allowing the analyst to specify the averaging period.

To determine the average concentration manually, the following formula can be used.

$$\text{TWA} = \frac{C_1T_1 + C_2T_2 + C_nT_n}{T_1 + T_2 + T_n}$$

Where:

C = Concentration (ppm or mg/m3)

T = Time period of exposure (min)

It is not recommended that individual time intervals less than 1 minute be used in the numerator of the above formula for calculating the TWA. For the peak 15-minute TWA, the 15-minute period of maximum exposure (concentration) is selected and input (as 15, one-minute segments) into the above formula. For exposure periods of less than 15 minutes, the product of C_xT_x may equal zero during the exposure period.

For release durations longer than 15 minutes, the peak 15-minute average concentration during the duration of the release is used for concentration dependent chemicals. These “zero" results may be factored into the 15-minute average or the use of a shorter averaging duration, such as the actual exposure period, may be warranted depending on the acute toxicity of the chemical of interest and the peak concentration observed.

Chemical releases that involve gas that have a density substantially different than air may require analysis using approved software codes designed and validated to handle the atmospheric dispersion for such gases (i.e., DOE Software Library codes such as ALOHA).

B.4 Chemical Mixtures

For chemical mixtures and concurrent releases of different substances, consequences should be assessed using the Mixture Methodology “Hazard Index” approach recommended by the Subcommittee on Consequence Assessment and Protective Actions (SCAPA) Chemical Mixtures Working Group (Craig, et. al., 1999).

A brief explanation of this approach and the published journal article are available on the SCAPA website, http://www.orau.gov/emi/scapa/index.htm, under Health Code Numbers (HCN). An EXCEL workbook that automates the implementation of the approach is also available on the SCAPA website.

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

APPENDIX C
FACILITY WORKER HAZARD EVALUATION

The hazard analysis includes the impacts of evaluated hazards on the facility worker (FW). For the purpose of this Standard, the FW is considered to be a worker that is not covered within the scope of the collocated worker, so it includes workers working within the facility).

For each hazardous condition evaluated for the public and collocated worker in the hazards analysis, a qualitative evaluation of unmitigated consequence to the FW and identification of candidate preventive and mitigative controls must be included. While safety management programs (SMP) may include most FW hazard controls, there are conditions that warrant consideration of safety significant structures, systems, and components (SSC). These include the following:

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

Safety significant SSCs are also considered for cases involving significant exposure of the FW to radiological or other hazardous materials. This involves qualitatively evaluating unmitigated consequences in terms of radiation dose, chemical exposure, or physical injury at specified receptor locations. Appendix B provides chemical screening criteria that may be used to screen out low-risk or common chemical hazards from further consideration for the collocated worker with respect to plume pathway consequence. These screening criteria are equally applicable to the FW and may be used accordingly; however, all chemicals must be evaluated against the FW hazards discussed above.

Consequence estimates can rely on experience or can be determined from (1) simple source term calculations, (2) existing safety documentation, and/or (3) qualitative assessment supported by “back-of-the-envelope” calculations. Additional (more detailed) evaluation may be necessary in the form of semi-quantitative analysis, accident analysis, and other such analyses. The Safety Design Integration Team (SDIT) uses its discretion, expertise, and knowledge of facility hazards to select one or more of the above methods appropriate for consequence determination.

For radiological consequences, the suggested evaluation criterion is 100 rem Total Effective Dose Equivalent (TEDE). For chemical exposure, the evaluation criterion is Acute Exposure Guideline Level-3 (AEGL-3) or equivalent (e.g., Emergency Response Planning Guideline-3 [ERPG-3], Temporary Emergency Exposure Limit-3 [TEEL-3]). These criteria are suggested to provide a qualitative sense of proportion to levels that might be considered to have significant impact to a facility worker. By comparing the qualitatively derived FW radiological or chemical consequence to these evaluation criteria, an assessment can then be made about the need for SS preventive or mitigative controls. Where the qualitative consequence assessment yields a result that is not clearly above or below the evaluation criteria, then the need for safety significant controls should be more closely considered by the project.

APPENDIX D
ADDITIONAL FUNCTIONAL CLASSIFICATION CONSIDERATIONS

D.1 Selection and Classification of a Complete Control Set

When controls are selected to perform a safety class (SC) or safety significant (SS) function, the control set must be adequate to fully perform the identified safety function. This control set must include all structures, systems, and components (SSC) that are either required to operate to perform the safety function or required not to fail if that failure would prevent the function from being performed. These SSCs must be classified at the same level (SC or SS), with the following limitation.

The functional classification designation (SS or SC) extends only to the attributes of the SSC involved in providing the safety function. For example, for an SSC identified as having an SC function based solely on seismic interaction, the only safety requirement the SSC needs to meet is that imposed by requirements on structural design for the seismic event.

Preventive control SSCs are designated in a judgment-based process involving many factors, such as effectiveness, a general preference of preventive over mitigative and passive over active, relative reliability, and cost considerations.

SSCs that function to monitor initial conditions assumed in the accident analysis are not required to be classified as SS- or SC-based on the monitoring function if all the following conditions are met.

- They do not generate a signal (indication, alarm, or interlock function) that causes action (operator action or equipment change of state) that is required to prevent or mitigate an accident.
- Their failure is not the initiator of an accident.
- Violation of the monitored parameter is not the initiator of an accident.

D.2 Criteria for Selecting SS Major Contributors to Defense-in-Depth

Selecting major contributors to defense-in-depth that will be identified as SS is an integral part of the hazard analysis process. The result of this selection process needs to be technically defensible. Major contributors to defense-in depth (DID) are identified from the candidate controls in the hazard analyses scenario documentation. These major contributors to DID should be designated as SS SSCs based on consideration of criteria such as suggested below.

- DID controls that are common to multiple accident scenarios may be considered to provide a significant contribution to DID in the context of all of the scenarios taken together and should be considered for classification as SS. In this evaluation, accident scenarios are scrutinized for common hazard control elements that qualify as hazard controls across the spectrum of hazards, considering how often a particular potential control appears in different scenarios. For example, if it is determined that the fire suppression system appears in a significant number of scenarios as a potential Safety SSC, then this would be a criterion for elevating the DID fire suppression system to an SS SSC.
- If a support SSC is common to several SS SSCs (but not necessarily required to ensure operability alone of any single SS SSC) then it should be considered, from a reliability perspective, as a candidate for SS classification.
- If a candidate control further significantly reduces the consequences of an accident scenario that has required an SC or SS control, then this control should be considered for designation as an SS SSC.
- If a candidate control that further significantly reduces the frequency of an accident scenario that has required an SC or SS control, then this control should be considered for designation as an SS SSC.
- The control appreciably reduces the risk of significant energetic events that potentially threaten multiple safety systems.
- If the reliability of a single control (preventative or mitigative) is not as high as desired, SSCs designed to increase reliability by providing multiple layers of protection should be identified as SS SSCs.

APPENDIX E
SAFETY DESIGN STRATEGY

E.1 Introduction

The Safety Design Strategy (SDS) is a tool to guide project design, document safety documentation development planning, and provide approving authorities sufficient information on which to make decisions. It provides a single source for the safety policies, philosophies, major safety requirements, and safety goals for the project. The SDS describes the major hazards anticipated in the facility, how those hazards will be addressed using safety structures, systems, and components (SSC) considering natural phenomena, confinement ventilation, and other significant safety needs. Any risks to these decisions from new technology or assumptions should be identified. In addition, the SDS identifies major safety documentation deliverables to be provided within each project phase.

A statement of DOE expectations for Safety-in-Design at the pre-conceptual stage is intended to address the DOE O 413.3A, Chg 1, requirement for Safety-in-Design planning and a tailoring strategy as related to safety and to provide the basis for development of an SDS during the conceptual design stage. The SDS should address all the elements of the SDS format and content to the degree supportable, appropriate to that design stage. The SDS is expected to be revised and updated as the project matures.

E.2 SDS Format and Content

The SDS should be tailored based on complexity and risk and should reference available information sources where possible. It should also address important aspects that affect the development of the safety design basis documentation or the interface with design and operations or areas that require concurrence (assumptions, calculations, decisions that affect the technical baseline, or the data used to generate hazard and safety analysis required from an Integrated Hazard Analysis). Additionally, the SDS content will vary significantly through the course of a major project that spans several years. As the project moves from conceptual design to preliminary design to final design, construction, and startup, the detailed information within the SDS will change, and the focus of various portions of the SDS will change to be consistent with project needs. The intent of this format and content guidance is to establish the minimum expectation for the types of material that will be addressed in the SDS. The depth of treatment is where tailoring occurs. The intent of the SDS is that it be as detailed as needed to communicate to the decision makers and the Safety Design Integration Team (SDIT) the strategy for successfully integrating safety and design and producing safety design basis documentation that will be approved to allow either entry into the next critical decision or into operation.

1.0 Purpose

This section introduces the SDS for the project. Effectively, this section should simply state that the SDS for the specific project will describe the overall safety strategy, the strategy for certain high-cost, safety-related design decisions, identify key assumptions or inputs that may represent potential risks to those design decisions, and the expected safety deliverables through the project.

2.0 Description of Project/Modification

This section provides a brief description of the project/modification or proposed activity consistent with the level of knowledge of the project phase. Fundamentally, the description should allow the reader to understand the discussion that follows regarding safety strategy. Such details may include mission, proposed location(s), description of major facilities/processes or changes to existing facilities/processes, and major hazards. Aspects that may be relevant to the overall strategy should also be included, such as storage capabilities of hazardous materials, waste streams and processes, and support systems. Reference to other project documents is acceptable.

3.0 Safety Strategy

This section is the core of the SDS and should present the overall safety strategy for the project. The following topics should be addressed in the section.

3.1 Safety Guidance and Requirements

This section should present the overarching philosophies and goals for the project in approaching the hazards involved in the project. Each of the following topics must be explicitly addressed.

- Describe or define the Safety-in-Design approach and philosophies (e.g., provide assurance that a member of the public will be protected from radiological exposure, minimization of materials-at-risk (MAR), passive controls over active, segmentation of hazards, approach to protection of facility worker).
- Define the criteria or approach to safety functional classification, including evaluation guidelines for both radiological and toxicological hazards and for public and worker protection.

- Identify the safety design criteria to be applied to the project (commitment to DOE G420.1-1, -2; DOE O 420.1B, etc.). Overarching requirements are sufficient for this purpose.

3.2 Hazard Identification

This section provides a logical discussion of the major hazards involved in the project and the possible consequences those hazards may pose. An exhaustive list of hazards is not needed; only those that could potentially drive identification of safety class (SC) or major safety significant (SS) SSCs need to be listed.

Hazard identification should be based on initial or assumed hazard inventories. Inventories must be consistent with those used for initial hazard categorization in accordance with DOE-STD-1027-92, Change Notice 1, September 1997. Provide the initial hazard categorization level.

3.3 Key Safety Decisions

Key safety decisions are those that potentially result in significant cost or have resulted in costly rework in past projects. These topics must be explicitly addressed and the strategy justified consistent with the hazard categorization and any associated preliminary consequence estimates. Highlight any key inputs or assumptions that influence these decisions.

- Seismic and other natural phenomena design categorization – Define expected facility design categorization based on initial hazard considerations.
- Confinement strategy – Describe overall approach to facility confinement including use of active confinement system(s); define expected functional classification of any confinement system(s).
- Fire mitigation strategy – Describe overall approach to fire protection including any use of fire barriers, segregation, and similar measures. Fire mitigation strategy may influence confinement strategy significantly.
- Anticipated safety functions – Identify major safety functions, their safety functional classification (SC, SS), and major safety function (e.g., confinement). Any potential need for emergency power for safety purposes

should be identified, particularly with respect to confinement ventilation systems.

4.0 Risks to Project Safety Decisions

Summarize any key risks identified in developing the strategy to the key safety design decisions in Section 3. These are summarized and included in the project Risk Management Plan until appropriate resolution of unknowns or solidification of assumptions. Factors that relate to these risks, such as application of new technology, need for additional data to substantiate assumptions (e.g., new material airborne release fraction [ARF]), hazardous material inventory assumptions and project constraints (e.g., schedule, cost, and location) that could affect design and safety decisions should be identified.

5.0 Safety Analysis Approach and Plan

This section describes the safety analysis process and deliverables planned for the project. A summary of the analysis steps and processes to be used with evolution of design should be sufficient. Deliverables expected to be completed, submitted, and approved should be described for all project phases. Integration with other safety discipline efforts (e.g., Fire Hazards Analysis) is pertinent to describing the project interfaces and synergy. Tailored project approaches (e.g., design/build) should be specifically identified, and safety design basis development should be described sufficiently to facilitate concurrence by approving authorities. Any tailoring approaches selected for satisfying the DOE O 413.3A, Chg 1, requirements for safety documentation should be described.

Major safety analysis tools (e.g., computer codes) to be used must satisfy the requirements of 10 CFR 830 Subpart A and DOE O 414.1C. Any tools not included in the DOE Safety Software Central Registry should be described and justified.

6.0 SDIT – Interfaces and Integration

This section describes strategy for establishing and employing an SDIT within the project. Discussion should address the primary interfaces within the project team that are specifically aimed at facilitating coordination not only with design functions, but with traditional worker safety disciplines, emergency management, and safeguards and security. This may be accomplished in a number of ways, including appropriate representation on the SDIT directly, periodic coordination, and design review meetings. Ultimately, the goal is to ensure coordination among these various interests to ensure development of a design compliant with the various requirements while achieving the overall safety strategy. Also, the role of the SDIT in the broader Contractor Integrated Project Team (CIPT) and Integrated Project Team (IPT) should be described. Often, key project members will comprise more than one of these teams.

Some measure of security is required to be addressed for most DOE facilities. However, for a limited number of facilities, the security interface is of particular importance. Competing requirements are not unusual, and important security requirements can often be classified. The strategy for security design based on input from the Design Basis Threat (DBT) and associated Vulnerability Assessments should be factored into the safety strategy. Engaging security and developing a parallel security strategy is recommended (see section 7.8 of this Standard).

It is critical that the various SDIT discipline roles not be "stovepiped" or narrowly performed by a single discipline. The SDIT has a significant role in developing both the design/facility modification and the associated safety documentation. However, within that team certain individuals need to be the SME or own that portion of the team's efforts.

APPENDIX F
SAFETY-IN-DESIGN RELATIONSHIP WITH THE RISK MANAGEMENT PLAN

Projects are required by DOE O 413.3A, Chg 1, to prepare Risk Management Plans (RMP) to define the roadmap to executing the project within a risk and opportunity environment. DOE O 413.3A, Chg 1, and its guidance describe the process for identification, assessment, and mitigation of project risks. Given the potentially significant costs associated with safety decisions, the integration of safety into the design process needs to also include a strong link between the development of Safety-in-Design and identification of project technical and programmatic risks. With anticipated risks, early identification of possible opportunities to address potential risks allows the project to define appropriate range estimates. Comprehensive risk identification, coupled with an appropriately conservative safety design posture, affords the project the opportunity to execute within the range estimate with a higher degree of reliability. The identification of risks and opportunities associated with the conceptual design along with the appropriate mitigation strategies will be a key component in identifying the contingency cost range for the project in accordance with DOE O 413.3A, Chg 1, expectations.

Developing the risk and opportunities assessment is especially important at the conceptual design stage. This assessment is the foundation that will demonstrate the overall technical risk and maturity of the other technical deliverables associated with the conceptual design package. The addition of opportunities is deliberate since the Safety-in-Design philosophy espoused herein is to make reasonably conservative safety design decisions early in the design process. A conservative posture at the equipment level can sometimes be found later in design to be unnecessarily conservative and lead to avoidable costs. For this reason, opportunities are intended to capture that possible outcome in addition to opportunities for addressing risks in general.

The risk and opportunity assessment of the conceptual design package is the foundation for demonstrating the adequacy of the safety design approach documented in the Conceptual Safety Design Report (CSDR) and overall technical risk and maturity of the other technical deliverables included in the conceptual design package. To be of value to the approval authorities, the risk and opportunity evaluation needs to be robust in identifying unknowns and potential technical issues related to the results of the preliminary hazard analysis; specifically, the selection of hazard controls. Consideration of the risks and opportunities completes the risk “picture” upon which decision makers can appropriately evaluate the proposed project. The risk process should demonstrate prudent conservative decision-making approaches were applied in the conceptual design. As such, it is imperative that all pertinent subject matter experts (SME), such as safety personnel, including criticality experts, engineering designers, and security personnel participate in this evaluation process to properly portray the level of technical maturity in the conceptual design and appropriate mitigation strategies.

If the guidance in this Standard is followed, the hazards analysis process should drive conservative decision making to envelop the bounding case effects of the risks associated with these unknowns and technical issues. Prudent conservative decision-making approaches applied in the conceptual design should ensure that final project costs and schedule baselines are within the range estimate established in the Conceptual Design Report (CDR) or Critical Decision-1 (CD-1) package.

In developing input for the risk and opportunity assessment, all risks that could affect the Safety-in-Design strategies delineated for Hazard Category 1, 2, and 3 nuclear facilities should be specifically considered in the analysis. In determining the overall risk and opportunities for the project, technical risks should be given at least equivalent weight to programmatic considerations. Risks and opportunities associated with Safety-in-Design issues should be specifically annotated in the risk assessment process to enable an understanding of all risks associated with the safety design strategy for the facility (versus programmatic and operational non-safety risks that may be in the risk assessment). This approach will help establish clear definition of Safety-in-Design risks and will enable demonstration of selected mitigation strategies. Risks that affect the safety design basis must be summarized in the RMP. For each risk and opportunity delineated, an appropriate identification of the necessary mitigation strategies is provided as required by DOE O 413.3A, Chg 1. This will enable improved management by the project managers as well as improved demonstration of the maturity and risk of the projects for approval authorities. The summary of the risks and opportunities associated with the Safety-in-Design strategies must be discussed in the Conceptual Safety Design Report (CSDR).

Table F-1 provides a list of typical factors that may be considered in identifying and developing risks and opportunities. This list is not exhaustive and each specific project should be considered on its own. As the project life cycle progresses, the risks and opportunities should be periodically revisited as the design matures and the project moves into different phases. A solid foundation at conceptual design is vital to ensuring that risks and opportunities can be managed through the project.

Where risks and opportunities are identified, appropriate strategies must be developed to address them. The goal should be to appropriately define responses to a realized risk or opportunity such that as preliminary and final designs proceed, actions are taken in accordance with planned mitigation strategies versus emergent issue resolution actions.

Table F-1. Safety-in-Design Considerations for Risk and Opportunity Analysis

Functional Areas	
Design	**Technology**
Undefined, Incomplete, Unclear Process or Safety Functions or Requirements • Potential impact to confinement ventilation strategy • Potential impact to functional classification of SSCs	New Technology application or new application or existing technology • hazards and upset conditions may not be well understood • material form may be one not previously studied for Airborne Release Fraction (ARF) • toxicological effects may not have sound basis
Complex Design Features • Security requirements and impact on safety analysis • Safety-related control system design, interface with safety analysis, and implementation	Unknown or undecided technology • Potential for different materials at risk (MAR) should be assessed with resultant impact to NPH categorization and SSC functional classification • Potential for additional or exacerbated accident scenarios
Assumptions on key utility interfaces • Capacity • Equipment compatibility • Safety precautions in existing utilities • Reliability of existing utilities Design Basis Threat requirements • Potential for changes affecting seismic design or hazards analysis Deferred capability decisions (where hazards could be introduced or increased with added capability in the future) • Potential for added capacity (MAR and SSC functional classification impact) • Potential for addition of significant mass to structure affecting seismic analysis • Potential for impacting confinement ventilation system Safety Class SSC selection confidence • Management judgments related to selection of borderline SSC classifications should be identified • Assumptions critical to consequence results with potential for change (e.g., ARF) Assumptions regarding production objectives • Increases in production objectives could affect MAR, NPH categorization, and/or SSC functional classification Errors and Omissions in Design • Potential for impact to MAR, NPH categorization, and/or SSC functional classification	Scale-up of bench scale technology or process or technology application maturity • Production quantities could introduce unknowns in hazard behavior or material interactions

Functional Areas	
Seismic design margin • 10-year site hazard reevaluation (e.g., change in seismic hazard curve) requirement may impact NP design basis for long-term design/construct projects	
Criticality Design Criteria • Ill-defined criteria can result in potential miscommunication between design disciplines and criticality safety	
Fire Protection • Failure to identify and comply with design requirements of codes, standards, and directives • Failure to integrate FHA with facility hazards analysis • Rigorous fire hazards is necessary to define facility fire mitigation design basis	Field Quality Control • Field installation/Quality Control errors during structure construction can result in design changes to protect seismic basis, separation requirements, etc.

APPENDIX G
HAZARDS ANALYSIS TABLE DEVELOPMENT

This appendix provides an acceptable example of the information needed for the documentation of hazard analysis results. Although other formats may be used to capture this information, a table has been selected as the base format to describe the intended information documentation requirements. This table is prepared with columns or sections corresponding to the headings of sections G.1 through G.10 of this appendix. Sections G.1 through G.10 describe the content of the corresponding column of the table for each hazard analysis accident scenario. This format can be used to document the Preliminary Hazard Analysis (PHA) developed during the conceptual design, or the Hazard Analysis (HA) at the process level developed during the preliminary design. It should be updated as the design matures through final design and transition to operations. As this documentation is a key element of the safety basis, it is maintained after project transition to operations as a basis document for the DSA or a part of the DSA. Although alternate formats may be used to capture this information, the information (e.g., a database), identified in this appendix is required to be developed. The appropriate hazard analysis technique is selected that will be sufficiently sophisticated or detailed to provide an appropriately comprehensive examination of the hazards associated with the facility given the complexity of the operation and degree of design maturity and develop the information required by this appendix.

G.1 Scenario Description

Describe each postulated accident scenario that could lead to the release of hazardous materials. The description should appropriately describe the mechanism(s) that lead to the release of hazardous material. Examples include spills, over-pressurization, deflagration, fire, and similar mechanisms. This description should be as complete as possible for the current design stage to facilitate use in developing controls and their functional and design requirements, as well as support USQ Determinations during operation.

The description should also include an explicit description or reference to the material at risk (MAR), chemical or radiological, as appropriate, involved with or potentially affected in the scenario. As appropriate, describe the effect that the initiating event has on the major facility structures, systems, and components (SSC), primarily those that could release energy or radioactive/hazardous material.

Scenarios identified during the Preliminary Hazards Assessment (PHA) process for conceptual design will be facility-level or major MAR location events for the facility. The key at conceptual design is to review the release mechanisms for the major MAR inventory locations sufficiently to ensure that high-cost safety functions have been identified and included in the project design and cost estimates.

G.2 Initiating Event Frequency

Provide the conservatively assigned frequency of the initiating event or of the accident itself, where a series of events contribute to a release of material, such as fire events or a natural phenomena hazard (NPH) followed by spill or fire. The goal is to qualitatively bin the event frequency sufficiently to aid in event prevention and mitigation strategy selection (e.g., Anticipated, Unlikely, Extremely Unlikely, and Beyond Extremely Unlikely). The initiating event frequency should be consistently applied as the initiator frequency.

G.3 Unmitigated Consequence Evaluation

Describe the hazardous material release with respect to facility workers in each unique location, collocated workers, and offsite personnel that are affected.

Identify the consequence to each receptor for the event. Although detailed knowledge may not be available, it is important to make appropriately conservative determinations of dose consequences so that the safety control selection is also conservative. When available, quantitative information should be used as a guide for consequences due to chemical or radioactive material releases based on bounding assumptions. However, binning into defined ranges is preferred and specific values are not required. This is especially true for worker consequences, which are intended to be qualitative.

Assumptions established as a part of the consequence determination should be identified, in order to provide the technical basis for parameters of interest. Particularly, the hazardous material inventory, airborne release fraction, and damage ratio and their bases should be described. Reference appropriate calculations that support the identified consequence, when they have been performed.

While an assessment of the level of accident consequences is necessary to determine the need and safety classification of SSCs providing protection of in-facility workers, these assessments should be, at most, “back of the envelope” calculations, to give a sense of the order of magnitude of the doses. In the case of in-facility worker consequences, especially immediately involved workers, the assumptions that could be made in the course of any more definitive calculations could easily affect the results by orders of magnitude. Thus, such calculations, if used to apply a numerical criterion, would divert attention from good safety decisions to arguments about the calculations and assumptions during the review.

G.4 Safety Functions

Based on the release event description, list the safety functions needed to prevent or mitigate the MAR release event. The safety function is a qualitative statement of a function that prevents an initiating event or mitigates the outcome. The safety function is the desired result from an administrative action or a system, structure, or component and should be stated in a general way, while still describing the preventative or mitigative action. The safety function in this entry should not specify a system, structure, or component (SSC) or otherwise state how the safety function is satisfied. This has two purposes: (1) it provides flexibility in SSC selections; and (2) it ensures that the specific functional and design attributes for a selected SSC fulfill the defined higher-level safety function identified for the event.

- The safety function statement serves as a link between the hazard analysis and the safety SSCs by defining the overall objective and top-level functional requirements for the SSC. The top-level functional requirements are those performance parameters of special importance because they are specifically relied upon in the safety analysis.
- Safety functions should not be predicated on the SSCs or Administrative Controls (ACs) that may be chosen to provide the function. The opportunity for novel and improved solutions is reduced when the solution drives the requirement.
- The safety function statement for each SSC or AC within a facility should be sufficiently specific to enable assigning appropriate supporting ACs or SSCs to fulfill the needed safety function completely.
- Safety functions should include the following:
  - situations and any general accident types during which the function is required to be met;
  - specific functional needs that prevent, detect, or mitigate an event; and
  - sufficient description to enable clear functional requirements and later, design requirements and acceptance limits for those SSCs ultimately chosen to meet the top-tier safety function described.

G.5 Preventive Features (Design and Administrative)

List all SSCs and ACs that have the potential to prevent the event initiator or reduce the frequency of accident progression. This should be consistent with the approach (initiator or event progression) used to determine the frequency (see G.3 above). In the early stages of the conceptual design process, this listing may include SSCs that are currently not part of the conceptual design; but, if selected, would be added to the conceptual design. Initiating events that cannot be prevented, such as NPH events that lead to a release, should be listed as not applicable (N/A).

This listing will be used to select the suite of safety systems, important to safety systems, and/or defense in depth SSCs for the MAR release events. When complete at Critical Decision-1 (CD-1), only SSCs actually present in the conceptual design should be included.

G.6 Method of Detection

Identify all SSCs and administrative functions that could detect the event. This would include SSCs that may or may not be selected, as well as direct observation by the operations staff. In the early stages of the conceptual design process, this listing may include SSCs that are currently not part of the conceptual design.

Although the instrumentation systems are generally not well defined at the conceptual design stage, the expected detection methods to be included in the preliminary design should be included in the PHA tables. This provides a means for providing future design guidance and a basis for estimating equipment costs, in particular for systems that may be a high-cost driver for the project. An example of this is when instrument air would be needed to support a safety class (SC) detection system. This could lead to the compressor systems for the air being SC and, ultimately, becoming a high-cost impact to the project. Therefore, it is important in conceptual design to consider this sufficiently to capture any major cost needs at a minimum during conceptual design. For prevention, this will identify instrumentation that will detect the event is about to occur.

When complete at CD-1, only SSCs in the conceptual design should be included.

G.7 Mitigative Features (Design and Administrative)

List all SSCs and Administrative Controls that potentially could mitigate the event by limiting the consequences after the event has happened. In early stages of the conceptual design process, this listing may include SSCs that are not currently part of the conceptual design. Consideration of the following mitigative systems and design features should be included:

- fire suppression/detection;
- confinement ventilation;
- emergency power;
- nuclear criticality design features and/or alarms, consistent with the guidance in DOE-STD-3007-2007 (if the facility will have at least a minimum critical mass of fissionable material);
- seismic design, including addressing level of confinement for primary confinement system (building structure); and
- flammable gas controls.

When complete at CD-1, only SSCs in the conceptual design should be included.

G.8 SSC Safety Control Suite and Safety Functions

This section summarizes the suite of hazard controls, including safety SSCs that will be relied upon to detect, prevent, or mitigate each event. Appendices A, B, C, and D and the requirements in DOE O 420.1B are key inputs to the identification of the safety control suite selected, the functional classification of selected SSCs, and the NPH requirements.

The hazard controls identified in the conceptual design PHA are preliminary until accident analysis confirms their need and validates that they are the correct and adequate controls for the event. The identification of the hazard controls should be reasonably conservative to establish an appropriate cost and schedule basis for the project. The selection of hazard controls is iterative. If, after selecting one or more of the available controls, the mitigated consequence still exceeds the applicable threshold criteria, additional controls must be selected or identified and classified accordingly. In some cases, it may be prudent to use multiple controls where only one may be required to effectively prevent or mitigate the event. Where SACs are included in lieu of an SSC, an explanation should be provided. The final list of selected controls should be provided in the Preliminary Hazards Analysis (PHA) tables.

G.9 Mitigated Consequences

The estimated consequences for the identified receptor after applying the hazard controls are listed. During conceptual design, the quantitative results for the unmitigated events may not be known. In this case, the mitigated results are qualitatively estimated based on a reduction factor on the unmitigated consequences. Once the accident analysis is performed, this section will be updated with the results of this quantitative analysis. If an event is prevented or the frequency is reduced by application of the hazard controls, this result is reported in the mitigated consequence column as “prevented.”

This information is input to the demonstration of sufficiency of the control suite selected in the Conceptual Safety Design Report (CSDR).

G.10 Planned Analyses, Assumptions and Risk/Opportunity Identification

List remaining analysis or assumption validations and risk/opportunities associated with the selected strategies. The bounding events that require further analysis are identified in the PHA. The events selected are grouped into accidents that are representative of the hazardous conditions. The accidents are defined in such a way as to predict the consequences so as to be bounding for all similar events with the same control suite. Other events, for which the need for hazard controls (or the functional classification or NPH criteria) was not obvious, should also be evaluated in more detail (potentially quantitatively) later in the preliminary design phase. This will ensure that the selection for each safety control has a firm basis and that the assigned functional classifications and design criteria are also based on objective determinations.

Assumptions used in the PHA process must be verified as the design matures. As an example, the facility Material-at-Risk (MAR) used in the hazards analysis may have been based on a highly conservative assessment of tank volumes and concentrations. When the final documents and piping and instrumentation diagrams (P&ID) are issued in preliminary design, the actual tank volumes should be used in the accident analyses. Other assumptions concerning the event progression, such as impact to SSCs, must also be verified. Remaining evaluations to be performed must be identified.

It is essential that potential risks and opportunities to be fed into the Risk and Opportunity Assessment as the safety control suite is selected. The presentation of risks and opportunities associated with the strategies are essential facets for risk-informed decision making in the authorization for the project to proceed to preliminary design.

G.11 Hazards Analysis Table

The final HA table (or equivalent) includes the items discussed above and portrays the hazard scenarios associated with the facility and the safety systems that will detect, mitigate, or prevent unacceptable MAR releases. The table should present the logical binning of events evaluated (e.g., fire, operational events, fire, NPH). In essence, these scenarios are those from which the design basis accidents (DBA) for the facility are selected. The table provides valuable information to be included in the risk and opportunities analysis and needed studies to validate key assumptions. This table portrays the functional safety attributes for the facility safety systems that are to be incorporated into the conceptual design and cost estimates. The final table will be used as the foundation for development of the CSDR, which will describe the events evaluated and the safety control suite in a format that can be used as the foundation for a final Documented Safety Analysis (DSA) for the facility.

APPENDIX H
CONCEPTUAL SAFETY DESIGN REPORT

H.1 Introduction

DOE O 413.3A requires a Conceptual Safety Design Report (CSDR) as a part of the approval package for Critical Decision-1 (CD-1) approval of the conceptual design. The purpose of the CSDR is to summarize the hazards analysis efforts and Safety-in-Design decisions incorporated into the conceptual design along with any identified project risks associated with the selected strategies. The DOE review of the CSDR, documented in a Conceptual Safety Validation Report (CSVR), confirms that the preliminary safety positions adopted during conceptual design constitute an appropriately conservative basis to proceed to preliminary design. These positions include the following:

- preliminary hazard categorization (HC-1, 2 or 3) of the facility;
- preliminary identification of facility design basis accidents (DBA);
- assessment of the need for Safety Class (SC) and safety significant (SS) facility-level hazard controls based on preliminary hazards analyses and DBA;
- preliminary assessment of the appropriate seismic design basis (seismic design category and limit state) for the facility structure and major hazard controls; and
- position(s) taken with respect to compliance with the safety design criteria of DOE O 420.1B or any alternate criteria proposed.

A major purpose of conceptual design is to propose a design concept and safety strategy that supports the mission to be accomplished by the facility and a conservative cost estimate. The design information that is available at the conceptual design approval stage is very likely to change and mature in various aspects as preliminary design proceeds. The design package may very likely propose several alternative approaches to some aspects of the design and also contain some aspects that require more research and development as part of the preliminary or even final design stage. Therefore, a rigorous safety assessment of the conceptual design is not needed as part of the CSDR review. That assessment is more properly a part of the more broadly focused design reviews during preliminary and final designs, which should include full participation by those DOE safety specialists that will be responsible for Safety Validation Reports (Conceptual and Preliminary) and the Safety Evaluation Report (SER) for the project. However, part of the CSDR review should assess the implementation of the principles of the hierarchy of hazard controls. The review should confirm that the process was implemented (at the facility level of hazard controls), assess the acceptability of the decisions made, and identify any safety issues that require further study. An important approval basis for the CSDR is that the safety system selection provides an adequate basis for proceeding to the preliminary design stage.

In reviewing the CSDR, DOE verifies that the safety design basis was developed in a reasonably conservative manner and that the risk associated with significant redesign required due to the addition of new or different is minimal. The review confirms that the hazards analysis process is complete commensurate with the available detail in the conceptual design, assesses the acceptability of the decisions made with respect to hazard controls, and includes identification of any safety issues that require further study. The Risk and Opportunity Assessment for conceptual design is also reviewed with the CSDR to verify that the technical uncertainties in the safety design basis are identified and that the risk-handling strategy (strategies) for each risk element has bounded the risk for proceeding with the project. The Risk and Opportunity Assessment is essential to enable the project risks to be understood by the project team and the Federal Project Authorization Executives.

H.2 CSDR FORMAT AND CONTENT GUIDE

1. INTRODUCTION

a. Facility and Mission Overview

Identify the facility and present general information on the background of the facility as it relates to the use of the project scope. Present the current mission statement. Present any relevant information (e.g., short facility life cycle, anticipated future change in facility mission, approved DOE exemptions) affecting the extent of Safety-in-Design approaches documented in the CSDR.

b. Site Location

Provide a description of the facility location, including the physical and institutional boundaries, relationship and interfaces with nearby facilities, facility layout, and significant external structures, systems, and components (SSC) interfaces (e.g., utilities) as they pertain to the hazard analysis.

If multiple sites are under consideration, describe each of them.

2. CONCEPTUAL DESIGN DESCRIPTION

a. Facility Structure and Layout

Provide information necessary to perform facility-level DBAs (as described in section 4.2 of this Standard). Such information as basic floor plans, material-at-risk (MAR) locations within the structure, general dimensions, and dimensions significant to the hazard analysis activities is necessary. Supply information to support an overall understanding general arrangement of the facility as it pertains to hazard analyses topics to be described in later sections of the CSDR.

b. Process Description

Describe the individual processes within the facility to support understanding of the overall postulated facility-level MAR release events and Safety-in-Design strategies taken to prevent or mitigate the events described. Include details as necessary on basic process parameters, including summary of types and quantities of hazardous materials, energy sources, process equipment, basic flow diagrams, and operational considerations associated with individual processes or the entire facility, including major interfaces and relationships between SSCs. Information is expected only at the level of conceptual design as described in Section 4.2 of this Standard. The intent is to supply information sufficient to understand facility-level MAR release events.

3. PRELIMINARY HAZARD CATEGORIZATION

a. Hazardous Material Inventories

Estimate the total inventory (with associated uncertainties) of radionuclides, hazardous chemicals, and flammable and explosive materials used or potentially generated in facility processes. Present the results either by direct inclusion of or by reference to the hazard identification data sheets in the Preliminary Hazard Analysis (PHA). The attributes of hazards identified in this section are the basis for subsequent hazard evaluation and accident analysis in future project stages.

This inventory must describe the maximum inventories of hazardous materials that are anticipated to be in the facility during its operational life. To the extent possible, the inventory is specified by component and location within the conceptual designed facility. This should be in sufficient detail to support a facility-level PHA that would, in turn, support the definition of facility-level DBAs or bounding accidents associated with the inventory locations (e.g., tanks, storage, process vessels) and the associated preliminary lists of SC and SS SSCs.

For the purposes of preliminary facility hazard categorization (before final design), the use of Type B containers to exclude MAR from the facility inventory may be used. During final design, material in Type B containers with current certificates of compliance may be excluded from the inventory for final hazard categorization when safety analyses demonstrate that containers can withstand all accident conditions.

b. Comparison of Inventories to Threshold Quantities

Compare the radionuclide and fissile material inventories with the threshold quantities in Table A.1 of DOE-STD-1027-92, Change Notice 1, September 1997, and identify the preliminary hazard categorization. When segmentation is proposed, identify segment boundaries and hazard inventories and justify the independence of the segments. Identify the individual segment preliminary hazard categorizations.

The preliminary hazard categorization must be in compliance with DOE-STD-, Change Notice 1, September 1997-92, as required by 10 CFR 830.202. The information compiled in the preliminary inventory of hazardous materials is used for this purpose. Note any likely issues that may change final hazard categorization, such as obvious inconsistencies with the basis of the DOE-STD-1027-92, Change Notice 1, September 1997, Table A.1. For example, if facility processes include the possibility of vaporization of radioactive materials, for which DOE-STD-1027-92, Change Notice 1, September 1997, assumed an airborne release fraction (ARF) of 1 E (-3), it should be noted that final hazard categorization would need to be based on an ARF of 1.0. Similarly, if the facility is intended for the storage of vitrified "logs," it should be noted that an ARF of 1 E (-6) might be appropriate in final hazard categorization.

4. DESIGN BASIS ACCIDENTS

a. Facility-Level DBAs

Provide a summary table identifying postulated hazardous material release events. The goal is to provide a perspective on facility hazards by summarizing the major events or hazardous situations (e.g., fires, explosions, loss of confinement) that were postulated in the facility during the PHA activities.

During the conceptual design stage, a facility layout, including process flow diagrams and locations of MAR will be developed. Bounding accident scenarios involving the MAR locations, such as fires, explosions, and seismic induced failures, can be postulated.

b. **Unmitigated DBA Analyses**

Appendix A and Appendix B of this Standard provide radiological dose- and chemical exposure-related criteria and guidance respectively. Appendix A criteria are to be used for the classification of SSCs as Safety Class or safety significant on the basis of unmitigated accident dose analyses and for the application of seismic design guidance of ANSI/ANS 2.26, *Categorization of Nuclear Facility Structures, Systems, and Components for Seismic Design*. Appendix B criteria are suggested for classification of SSCs as safety significant based on chemical hazards. Application of the criteria requires unmitigated accident analyses for the facility-level DBAs.

For each DBA:

1. Identify the release category by individual title, category (i.e., operational, natural phenomena, external) and general type (e.g., fire, explosion, spill, earthquake, tornado).
2. Describe the source-term determination for the event category. Discuss all parameters used to derive the source term. This definition includes the MAR (as derived from the hazard identification), the damage ratio (DR) and the ARF. The degree of conservatism believed to be present in the calculation needs to be consistent with DOE-STD-3009-94, CN 3, Appendix A, definitions and requirements.
3. Present the results of the DBA analysis, both to the collocated worker at 100 m and to the public according to the guidance of appendices A and B of this Standard.
4. Compare the DBA results to guidance for safety system classification and seismic design criteria of Appendix A of this Standard and the suggested criteria for chemical hazards of Appendix B of this Standard.

c. Preliminary Selection and Classification of Safety SSCs

For each DBA, the following information is presented, based on the analyses of the DBAs in the PHA and the safety classification criteria in appendices A and B of this Standard:

i. preliminary identification of facility-level safety functions; and, if proposed, the associated Safety Class and SS structures, systems, and components (safety SSCs) and their necessary support systems;

ii. requirements for the identified safety functions and, if proposed, for the associated safety SSCs; and

iii. applicable structural design basis associated with each system (seismic design criteria and PC categories for other NPH).

Based on unmitigated analyses of the facility DBAs, candidate preventative and mitigative safety SSCs can be identified and classified, according to the guidance of appendices A through D.

This section provides a discussion of safety functions and design criteria for selected safety SSCs; for example, the required safety functions for the confinement, active ventilation, fire protection, and electrical power and distribution SSCs. This section should also describe the rationale from a Safety-in-Design perspective for the following major systems (including NPH design expectations) recognized as having significant cost impact if changed later in the project cycle:

- facility structure;
- facility hazardous material confinement;
- fire protection; and
- emergency power

As described in Appendix A, DOE is adopting ANSI/ANS 2.26, *Categorization of Nuclear Facility Structures, Systems, and Compon*ents, for the purpose of new facility and major modification design. Once the Seismic Design Category is identified for facility SSCs, the appropriate Limit State for those SSCs should be selected, based on their safety function. See Appendix A and ANSI/ANS 2.26 and its appendices for guidance.

5. SECURITY HAZARDS AND DESIGN IMPLICATIONS

This section, depending on security classification considerations, may have to be a placeholder that references a classified report. That report would describe the facility design aspects that respond to Design Basis Threat (DBT) information, the results of the VA, and would address how the security design aspects take into account facility safety issues in protection of workers and the public.

DOE Security Orders (i.e., 470 series) have requirements that may affect design and the safety aspects thereof for some facilities. These directives should be reviewed as part of the design process. In particular, there are requirements regarding the DBT, the implementation of which may have implications regarding public and worker safety. The concept considered in ensuring that both the security requirements and safety requirements are satisfied for any security installation at a facility meeting the DBT is that the approach (1) encompasses all threats for which the security system is required to be designed based on the DBT and/or VA, (2) be employed in an effective manner to assure neutralization and protect the national security, and (3) assures that safety requirements are met.

6. NUCLEAR SAFETY DESIGN CRITERIA

a. Approach for Compliance with Design Criteria

Provide a listing of the applicable safety design criteria of DOE O 420.1B, *Facility Safety*, and a brief summary of the implementation approach being taken in the project for each design-related criterion. Programmatic criteria are not expected to be discussed. This section is meant to be a description of, or a roadmap to, the specific information that demonstrates the implementation approaches for the various criteria, not a detailed re-write of information included in other sections of the CSDR or other available project documentation.

Note that some of the attributes applicable to the project may not be items that would be addressed by the hazards analysis process (e.g., provisions for decontamination and decommissioning and provisions for radiological controls for ALARA expectations). These items still are expected to be included as applicable criteria and discussed in this section of the CSDR to demonstrate that the key items that will be in the final DSA are being considered appropriately in the conceptual design process.

The nuclear safety design criteria of DOE O 420.1B are primarily located in both the Order and Attachment 2 to the order in Chapter I, "Nuclear and Explosives Safety Design Criteria"; but additional applicable safety design criteria can be found in Chapter II, "Fire Protection"; Chapter III, "Nuclear Criticality Safety"; and Chapter IV, "Natural Phenomena Hazards Mitigation." The implementation guides for these chapters should also be followed.

To the extent possible at this stage of design, for the selected safety SSCs, tie the structure or system level specific criteria (e.g., DOE-STD-1020-2002, ANS 2.26 for natural phenomena criteria in DOE O 420.1B) to the DOE O 420.1B criterion that it satisfies. Programmatic criteria (e.g., system engineer program, configuration management) are not expected to be discussed.

b. Exceptions to Design Criteria

Provide, for any exception to the high-level safety design criteria in DOE O 420.1B, or the implementing standards listed in DOE G 420.1-1 and listed in Section 6.a, the project's alternative criterion and a justification for the alternative. The justification must show why the alternative is an acceptable criterion or standard.

7. OTHER CONSIDERATIONS

a. Planned Studies or Analyses

Describe any key planned technical studies essential for development or validation of the safety design basis that will be accomplished in preliminary/final design. These studies may be necessary to confirm key assumptions or key process component equipment selections that could affect safety. The primary source for this information is the PHA and Safety Strategy.

b. Safety-in-Design Risks and Opportunities

Summarize the Safety-in-Design risks and opportunities from the CDR. The intent of this summary is to provide an overall perspective of the risks and opportunities associated with the Safety-in-Design strategies considering the maturity of the project, the remaining technical studies, and the mitigative and preventive strategies selected for the recognized preliminary design basis events. Describe only key risks and opportunities and the associated mitigation strategies that are important to be recognized by the approval authority. These discussions are intended to support a risk-informed decision regarding progressing to preliminary design.

c. Lessons Learned From Previous Experience Involving Major Systems

In this section, discuss the logic used to select the safety-related functions for SSCs that may generate significant cost changes to the project if changed in later stages of the project. This logic may be based on lessons learned from previous experience involving major systems.

It is important for safety SSCs be identified early in the design process. Otherwise, costly upgrades to the facility design could occur. When a safety classification is unclear for a major SSC (based upon very preliminary analysis), a higher level of categorization should be the default position early on until the analysis progresses to the point that a confident and defensible determination can be made for a lower level.

When followed correctly, the hazard and accident analysis process should supply a reproducible logic for safety SSC choices. Specific examples of potential safety SSCs include the following:

- fire suppression;
- fire detection;
- confinement ventilation;
- emergency power;
- nuclear criticality design features and alarms;
- seismic design, including addressing level of confinement for primary confinement system (building structure); and

- flammable gas controls.

These items have the potential for large cost and schedule impacts if their design expectations are added later in the project life cycle.

APPENDIX I

PRELIMINARY AND FINAL DESIGN STAGE SAFETY DOCUMENTATION

I.1 Introduction

I.1.1 Preliminary Safety Design Report

The Preliminary Safety Design Report (PSDR) should update the information in the Conceptual Safety Design Report (CSDR), if needed (i.e., if the information has changed). In addition, more detailed site information of the type that can affect Safety-in-Design should be provided (e.g., location of nearby facilities and external hazards, meteorological information for dispersion analyses, seismic and other natural phenomena information).

PSDR review and approval is very important during the design process. Decisions made and approved as a result of preliminary design reviews and documented in the PSDR will provide the basis for the approach for detailed design and construction. Decisions that are reversed after this stage, for whatever reasons, can have significant impacts on overall project cost and schedule. It is essential that contractor and DOE safety personnel be totally engaged and fully participate in design reviews during this stage, so that their views and advice can be considered in the design in a timely fashion.

There should be a crosswalk between the top-level safety design criteria of DOE O 420.1B and its implementation guides (e.g., DOE G 420.1-1 and DOE G 420.1-2), or any approved substitute criteria and implementation, and the specifics of the design description and the specified Safety Class (SC) and safety significant (SS) structures, systems, and components (SSC). This should include any SSCs that are intended to become design features in operational technical safety requirements (TSRs). It is not necessary for the full details of consensus design codes and standards to be listed in the PSDR. These details should be in the documents available for the design reviews and should be fully scrutinized during design reviews as part of safety personnel participation in those reviews. The PSDR should, however, include the identification of any codes and standards used that are not included in DOE G 420.1-1 and DOE G 420.1-2 guidance and a brief description regarding why they are appropriate. The basis for tailoring of codes and standards should be provided when tailoring is required. See Appendix B of this format guide.

The bases of the PSDR approval in a Preliminary Safety Validation Report (PSVR) are primarily focused on the adequacy of the hazards analyses and selection and classification of the hazard controls, including consideration of the application of the principles associated with the hierarchy of controls. Further, the PSVR evaluates the commitments made in the PSDR and design documents to determine that, if carried through in detailed design, they would result in a final design and a constructed facility that could be approved for operations, without major changes. The review and approval specifically address the acceptability of the design implementation in complying with the nuclear safety design criteria of DOE O 420.1B, or the acceptability of alternate safety design criteria and alternate codes and standards that are proposed and their implementation in design.

Because the design is not complete at this point in the process, adequate Safety-in-Design for the preliminary design is based primarily on the identification of viable engineered solutions to nuclear design requirements and the specification of an adequate set of more detailed safety design requirements that are integrated with the safety analysis. The following points are to be demonstrated in the PSDR.

- The design addresses the nuclear facility design requirements of DOE O 420.1 as described in PSDR, Appendix B.
- The design is integrated with safety analyses as described in Section 3.
  - A viable design solution (e.g., safety SSCs) is identified to provide the safety functions required by the hazard analysis.
  - The unmitigated accident consequence assessment properly indicates the required functional classification (i.e., Safety Class vs. safety significant) and seismic and other natural phenomena hazard (NPH) design requirements (i.e., the proper seismic design criteria (SDC) for seismic design and PC for other NPH design).
  - The analysis of DBAs identifies the functional requirements and accident conditions (e.g., environmental qualifications) that the safety SSCs need to address.
- Appropriate supplemental design criteria (DOE G 420.1-1, Chapter 5) are specified for safety SSCs, as described in PSDR Chapter 4.
  - General requirements for safety SSCs are specified (e.g., conservative design features, design against single-point failure, environmental qualification, safe failure modes).
  - Based on the functional classification and the safety SSC design function, appropriate codes and standards are specified

and tailored, as needed, or alternate codes and standards are identified and justified.

- Technical studies still needed to complete the safety design are identified and described.
- Safety design risks and risk mitigation strategies for the final design phase are identified.

I.1.2 Preliminary Documented Safety Analysis

The PDSA, as opposed to the hazards analysis (HA), demonstrates the adequacy of the design from the safety prospective. As with the design, it is not necessary to show the progression of the design that led to the final choices, only those final choices, and the justification for their adequacy. The PDSA format and content discuss how this information is documented.

Demonstrating safety design adequacy for final design is focused on demonstrating that the safety design requirements specified at the end of preliminary design have been satisfied and describing the mitigated condition for hazards and accidents with the hazard controls applied.

To provide a baseline understanding of the adequacy of controls, the accident analysis in the PDSA should describe how the selected controls adequately prevent/mitigate the accidents, including how the controls provide defense in depth, if warranted, based on accident frequency and control reliability. The analysis should provide an adequate understanding of the baseline mitigated consequences for the facility. The discussion puts the hazard controls' effectiveness in accident context and also provides the baseline safety analysis for the evaluation of changes, as the facility DSA is developed for the transition to operation.

This Standard anticipates that the eventual safety basis for the facility being constructed or modified is based on the methodology of DOE-STD-3009-94, CN 3. If a different safe harbor is applicable to the project or modification, the Safety Design Strategy should establish that expectation, and the format of the PSDR/PDSA, as provided in this appendix, should be modified as appropriate. However, the expectations for integration of safety into the design process and application of nuclear safety design criteria apply to all projects and modifications within the scope of this Standard. Application of an SDS using the existing safety documents created under DOE-STD-3009-94, CN 3; DOE STD-3011-2002, *Guidance for Preparation of Basis for Interim Operation (BIO) Documents*; or DOE-STD-1120-2005, *Integration of Environment, Safety, and Health into Facility Disposition Activities*, could be appropriate for legacy facilities or departmental decontamination and decommissioning (D&D) activities.

I.2 PSDR/PDSA FORMAT AND CONTENT GUIDE

The project documentation describing the Safety-in-Design for the preliminary design consists primarily of the Hazard Analysis Report (HA) and the PSDR. The project documentation describing the Safety-in-Design for the final design consists primarily of the PDSA. The PDSA is an evolution of the PSDR. The format and content for the PSDR begins to build toward a PDSA, and the PDSA will build toward a DSA that will form a key part of the safety basis for the operating facility. This format and content guide often refers to “the document” meaning the PSDR or the PDSA. It is intended that the content of a PSDR or PDSA be commensurate with the stage of Safety-in-Design that it is intended to document. For example, hazards analyses that are documented in a PSDR would be expected to include process hazards analyses and process level hazard controls. The PDSA would be expected to include activity level hazard controls.

EXECUTIVE SUMMARY

PURPOSE. The Executive Summary provides an overview of the facility Safety-in-Design approach 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-in-Design as documented in detail in the remainder of the document. The PSDR may be relatively short and higher level and may not warrant an executive summary whereas the PDSA is more detailed and, therefore, an executive summary is recommended.

E.1 FACILITY MISSION

This section identifies the facility for which the document has been prepared and presents general information on the mission. Clearly present the mission statement for which the PSDR/PDSA documents the Safety-in-Design approach (e.g., the purpose for which authorization to proceed to final design is sought).

Present any relevant information (e.g., short facility life cycle, anticipated future change in facility mission, approved DOE exemptions) affecting the extent of safety analysis documented in the document 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).

E.3 FACILITY HAZARD CATEGORIZATION

This section provides a statement of the facility hazard category as determined in accordance with DOE-STD-1027-92 , Change Notice 1, September 1997. 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 the following:

- description of the facility operations analyzed in the document;

- summary of the significant accidents resulting from the facility processes, natural events and external man-inducted hazards; and
- summary of the main preventive and mitigative engineered features (SSCs), their functional classification (i.e., safety class or safety significant), and associated NPH performance category, and seismic design category.

E.5 ORGANIZATIONS

This section identifies the prime contractors responsible for facility design and participants (including consultants) in the Safety-in-Design process.

E.6 SAFETY-IN-DESIGN CONCLUSIONS

This section provides a brief assessment of the appropriateness of the facility Safety-in-Design approach. As part of this summary, this section would identify any Safety-in-Design issues significant to project risk (e.g., cost and schedule) and risk mitigation measures applied to address them.

E.7 DOCUMENT ORGANIZATION

This section provides a guide to the structure and content of the document (e.g., a table that indicates where the requirements of this Standard are addressed, its sections, and appendices) if the format in this appendix is not followed. If the main body of the document parallels the format delineated in this Standard, a simple statement to that effect will suffice.

Chapter 1
Site Characteristics

PURPOSE. This chapter provides a description of site characteristics necessary for understanding the facility environs important to integrating safety into the design. Information is provided to support and clarify assumptions used in the hazard analyses to identify and analyze potential external and natural event accident initiators and accident consequences external to the facility. 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 may not be required if consequences can be shown to be limited to the facility itself. Note, however, that if chemical hazards are present in a Hazard Category 3 facility and they 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; that is, can challenge the evaluation guideline (see Appendix A of this Standard, section A.2.1). 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.

If the final site selection is not complete, information for siting options may need to be provided.

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 SITE DESCRIPTION

This section describes the site boundary and facility area boundary.

1.2.1 Geography

This section provides basic geographic information, such as the following:

- 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; and
- additional detail maps, as needed, to present near plant detail such as orientation of buildings, traffic routes, transmission lines, and neighboring structures. (Note: This level of detail is typically not necessary for the PSDR.)

1.2.2 Demography (Not required for PSDR)

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 (e.g., schools and hospitals) to the degree warranted by potential offsite consequences. The minimum area addressed is defined by the area significantly affected by the accidents analyzed in Chapter 3, “Hazard Analyses, Accident Analysis, and Control Selection.”

1.3 ENVIRONMENTAL DESCRIPTION

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

1.3.1 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.

1.3.2 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. (Note: hydrology is not typically a significant input to the safety analysis required for a PDSR. Therefore, this section is not required for the PDSR, unless there are unique features of the proposed facility, such as a high aquifer level that interfaces directly with the building structure.)

1.3.3 Geology

This section provides the geological information necessary to understand any regional geological phenomena of concern for facility operation and possible effects on seismic structural design. Describe the nature of geotechnical investigations performed and provide the results of the investigations. Include geologic history, soil structures, and other aspects of the geologic character of the site.

1.4 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 Analyses, Accident Analysis, and Control Selection.”

1.5 MAN-MADE EXTERNAL ACCIDENT INITIATORS

This section provides identification of specific man-made external events associated with the site (e.g., 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 Analyses, Accident Analysis, and Control Selection.”

1.6 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 affect the facility under evaluation. Summarize assumptions supporting the analysis in Chapter 3, "Hazard Analyses, Accident Analysis, and Control Selection."

1.7 EVALUATION OF SITING CRITERIA

This section addresses the siting criteria used in selection of the site. If the siting criteria used in DOE G 420.1-1 are used, discuss how the criteria are met by the site; if they are not met, discuss the impact of not meeting them. If alternative siting criteria were selected, discuss them and explain how well they were met.

Chapter 2
Facility Description – Preliminary Design

PURPOSE. The purpose of this chapter is to provide the facility and process information necessary to support the hazard analysis and also to describe key aspects of Safety-in-Design. However, this chapter does not include information at the level of functional requirements and performance criteria; that information is provided for safety SSCs only, and the information is provided in Chapter 4. In the basic description of safety SSCs, their categorization as safety class SSC or safety significant SSC should simply be noted.

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 analyses. The facility description will 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 subject to hazard analysis. Significant subjects typically include the location, quantity, and nature of hazardous materials; energy sources that could disperse these materials, including combustible or explosive materials; and significant pathways for release. In addition, for aspects that are important to Safety-in-Design, sufficient description is provided to demonstrate that the preliminary design addresses the nuclear design requirements of DOE O 420.1B, as appropriate for preliminary design in the PSDR and as appropriate for final design in the PDSA.

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 major design codes, standards, regulations, and DOE Orders that are required for establishing adequate Safety-in-Design for the facility; however, it is not intended to be a comprehensive listing of all industrial standards or codes or criteria. Project requirement documents (e.g., Functional and

Operational Requirements, Design Criteria documents) may be referenced as appropriate.

2.3 FACILITY OVERVIEW

This section includes a brief overview of the facility mission, 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, and dimensions significant to the hazard analysis activity. Supply information to support an overall understanding of the facility structure and the general arrangement of the facility as it pertains confinement and the hazard analysis. (Note: Less detail is expected in the PSDR and more detail is expected in the PDSA, consistent with the design stage.)

2.5 PROCESS DESCRIPTION

This section describes the individual processes within the facility. Include information on basic process parameters, 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. For the PSDR, process flow diagram level of detail is appropriate; for the PDSA, more detailed information is expected (e.g., piping and instrumentation diagram level of detail).

2.6 SUMMARY OF SAFETY CLASS AND SAFETY SIGNIFICANT STRUCTURES, SYSTEMS AND COMPONENTS

This section provides a summary description of safety SSCs. However, this chapter does not include information at the level of functional requirements and performance criteria; that information is provided for safety SSCs only and the information is provided in Chapter 4. Their categorization as safety class SSC or safety significant SSC should simply be noted.

2.7 UTILITY DISTRIBUTION SYSTEMS

This section provides information regarding basic utility distribution systems, including offsite power supplies and onsite components of the system. For the PSDR the information may be focused more on the need for utilities, whereas the PDSA should provide details of systems, to the level necessary, for understanding the utility distribution philosophy and facility operations (e.g., schematic outline of power supplies and other utilities).

2.8 AUXILIARY SYSTEMS AND SUPPORT FACILITIES

This section provides information on the remaining portions of the 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 analyses. For the PSDR, the information may be focused more on the need for auxiliary systems and support systems, whereas the PDSA should provide details necessary to understand the more detailed safety analysis content in the PDSA.

2.9 DESIGN PROVISIONS FOR DECONTAMINATION AND DECOMMISSIONING

This section provides information regarding design provisions for decontamination and decommissioning (see DOE G 420.1-1, Section 3.7).

Chapter 3
Hazard Analyses, Accident Analysis, and Control Selection

PURPOSE. The purpose of this chapter is to describe the process used to systematically identify and assess hazards, select and analyze accidents, identify and classify controls for significant hazards, and specify the seismic and natural phenomena design criteria for these hazards. This chapter also presents the results of this hazard and accident analysis and control selection process.

The hazard and accident analyses expected during the preliminary and final design phase are described in this Standard.

APPLICATION OF THE GRADED APPROACH. 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 graded approach for hazard analysis is a function of selecting techniques for process hazard analysis. The technique selected will be sufficiently sophisticated or detailed to provide an appropriately comprehensive examination of the hazards associated with the facility given the complexity of the operation and degree of design maturity. *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples* contains guidance on some of the techniques that may be appropriate for hazard analysis specific to the application and process hazards.

The level of analytical effort used for accident analysis (e.g., facility-level accident consequence analysis, analysis of DBAs, and mitigated accident analysis) 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. The graded approach cannot be based solely on facility hazard categorization because Hazard Category 3 facilities may also have chemical hazards, and the hazard classification mechanism used in DOE-STD-1027, Change Notice 1, September 1997, does not consider the potential for hazardous chemical releases. The results of the hazard analysis (e.g., chemical screening) will indicate whether a facility contains significant chemical hazard(s) that may necessitate DBA analysis.

Accident analysis is also inherently graded in terms of the degree of physical modeling and engineering analysis needed to quantify accident consequences. The use of bounding assumptions and less detailed physical modeling in DBA analysis during preliminary design is appropriate.

In addition to analysis of accidents that can affect the public or collocated worker, hazards are evaluated to determine if hazard controls (i.e., safety significant SSCs and SACs) are required for significant facility worker hazards, and this would typically be expected to result from hazards analysis in preliminary and final design. This is a qualitative analysis and uses guidelines and examples for significant facility worker hazards described in Appendix C.

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 HAZARD ANALYSIS, ACCIDENTANALYSIS, CONTROL SELECTION, AND CLASSIFICATION METHODOLOGY

This section summarizes the methodology used to perform hazard analysis, accident consequence analysis, analysis of Design Basis Accidents, and control selection, as applied during preliminary and final design.

3.2.1 Hazard Analysis Methods

This section summarizes the methods used to perform the hazards analysis at the stage of design (preliminary or final) that is being documented. See Vol. 1 and Appendix G of this Standard for more guidance.

3.2.2 Accident Consequence Analysis Methods

This section describes the methods used to identify and analyze accidents for comparison to guidelines established to establish their classification (i.e., safety class, safety significant) and required seismic and other natural phenomena design criteria. These accidents are analyzed for radiological source terms and toxicological exposures to the public and collocated workers. Expectations for these analyses are described in appendices A and B. (Note: Safety functions may also be identified and classified based on facility worker hazards as described under control selection and classification below.)

3.2.3 Method for Analysis of Design Basis Accidents

This section describes the methods used to identify and analyze DBAs. DBAs are the minimum set of accidents needed to define safety design requirements for safety SSCs under postulated accident conditions. The DBA analysis also provides accident environmental conditions for which the safety SSCs need to be designed to withstand and perform their safety function. If the methodology is specific to a particular accident, the methodology may be described as part of the accident description in Section 3.4.

3.2.4. Control Selection and Classification Methods

This section describes the method used to select safety SSCs. Focus is on the selection method for safety class and safety significant SSCs. Control hierarchy preferences are described. Methods used to establish a necessary and sufficient set is described. Selected safety SSCs are classified as described in Appendix D based on radiological source terms and criteria described in Appendix A of this Standard, chemical exposures and criteria described in Appendix B of this Standard, and facility worker consequences based on considerations and examples described in Appendix C.

3.3 HAZARD ANALYSIS RESULTS

Provide a high-level summary of the hazard analysis results. This summary can be short, as key results will be described in later sections. The detailed results of the process hazard analysis are described in the Hazard Analysis (HA) report.

3.4 FACILITY HAZARD CATEGORIZATION

This subsection presents the results of the hazard categorization activity specified in DOE-STD-1027, Change Notice 1, September 1997. Include the facility hazard categorization and, where segmentation has been used, 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 HA report. In the case of a segmentation or nature of process argument for below Hazard Category 3 designation related to criticality hazards, clearly articulate the justification and design features or controls upon which it rests.

3.5 RESULTS OF ANALYSIS OF ACCIDENTS

This section describes each accident analyzed. For the PSDR, the focus is on analysis of facility and selected system level accidents, including an unmitigated consequence assessment and an analysis of selected Design Basis Accidents to derive design requirements and accident environmental conditions. The PDSA adds description of mitigated accidents to demonstrate the adequacy of controls.

3.5.1 Accident #1 (e.g., Fires and Explosions)

3.5.1.1 Scenario Development

Describe the scenario, including a summary of the MAR (radioactive, chemical, or both), energy source, and release pathway. State the qualitative frequency assigned during hazard analysis (i.e., anticipated, unlikely, extremely unlikely). Identify the top-level safety functional requirements that involve responses to fires and explosions.

3.5.1.2 Analysis of Radiological Source Term and/or Chemical Exposure

Describe the MAR, DR, and ARF and bases used to determine the radiological source term. Describe the chemical release rate and concentration, and the bases that were used to determine the toxicological exposures. Describe and justify any adjustments made to respirable fractions, receptor breathing rates, or atmospheric dispersion factors and why such adjustments are warranted. Compare the radiological source terms and/or chemical exposures to classification guidelines. State the results of the hazard evaluation for facility workers (i.e., does the hazard/accident present a significant facility worker hazard, yes or no).

3.5.1.3 Design Requirements

Identify the design requirements that are derived from the DBA. These could include the worst-case fire temperature, duration, locations (interior, exterior), type of fuels (to derive soot loading), and other constraints (such as a not to exceed temperature to prevent auto ignition for materials protected by a fire barrier). For explosion events, identify TNT equivalents, overpressures (detonation and deflagration), for the various explosion events. Also, identify required protective response associated with secondary events, such as fires or structural failures, pressure relief requirements, and other design aspects needed to meet the functional safety requirements.

3.5.1.4 Control Selection and Classification

Describe the SSCs and SACs selected to prevent or mitigate the accident including the safety function. For SSCs, provide the safety classification, seismic design criteria, and other natural phenomena design criteria. For the PDSA, describe how the selected control suite adequately prevents/mitigates the accident, including how the control suite provides defense in depth, if warranted, based on accident frequency and control reliability.

3.5.2 DBA #2

Same format and content as DBA #1

3.5.3 DBA #3

Same format and content as DBA #1

3.6 SUMMARY OF SIGNIFICANT FACILITY WORKER HAZARDS AND CONTROLS

Describe the significant facility worker hazards identified (if not addressed in the accidents described above) and the SSCs and specific administrative controls (SAC) selected to address them. A table identifying the SSC or SAC and its safety function, and for the SSCs the classification, seismic design criteria, and other natural phenomena design criteria is adequate. (Note: For the PSDR, this section may be limited based on the maturity of the design and hazard analysis. The PDSA section would be complete for significant facility worker hazards identified during the design effort. The DSA may address additional significant facility hazards identified during hazard analysis based on a more complete understanding of operations as operating procedures are developed.)

3.7 SUMMARY OF SAFETY FUNCTIONS AND SSCs and SACs

This section provides a summary (e.g., table) listing the safety functions and the SSCs and SACs selected to provide them. For SSCs, provide the safety classification, seismic design criteria, and other natural phenomena design criteria. In addition, SSCs needed to support the identified Safety SSCs, or whose failure can prevent operation of the Safety SSCs, are identified, along with their safety classification, seismic design criteria, and other natural phenomena design criteria. (Note: The identification of support SSCs and SSCs whose failure can prevent operation of the Safety SSCs maybe limited during preliminary design and thus in the PSDR but should be addressed to the extent the design maturity allows.)

3.8 ACCIDENTS BEYOND THE DESIGN BASIS

The Nuclear Safety Management 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 evaluation of accidents beyond the design basis serves as bases for cost-benefit considerations in determining if the facility design basis should be revised to consider more severe (although less likely) accidents and accident conditions. This evaluation of accidents beyond the design basis establishes the facility design basis by providing the division between events and conditions the facility will be designed for and those for which it will not be designed. Thus, the selection of facility design basis is established with the concurrence of DOE.

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

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

Chapter 4
Safety Structures, Systems and Components for Preliminary Design

PURPOSE. This chapter provides details on those facility structures, systems, and components that are necessary for the facility to protect the public, or significantly contribute to worker safety. Similarly, this chapter provides details on Specific Administrative Controls (SAC) that are also necessary for the facility to protect the public or significantly contribute to worker safety. Descriptions are provided of the attributes (i.e., design and functional requirements and performance criteria) required to accomplish the safety functions identified in the hazard and accident analyses and to demonstrate adequacy of the final design of these SSCs. Maximum advantage should be taken of pertinent design and safety design analysis information developed during the project design effort (e.g., structural analysis, safety design analysis). 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. The extent and detail for this chapter is generally graded based on the facility hazard category. Hazard Category 3 facilities will generally not have Safety Class SSCs, and the number of safety significant SSCs and SACs, if any, typically would be less than those of a Hazard Category 2 facility due to the reduced magnitude of radiological hazards. However, exceptions to this general guidance pertain to chemical hazards and facility worker hazards. The hazard classification mechanism used in DOE-STD-1027-92, Change Notice 1, September 1997 does not consider potential hazardous chemical releases. It is possible that a Hazard Category 3 facility could need safety significant SSCs for chemical hazards and significant facility worker hazards (i.e., those that could result in prompt worker fatality, or severe injury or significant radiological or chemical exposure to workers).

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 SAFETY CLASS STRUCTURES, SYSTEMS, AND COMPONENTS

Relevant information is provided, in the following SSC specific subsections, for safety class SSCs. 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.

4.2.X Applicable Safety Class Structure, System and Components

Identify the Safety Class SSC.

4.2.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 analysis. Do not discuss non-safety functions.

Safety functions are top-level statements that express the objective of the SSC in a given accident scenario. For example, the safety function of a hydrogen detector in a dissolver vessel offgas line could be stated as, "To monitor hydrogen concentration in the dissolver offgas and provide a signal to shut down the dissolving operation before explosive concentrations of hydrogen are reached." The specific accidents associated with the safety function should be identified.

4.2.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 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.

4.2.X.3 Design and Functional Requirements

This subsection identifies requirements that are specifically needed to fulfill safety functions. Such design and 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 is required to 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 non-ambient 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. (Note: The level of design maturity at the end of preliminary design may limit the description of safety SSCs to the requirements identified for the SSCs.)

4.2.X.4 System Evaluation

Safety class SSCs are designed to reliably perform their safety function under those conditions and events for which their safety function is intended. For the PDSA, this subsection summarizes the safety design analysis and other justification for the adequacy of the SSCs ability to reliably perform its safety function. Performance criteria are identified that characterize the specific operational responses and capabilities necessary to meet functional requirements. Evaluate the capabilities of the SSC to meet design and functional requirements. The evaluation of safety class SSCs addresses the following **(all are specified by DOE G 420.1-1)**:

Conservative Design Margins – Safety SSCs must be designed to withstand design basis loadings with an appropriate margin of safety. The design should incorporate multiple levels of protection against normal, anticipated, and accident conditions. For example, while built-in process controls may maintain pressure within a conservative limit, the design may also require provisions for relief valves, automatic shutdown capability, or other preventive features.

Design Against Single Point Failure – The facility and its systems must be designed to perform Safety Class functions with high reliability. The single-point failure criterion, requirements and design analysis identified in ANSI/IEEE 379 must be applied during the design process as the primary method for achieving this reliability.

Environmental Qualification – Environmental qualification must be used to ensure that Safety Class SSCs can perform all safety functions with no failure mechanism that could lead to common cause failures under postulated service conditions. The requirements from ANSI/IEEE 323 for mild environmental qualification must be used unless the environment in which the SSC is located changes significantly as a result of the DBA(s) for which the SSC must perform a safety function, in which case the requirements for harsh environmental qualification must be used. In general, qualification for mild environments should consist of two elements:

- ensuring that all equipment is selected for application to the specific service conditions based on sound engineering practices and manufacture's recommendations; and
- ensuring that the system documentation includes controls that will preserve the relationship between equipment application and service conditions.

Safe Failure Modes – The design must ensure that more probable modes of failure will increase the likelihood of a safe condition.

Support System – If the safety class SSC relies on support systems to perform its safety function, the support system must be classified as safety class as well. That is, if a support system failure can prevent the safety class SSC from performing its safety function, the support SSC must be classified as safety class.

Interface Design – A nuclear safety design goal is to minimize the interfaces between safety SSCs and non-safety SSCs.

Ideally, safety SSCs would not have any interfaces; however, this is not always practical. Interfaces, such as pressure retention boundaries, integrity of fluid systems, electrical equipment, I&C, and mechanical and support systems exist between safety class and non-safety SSCs. These interfaces must be evaluated to identify failures that would prevent the safety class SSC from performing its safety function. For these failures, isolation devices, interface barriers or design class upgrades (i.e., upgrade the interfacing SSC to safety class) should be provided to protect and ensure the safety class SSC reliability. In many cases, systems may consist of a group of subsystems, where each subsystem supports the operation of the whole system. For example, an auxiliary power diesel generator system may consist of lubricating oil, fuel oil, diesel engine, jacket cooling, and room ventilation subsystems. System interface evaluations should clearly define these boundaries. In all instances, a case-by-case evaluation should be performed.

Specific Criteria – A portion of the application of design criteria to safety SSCs entails the selection of appropriate and relevant design codes and standards. The intent is to apply the design codes and standards that will ensure that the safety SSC will perform it required safety function, including due consideration of the intangible areas of influence. Blanket application of national codes and standards is not necessary. Rather, it may be necessary to tailor selections of codes and standards for each specific application based on the safety function. DOE G 420.1-1, Chapter 5, provides specific criteria for various types of safety class SSCs. Aspects of these criteria that are key to the safety class SSC performing its safety function, when required, should be evaluated and summarized in this section.

4.2.X.5 Controls (TSRs)

This subsection identifies those assumptions requiring TSRs to ensure performance of the safety function. This section is meant to provide the information necessary to ensure that the facility design adequately considers design features that will be needed to implement TSRs required by 10 CFR 830.205 as the facility transitions to operation. Identify, as appropriate, the type of TSR needed to ensure each safety function, in particular:

- Safety Limits (SL);

- Limiting Control Settings (LCS);
- Limiting Conditions for Operation (LCO); and
- Surveillance Requirements (SR).

Identify facility design features included to ensure that the TSRs can be implemented (e.g., instrumentation, equipment accessibility to perform surveillances, sufficient redundancy to allow safety SSC outages for maintenance, if required). Specific TSR values (e.g., setpoints, surveillance limits) are not expected for preliminary design.

For passive design features, identify any required inspections that will be needed during facility operation, and design provisions to support these inspections. (Note: The design maturity during preliminary design may limit the amount of information in the PSRD. However, the PDSA should demonstrate adequacy of the final design to support implementation of expected TSRs.)

4.3 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. The content of the following sections is similar to that described under Safety Class SSCs (Section 4.2) except as described below.

4.3.X Applicable Safety Significant Structure, System and Components

Identify the safety significant SSCs.

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 significant SSCs may 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 4.4.X.1). Describe its boundaries and interface points with other SSCs relevant to the safety function.

4.4.X.3 Design and Functional Requirements

This subsection identifies requirements that are specifically needed to fulfill safety functions. Such requirements are specified for both the safety significant SSCs and any needed support safety significant SSCs. (Note: The level of design maturity at the end of preliminary design may limit the description of safety SSCs to the requirements identified for the SSCs.)

4.4.X.4 System Evaluation

Safety significant SSCs are designed to reliably perform their safety function under those conditions and events for which their safety function is intended. For the PDSA, this subsection summarizes the safety design analysis and other justification for the adequacy of the SSCs ability to reliably perform it safety function. Performance criteria are identified that characterize the specific operational responses and capabilities necessary to meet functional requirements. Evaluate the capabilities of the SSCs to meet design and functional requirements. The evaluation of safety significant SSCs addresses the following **(all are specified by DOE G 420.1-1)**:

Conservative Design Features – Safety SSCs must be designed to withstand design basis loadings with an appropriate margin of safety. The design should incorporate multiple levels of protection against normal, anticipated, and accident conditions. For example, while built-in process controls may maintain pressure within a conservative limit, the design may also require provisions for relief valves, automatic shutdown capability, or other preventive features.

Safe Failure Modes – The design must ensure that more probable modes of failure will increase the likelihood of a safe condition.

Environmental Design – To ensure that Safety Significant SSCs can perform all safety functions with no failure mechanism that could lead to common cause failures under postulated service conditions, the SSCs are designed for the environmental conditions that could exist for the postulated accident scenario.

Support System – If the safety significant SSC relies on support systems to perform its safety function, the support system may need to be classified as safety significant. That is, support SSCs to safety significant SSCs that prevent or mitigate accidents with the potential for significant onsite consequences should also be classified safety significant if a support system failure can prevent the safety significant SSC from performing its safety function. However, support SSCs to safety significant SSCs that prevent or mitigate accidents with the potential for only localized consequences (i.e., significant facility worker hazards) need not be classified as safety significant.

Interface Design – A nuclear safety design goal is to minimize the interfaces between safety significant and non-safety SSCs. Ideally, safety SSCs would not have any interfaces; however, this is not always practical. Interfaces, such as pressure retention boundaries, integrity of fluid systems, electrical equipment, instrumentation and control (I&C), and mechanical and support systems exist between safety class and non-safety SSCs. These interfaces must be evaluated to identify failures that would prevent the safety significant SSC from performing its safety function. For these failures, isolation devices, interface barriers or design class upgrades (i.e., upgrade the interfacing SSC to safety class) should be provided to the safety class SSC reliability. In many cases, systems may consist of a group of subsystems, where each subsystem supports the operation of the whole system. For example, an auxiliary power diesel generator system may consist of lubricating oil, fuel oil, diesel engine, jacket cooling, and room ventilation subsystems. System interface evaluations should clearly define these boundaries. In all instances, a case-by-case evaluation should be performed.

Specific Criteria – A portion of the application of design criteria to safety SSCs entails the selection of appropriate and relevant design codes and standards. The intent is to apply the design codes and standards that will ensure that the safety SSCs will perform its required safety function, including due consideration of the intangible areas of influence. Blanket application of national codes and standards is not necessary. Rather, it may be necessary to tailor selections of codes and standards for each specific application based on the safety function. DOE G 420.1-1, Chapter 5, provides specific criteria for various types of safety significant SSCs. Aspects of these criteria that are key to the safety significant SSC performing its safety function should be evaluated and summarized in this section.

4.4.X.5 Controls (TSRs)

This subsection identifies those assumptions requiring TSRs to ensure performance of the safety function. For preliminary design, this section is meant to support and provide the information necessary to ensure that the facility design adequately considers design features that will be needed to implement TSRs required by 10 CFR 830.205 as the facility transitions to operation. Identify, as appropriate, the type of TSR needed to ensure each safety function, in particular the following:

- Limiting Control Settings (LCS);
- Limiting Conditions for Operation (LCO); and
- Surveillance Requirements (SR).

Identify facility design features required to ensure that the TSRs can be implemented (e.g., instrumentation, equipment accessibility to perform surveillances, sufficient redundancy to allow safety SSC outages for maintenance, if required). Specific TSR values (e.g., set points, surveillance limits) are not expected for preliminary design.

For passive design features, identify any required inspections that will be needed during facility operation, and design provisions to support these inspections. (Note: The design maturity during preliminary design may limit the amount of information in the PSRD. However, the PDSA should demonstrate adequacy of the final design to support implementation of expected TSRs.)

4.5 SPECIFIC ADMINISTRATIVE CONTROLS

It is not expected that Specific Administrative Controls (SAC) will be developed in detail during preliminary or final design. However, the safety function of SACs needs to be understood so that the decision to use an SAC rather than a safety SSC can be understood. In addition, any design requirements needed to implement the SACs are identified (e.g., instrumentation, access control provisions, provisions for lock and tag). It is recognized that as part of a major modification, or new facility design, there may be important assumptions or initial conditions that eventually become specific administrative controls in the TSR. In those cases, it is appropriate for the PSDR/PDSA to capture these types of known controls so they are maintained as part of the approval basis and eventually carried forward into the DSA and TSR.

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 an SAC, followed by specific identification of its preventive or mitigative safety function(s) as determined in the Chapter 3 hazard analysis. Do not discuss non-safety functions.

Safety functions are top-level statements that express the objective of the SAC in a given accident scenario. For example, the safety function of a MAR limit could be stated as, “To limit the total quantity of nuclear material present within the facility to no more than 2000 Curies.” The specific accident(s) or general rationale associated with the safety function should be identified.

4.5.X.2 SAC Description

This 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 an 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 an SAC within the timeframes assumed in the safety basis. If SACs require operator action and perform a function similar to a safety SSC, assurance should be provided that the operators can adequately perform their required tasks by analyzing the following human performance factors to be considered during preliminary design such as the following:

- environmental conditions created by the accident, and in which operators may need to perform a safety task;
- level of difficulty of the task;
- design of the equipment and feedback (e.g. indicators and alarms); and
- 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, flowrate 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 design where possible.

Chapter 5
Preliminary Derivation of Technical Safety Requirements

PURPOSE. This chapter builds upon the control functions determined to be essential in Chapter 3, “Hazard Analyses, Accident Analysis and Control Selection,” and Chapter 4, “Safety Structures, Systems and Components for Preliminary Design,” to derive TSRs. This chapter is not necessary for preliminary design in the PSDR. Necessary description of TSR considerations is provided in PSDR chapters 3 and 4. For final design, this PDSA chapter is meant to support and provide the information necessary to ensure that the facility design adequately considers design features that will be needed to fully develop TSR controls required by 10 CFR 830.205 as the facility transitions to operation. The effort required to address this chapter in a PDSA is considerably less than that expected for derivation of TSRs from a DSA.

APPLICATION OF THE GRADED APPROACH. 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 protect the public. TSRs assigned for worker safety and safety significant SSCs will not use SLs.

For administrative controls designated as Specific Administrative Controls (SAC), the DSA preparer should refer to DOE-STD-1186-2004, “Specific Administrative Controls,” for implementing SACs into TSRs.

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 TSR COVERAGE

This section provides assurances that TSR coverage for the facility is complete in relation to the hazard analysis completed for final design. The section lists the features identified in chapters 3 and 4 that are needed to:

- Provide for significant public safety. These features are Safety Class SSCs or SACs, and assumptions requiring TSR coverage identified in previous chapters.

- Provide for significant worker safety. These features are safety significant SSCs or SACs, and assumptions requiring TSR coverage identified in previous chapters.

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 upon 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.

5.3 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 are needed to understand the adequacy of design. As such, this section may be minimal for final design but developed in detail in the DSA as the facility transitions to operation. The definition of modes required in this subsection expands and formalizes the information provided in Chapter 3, "Hazard Analyses and Control Selection," regarding operational conditions associated with accidents.

5.4 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 PDSA preparer. The following format is repeated sequentially for each TSR ("X").

5.4.X [Applicable Hazard/Feature/TSR "X"]

This subsection identifies the specific feature(s) listed in Section 5.2 and the relevant modes of operation.

5.4.X.1 Safety Limits, Limiting Control Settings, and Limiting Conditions for Operation

This section provides the basis and identifies information sufficient to identify what SLs, LCSs, and LCOs will be needed to support the facility TSR documentation required by 10 CFR 830.205 as the facility transitions to operation. For final design, this chapter is meant to support and provide the information necessary to ensure that the facility design adequately considers design features that will be needed to fully develop TSR controls. Specific limits and setpoints are not expected at this stage of design. .

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 set points. 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 safety class criteria. Mitigation of releases is generally not amenable to useful definition of SLs. For example, a ventilation system directing airflow through HEPA filters to protect the public from radiological dose 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 an 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 safety class SSC criteria without ventilation mitigation. If that tank could experience a hydrogen explosion and rupture, then the tank hydrogen concentration may warrant coverage by an SL.

5.4.X.2 Surveillance Requirements

This section identifies Surveillance Requirements that address testing, calibration, or inspection requirements to maintain operation of the facility within SLs, LCSs, and LCOs. Specific requirements are not expected for final design, but facility design features required to implement Surveillance Requirements should be identified (e.g., instrumentation, equipment access).

5.4.X.3 Administrative Controls

Deferred until operational safety basis development.

5.5 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.

Chapter 6
Design for the Prevention of Inadvertent Criticality

PURPOSE. The purpose of this chapter is to provide information regarding aspects of the design that are required to support the prevention of inadvertent criticality.

SCOPE. By definition facilities with the potential for sufficient fissionable material to present a criticality hazard must be categorized either a Hazard Category 1 or 2 nuclear facilities; they may not be categorized as a Hazard Category 3 nuclear facility or below. This chapter, therefore, is not applicable to Hazard Category 3 nuclear facilities even if they are within the scope of this Standard. This chapter applies only to Hazard Category 2 facilities with inventories of fissionable materials sufficient to present an inadvertent criticality hazard. Inventory limits are specified in the TSRs for Hazard Category 1, 2, and 3 nuclear facilities to control the amount of fissionable materials appropriate for those hazard levels.

APPLICATION OF THE GRADED APPROACH.

6.1 INTRODUCTION

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

6.2 CRITICALITY CONCERNS

This section identifies the fissionable material available within the facility and provides information on the location of potential criticality hazards (e.g., description, and drawing), the fissionable material form (e.g., chemical and/or physical, including isotopic content, concentration, densities), and the maximum quantities involved.

6.3 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.

6.3.1 Engineering Controls

This section lists the engineered design features, including those designated as safety significant and important to safety or defense-in depth, used to ensure subcritical conditions under all normal, credible abnormal, and accident conditions. Design features to ensure the preliminary design includes provisions to implement criticality limits should be described. For all features described in detail in other sections of the PSDR/PDSA, provide a brief description of the feature and a reference to the specific section where details are contained (for example, a reference to Chapter 4). For other engineered features that may not affect the facility design, a summary or general safety design approach is sufficient, such as the elimination of moderators, shipping container design, and level detectors. The adequacy of the final design to prevent inadvertent criticality needs to be demonstrated in the PDSA.

6.3.2 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 provisions for handling, storing, and transporting fissionable materials. Specific limits are not expected for preliminary design or final designs in the PSDR or PDSA. However, the nature of the controls should be described to ensure that the design includes provisions to implement such controls.

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 analysis or CSE). The contingency analysis or CSE will identify how the double contingency principle, as defined in ANSI/ANS 8.1, *Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors,* as required by DOE O 420.1B , is being met (i.e., control of two independent process parameters). It is not the intention of this section to individually present all facility contingency analyses or CSEs.

The results of the contingency analyses or CSEs help 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 Analyses and Control Selection”; Chapter 4, “Safety Structures, Systems and Components” ; and Chapter 5, “Preliminary Derivation of Technical Safety Requirements” in concert with the guidance provided in DOE-STD-3007-2007.

Appendix A
Safety Management Program Roadmap

A chapter-by-chapter description of safety management programs that will support safe operation is not necessary for preliminary or final design. The design will include features to implement safety not derived from the nuclear safety analysis and not designated as Safety SSCs or provided with specific TSR coverage. Information regarding these design features is included in project design information. This appendix provides a roadmap to such considerations in the project design information.

Table I-1. Sample SMP Roadmap

Safety Management Program	Project Document	Comments
Occupational Radiation Protection Program	ALARA analysis and shielding design, and similar documents	
Worker Safety and Health Program		
Criticality Safety Program	DOE Approved CSP required by DOE O 420.1B	
Radioactive Waste Management Program		
Fire Protection Program	Preliminary FHA (example)	
Environmental Protection Program	Permitting (example)	
In-service Testing, Inspection and Maintenance		
Engineering Program		
Quality Assurance and Performance Assessment		
Emergency Management		
Management, Organization and		

Institutional Safety Provisions		

Comments section addresses key design considerations included in preliminary design.

Appendix B
Design Approach to Address DOE O 420.1B Design Requirements

The PDSR must update the structure and system-level crosswalk developed in the CSDR to demonstrate application and implementation of the nuclear safety design criteria of DOE O 420.1B and its implementing guidance documents or DOE-approved alternate criteria. During the preliminary design stage, selection of applicable safety criteria should be completed and documented to guide detailed design. For the selected safety SSCs, provide a listing of the applicable safety design criteria from DOE O 420.1B, *Facility Safety*, and its associated guides (see specific listing in Chapter 5). This listing must tie the structure or system level specific criteria (e.g., DOE-STD-1020-2002, ANS 2.26 for natural phenomena criteria in DOE O 420.1B) to the DOE O 420.1B criteria that it satisfies. Programmatic criteria (e.g., system engineer program, configuration management) are not expected to be discussed. Exceptions are identified and justified.

An example of a system level crosswalk is shown below (note that the NPH criteria are out of date for seismic design, see Appendix A of this Standard).

Major Requirements for Facility Fire Walls

Document	Section	Requirement	Evaluation/Comments (Reference)
Fire Barrier Criteria			
DOE O 420.1B	II.3.a.3	Fire protection for DOE facilities, sites, activities, design, and construction must meet …	As documented in facility drawings, facility fire walls were designed in accordance with … (document reference)
	II.3.c.3	Complete fire-rated construction and barriers, commensurate with …	Facility fire walls are placed in accordance with fire analyses to … (document reference)
	Others	*As appropriate for the analyzed safety functions*	
DOE-STD-1066-99	9.2.1	Wall, floor and ceiling, and roof and ceiling assemblies should be tested and rated for their fire resistance …	As documented in component specifications, facility fire walls have been certified to meet their fire resistance rating by … (document reference)
	9.2.2	Fire Resistance - The development of an FHA and SAR should include consideration of conditions …	The hazard and accident analysis performed in the FHA and DSA took into consideration … (document reference)
	Others	*As appropriate for the analyzed safety functions*	
NFPA 221	All	Compliant	Consistent with the design criteria documents, facility fire walls have been designed in accordance with NFPA 221 (document reference)
Others codes and standards		*As appropriate for the analyzed safety functions*	
Natural Phenomena Hazard Performance Criteria			
DOE O 420.1B	IV.3.a.1	Facility SSCs must be designed, constructed, and operated to withstand NPH …	As documented in facility drawings, facility fire walls were designed in accordance with … (document reference)
DOE-STD-1020-2002	2.2	Select Performance Categories of structure, system, or component based on DOE G 420.1-2 and DOE-STD-1021.	Consistent with the methodology of DOE G 420.1-2 and DOE-STD-1021, facility fire walls have been designated as performance category … (document reference)

	2.2	Follow IBC 2000 in its Entirety. Use seismic use group …	Consistent with the design criteria documents, facility fire walls have been designed in accordance with IBC 2000 with the following considerations … (document reference)
	Others	*As appropriate for the analyzed safety functions*	
DOE G 420.1-2	7.1	Establish performance categories for SSCs using DOE-STD-1021.	Consistent with the methodology of DOE-STD-1021, facility fire walls have been designated as performance category … (document reference)
	Others	*As appropriate for the analyzed safety functions*	
DOE-STD-1021-93	2.3	An SSC, failure of which may impair or adversely affect …	Failure of the facility fire walls has been determined in the safety analysis to … (document reference)
	Others	*As appropriate for the analyzed safety functions*	
IBC 2000	All	Compliant	Consistent with the design criteria documents, facility fire walls have been designed in accordance with IBC 2000 (document reference)
Others codes and standards		*As appropriate for the analyzed safety functions*	
Structural			
DOE G 420.1-1	5.2.1	Design safety-significant concrete structures in accordance with ACI-318 (Building Code Requirements for Reinforced Concrete)	Consistent with the design criteria documents, concrete facility fire walls have been designed and will be installed in accordance with ACI-318. (document reference)
ACI-318	All	Compliant	Procurement specifications will require concrete be installed per ACI-318 (document reference)
Others codes and standards		*As appropriate for the analyzed safety functions*	
Others as appropriate for the analyzed safety functions			

APPENDIX J
MAJOR MODIFICATION DETERMINATION EXAMPLES

The following Major Modification Evaluation examples are provided for illustration. Capturing the evaluation in a tabular format provides a concise means of documenting the evaluation results and their bases.

Example 1

Major Modification Evaluation		
Project Information *Waste tank material will be processed in a new Steam Reforming facility in a preexisting building (segmented from other processes in the building) prior to transfer to the permanent disposal facility. The project involves limited design activities and significant physical modifications to support the Steam Reforming process with an estimated cost of greater than $25M.*		
Criterion No.	**Evaluation Criteria**	**Evaluation**
1	Add a new building or facility with a material inventory ≥ HC 3 inventory limits or increase the HC of an existing facility?	*The project does not involve the addition of a new building or facility. The project will be housed within a preexisting building, segmented from other processes in the structure. The project involves the processing of the existing waste inventory within a Steam Reforming facility and will not affect the hazard classification of the facility. Steam reforming is a moderate temperature process used to destroy volatile organic chemicals contained in an aqueous solution without vaporizing radionuclides. The process produces durable, solid mineral glass-like material suitable for permanent storage*
2	Change the footprint of an existing HC 1, 2, or 3 facility with the potential to adversely affect any credited safety function?	*The steam reforming process will be housed in a section of an existing building which has not previously been utilized. New equipment will be installed and includes a steam generator and superheater, mix tanks, evaporators, scrubbers, demisters and ventilation equipment.*
3	Change an existing process or add a new process resulting in a Safety Basis change requiring DOE approval?	*The project will introduce a process which is utilized in multiple other locations for processing similar material. However, the steam reforming process is new to the facility and the current facility safety basis does not address steam reforming.*
4	Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*Steam reforming is not new technology and no GFE equipment is utilized in this process. Steam reforming has been licensed by the EPA as a non-incineration method for the destruction of organics and is in use at Erwin, TN and other DOE and commercial locations Steam reforming is utilized in multiple other locations for processing similar material and the technology is not new to DOE facilities, but is new to this particular facility.. Therefore, the specification of applicable nuclear safety design criteria can be performed with a high degree of certainty. However, the safety basis for this facility does not address steam reforming.*

Major Modification Evaluation		
5	Create the need for new or revised Safety Basis controls (hardware or administrative)?	*Safety basis controls for the facility will require modification. However, steam reforming is utilized in multiple other locations for processing similar material and the required controls are known and have been proven. Therefore, the specification of applicable nuclear safety design criteria can be performed with a high degree of certainty.*
6	Involve a hazard not previously evaluated in the DSA?	*Although steam reforming is utilized in multiple other locations for processing similar material and the hazards of the process are known and understood, the project will introduce hazards which are new to this facility and which are not addressed by the existing facility safety basis.*
Summary and Recommendation: *Three of the six criteria (Criterion 3, 5 and 6) were tripped in this PDSA evaluation. As discussed above, there is no substantial risk involved in changing the footprint of the existing HC 2 facility as a result of this project. The process does not involve new technology and has been proven at other locations. However, the project does introduce a new process and new hazards to the facility and will therefore result in significant impact to the facility safety basis. Per 10CFR830, this qualifies the project as a Major Modification and therefore requires the development of a PDSA.*		

Example 2

Major Modification Evaluation		
Project Information *A proposed project will install new mixing devices and supporting infrastructure in a HC 2 Safety Class radioactive waste storage tank at a TEC of $10,000,000. A similar technology has been used previously to mix radioactive waste in small process tanks located within cell structures at this and other DOE sites. Although the mixing capability of this specific technology has been successfully demonstrated using simulant in a full-scale mock-up, it has never been deployed within the DOE complex for mixing the contents of a large radioactive waste tank. Therefore, the current HA and DSA do not address all of the hazards inherent in the use of this technology for this application. The waste to be mixed is bounded in terms of isotopic inventory by the waste analyzed in the facility HA and DSA; however, a preliminary review of the potential application has identified some potential waste-release mechanisms not currently analyze, as well as the potential to release a total quantity of waste in excess of that current analyzed.*		
Criterion No.	**Evaluation Criteria**	**Evaluation**
1	Add a new building or facility with a material inventory $\geq$ HC 3 inventory limits or increase the HC of an existing facility?	*The project does not does not involve the addition of a new building or facility, nor will it increase the HC of the existing waste tank.*
2	Change the footprint of an existing HC 1, 2, or 3 facility with the potential to adversely affect any credited safety function?	*The project changes the footprint of a HC 2 facility (waste tank) to accommodate the required supporting infrastructure equipment. The existing waste tank structural analysis will be revised as part of the project scope to account for the increased loads due to the mixing device and support equipment. The weight associated with this proposed mixing system exceeds the weight typically associated with typical mixing systems previously used. The ability of the Safety Class tank structure to accommodate this weight or the ability to design a means to support this weight independent of the tank structure is indeterminate at this point in the project.*
3	Change an existing process or add a new process resulting in a Safety Basis change requiring DOE approval?	*Although the new mixing system could potentially be viewed as new process, for the purposes of this evaluation it will not. The consideration of technology application and Safety Basis impact potential will be addressed by criteria 4 and 5. No further assessment of this criterion is therefore required for this evaluation.*

Major Modification Evaluation		
Criterion No.	**Evaluation Criteria**	**Evaluation**
4	Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*The project will utilize a mixing technology that has never previously been formally reviewed / approved by DOE for mixing radioactive waste inside of a large radioactive waste tank. Full scale mock-up testing performed to date using simulant has yielded promising results. Additionally, this technology has been successfully used at this site in the past for mixing of radioactive waste in relatively small (< 10,000 gallons) process vessels with minimal operational problems. Based upon the large scale mock-up testing and on the successful application of similar technology on smaller tanks, there is a reasonably high degree of confidence in the ability of the technology to be successfully applied via this project. Uncertainty with the ability to properly specify applicable nuclear safety design criteria will be addressed in Criterion 6.*
5	Create the need for new or revised Safety Basis controls (hardware or administrative)?	*The project will require new or revised Safety Basis controls (hardware or administrative) given the potential failure modes and release mechanisms. At this point in the project, substantial design details have not been completed. Additional design details are expected to identify additional hazards requiring new/revised controls. Given the number of new potential failure modes and release mechanisms, it is reasonable to assume that the number of controls required will be quite significant in scope. Due to the complexity of the project, any significant new/revised controls may involve significant redesign with accompanying cost and schedule impacts. Therefore, there is a relatively high degree of design and regulatory uncertainty.*
6	Involve a hazard not previously evaluated in the DSA?	*As discussed above, the project will involve hazards not previously evaluated in the DSA and is likely to require additional unidentified controls. In addition, the change creates a new condition where the total potential quantity of waste released may be in excess of that currently analyzed. Given this situation, it is expected that the use of the proposed mixing devices will have a substantial impact on the current DOE-approved Safety Basis and precludes the ability to specify applicable nuclear safety design criteria with a reasonable degree of certainty*
Summary and Recommendation: *Three of the six criteria (criteria 2, 5 and 6) were tripped in this PDSA evaluation. The assessment of each of these three criteria identified a high degree of risk inherent in the application of the new mixing technology as proposed by this project. Additionally it is noted that although Criterion 4 was not tripped, the application of this mixing technology to a large radioactive waste tank represents an untried approach despite previous success with similar technology on much small scale tanks and full scale simulant testing. Based on these considerations, it is concluded that this project constitutes a Major Modification and will therefore, require the development, review, and approval of a PDSA. Therefore, it is recommended that the project proceed accordingly.*		

Example 3

Major Modification Evaluation		
Project Information *A proposed project will add a new loading dock to a HC-2 facility. The new loading will not interface with the Safety Class and safety significant infrastructure of the existing facility. Estimated TEC is $8,000,000. The types of project and infrastructure equipment are identical to that already used and considered in the facility hazard analysis and DSA with appropriate safety-related controls specified. The material to be processed is bounded by the MAR currently analyzed in the facility hazard analysis and DSA.*		
Criterion No.	**Evaluation Criteria**	**Evaluation**
1	Add a new building or facility with a material inventory ≥ HC 3 inventory limits or increase the HC of an existing facility?	*The project involves the addition of a new loading dock to an existing HC-2 facility. It will not increase the material inventory of the existing facility and will not change the HC.*
2	Change the footprint of an existing HC 1, 2, or 3 facility with the potential to adversely affect any credited safety function?	*The addition of a new loading dock changes the footprint of a HC-2 facility, but it does not have any potential for adverse impacts on credited safety functions. The structural qualification, evacuation egress path, fire suppression system performance and other safety analysis assumption are preserved.*
3	Change an existing process or add a new process resulting in a Safety Basis change requiring DOE approval?	*The addition of a new loading dock does not change the existing processes and does not result in a Safety Basis change requiring DOE approval. The current DOE-approved Safety Basis already addresses the use of loading docks.*
4	Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*The addition of a new loading dock will not utilize new technology or GFE not previously formally reviewed and approved by DOE for use in this facility.*
5	Create the need for new or revised Safety Basis controls (hardware or administrative)?	*The addition of a new loading dock does not create the need for new or revised Safety Basis controls due to new processes. The current DOE-approved Safety Basis already addresses the use of loading docks.*
6	Involve a hazard not previously evaluated in the DSA?	*The addition of a new loading dock does not involve a hazard not previously evaluated in the DSA. The current DOE-approved Safety Basis already addresses the use of loading docks.*
Summary and Recommendation: *No criteria were tripped in this PDSA evaluation. Based on this finding, it is concluded that this project does not involve a Major Modification and, therefore, no PDSA is required. The changes to the existing DSA/TSR to reflect this project will be made following the normal DSA/TSR change process. Therefore, it is recommended that the project proceed accordingly.*		

Example 4

Major Modification Evaluation		
Project Information *A proposed project will add a new operation to an existing HC-2 facility to package TRU waste for offsite shipment. The estimated TEC is $8,000,000. Although new to this facility, the project involves a process that will use a well-proven technology with a history of positive operating experience at other facilities throughout the DOE Complex (reference engineering study). The new processing equipment will interface with the existing safety significant ventilation, fire suppression, and electrical systems. The project design criteria will ensure that no interactions with the current SS SSCs are introduced by the project that could adversely alter the response or performance of these SS SSCs. Additional modification work required for these SS systems is limited to standard interface support issues that do not present a significant project risk such as running conduit, plugging into utilities, mating connections, and bolting supports to structural members. The types of process equipment differ from those used and evaluated in the current facility hazard analysis and DSA with the potential to present new hazards. However, based on the preliminary hazard analysis (reference), these hazards are well characterized and the associated hazard controls needed are encompassed by the safety SSC and safety management programs already implemented in the facility. The material to be processed is an existing TRU waste stream already analyzed in the facility hazard analysis and DSA.*		
Criterion No.	**Evaluation Criteria**	**Evaluation**
1	Add a new building or facility with a material inventory ≥ HC 3 inventory limits or increase the HC of an existing facility?	*The material to be processed by the new packaging operations is bounded by the MAR currently analyzed in the facility hazard analysis and DSA and the existing facility hazard categorization (HC) documentation. It will not increase the material inventory of the existing facility and will therefore, not change the HC.*
2	Change the footprint of an existing HC 1, 2, or 3 facility with the potential to adversely affect any credited safety function?	*The new packaging process will be housed within an existing facility structure with minor structural modifications. The project design criteria will ensure that no adverse interactions with current SS SSCs are introduced by the project. The facility structural qualification, evacuation egress path, and functional capabilities of the existing safety significant ventilation, fire suppression system, and electrical system performance, and other safety analysis assumptions will be preserved.*
3	Change an existing process or add a new process resulting in a Safety Basis change requiring DOE approval?	*The project involves the addition of a new TRU waste packaging process to the existing facility and was determined to require a safety basis change requiring DOE approval.*
4	Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*Although the technology to be used in the new TRU waste packaging process is widely used throughout the complex, DOE has not previously reviewed/approved the use of this technology for this facility.*

Major Modification Evaluation		
5	Create the need for new or revised Safety Basis controls (hardware or administrative)?	*The addition of a new waste processing operation will create the need for extending the capability of the existing safety significant ventilation, fire suppression, and electrical systems. However the design does not introduce interaction effects that alter the response or performance of these SSCs, so additional modification work required for these systems is limited to standard interface support issues that do not present a significant project risk such as running conduit, plugging into utilities, mating connections, and bolting supports to structural members. The hazards associated with the new process are well characterized and the associated hazard controls needed are encompassed by the safety SSC and safety management programs already implemented in the facility, so there is an acceptably low project risk that further modification or addition of safety SSC will be necessary.*
6	Involve a hazard not previously evaluated in the DSA?	*The addition of a new TRU waste processing operation will involve hazards not previously evaluated in the DSA for this facility. Similar operations have been extensively evaluated at other DOE sites such that the new hazards are well understood and characterized.*
Summary and Recommendation: *Four of the six criteria (3, 4, 5, and 6) were tripped in this PDSA evaluation. The associated USQ determination was positive, indicating that DOE approval is required in revising the existing Safety basis to add the new waste processing operation. Although new to this facility, the TRU waste processing operations and the attendant hazards are well understood and characterized. The hazard controls required for this operation at these facilities are encompassed by the safety SSC and safety management programs already implemented in the facility. Furthermore, the normal design review and control process will be followed to confirm the engineering evaluation conclusion that no adverse impacts to existing facility safety significant SSCs are introduced by the new design. This results in an acceptably low project risk. Since the project involves a process that will use a well-proven technology with a history of positive operating experience, it is concluded that there is no significant Safety Basis risk associated with this project and thus, no need for a PDSA. The changes to the existing DSA/TSR to reflect this project will be made following the normal DSA/TSR change process. Therefore, it is recommended that the project proceed accordingly.*		

CONCLUDING MATERIAL

Review Activities:

DOE	**Ops Offices**	**Preparing Activity:**
NA	AL	
HS	SR	DOE HS-21
EM	ID	
SC	NV	**Project Number:**
NE	OR	
GC	RL	SAFT-0108
Energy CTA		
NNSA CTA		

Area/Site Offices	**National Laboratories**
Pantex	SRL
Carlsbad	LANL
Princeton	LLNL
ORP	PNNL
Los Alamos	INL
Y-12	PPPL