ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

INTEGRATING SAFETY INTO THE DESIGN PROCESS

Main Category:	Project Management
Sub Category:	-
Course #:	PRJ-120
Course Content:	98 pgs
PDH/CE Hours:	7

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM
TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)
SUPPORT@ENGINEERING-PDH.COM

PRJ-120 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. According to the reference material, 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.
    a. True
    b. False
2. Which DOE regulation requires a technology readiness assessment to be conducted for the preferred alternative and development of a Technology Maturation Plan, as appropriate?
    a. DOE G 413.3-4A
    b. DOE O 413.3B
    c. DOE-STD-1066-2016
    d. DOE O 420.1C, Chg. 1
3. According to the reference material, major modification assessments assigned at least one "no" answer shall be provided to the DOE field element manager or designee, together with supporting technical justification.
    a. True
    b. False
4. According to the reference material, the goal of the final design phase is to achieve __ percent design completion, meaning a level capable of supporting procurement, construction, testing, and operation.
    a. 80
    b. 85
    c. 90
    d. 95

5. Using section 6.0 REFERENCES, which of the following DOE Directives was used as guidance for implantation of safeguards and security programs?
    a. DOE O 425.1D
    b. DOE O 413.3B, Chg. 2
    c. DOE O 414.1D
    d. DOE Order 470 Series
6. According to the reference material, communication is an essential ingredient for successful implementation of the safety-in-design process.
    a. True
    b. False
7. The five phases of the acquisition process are delimited by "Critical Decisions," referred to as CDs. Which of the following phases corresponds to the description: development of a conceptual design for alternative selection; the selected alternative and approach is the optimum solution?
    a. CD-0
    b. CD-1
    c. CD-3
    d. CD-5
8. According to the reference material, the preliminary design phase is devoted to a more rigorous evaluation of the conceptual design. The hazards analysis evolves from a system-level analysis to a facility-level analysis as more design detail becomes available.
    a. True
    b. False
9. Using APPENDIX H in the reference material, which of the following categories is NOT included in the Pre-conceptual Design diagram?
    a. Program and Project Management
    b. Project Engineering
    c. DNFSB External Safety Oversight
    d. Safety Design Basis
10. The design process shall evaluate and consider inherently safer design concepts that can lead to the removal or reduction of hazards before controls need to be developed. Which of the following design considerations is characterized by: eliminating problems by design rather than adding additional equipment or features to deal with them?
    a. Subtraction
    b. Simplify
    c. Withdraw
    d. Substitute

CONTENTS

1.0 INTRODUCTION

This Standard (STD) provides requirements and guidance for the integration of safety into the design process for Department of Energy (DOE) Hazard Category (HC) 1, 2, and 3 nuclear facilities as defined in 10 Code of Federal Regulations (CFR) Part 830, *Nuclear Safety Management*.

1.1 SCOPE

This Standard specifies the requirements and responsibilities for project management, engineering/design, and safety analysis, and their interactions essential for successful integration of safety into design and construction. The Standard also specifies the engineering and design process, as well as key interfaces required for the integration of safety into design.

1.2 APPLICABILITY

This Standard applies to the design and construction of (a) new DOE HC 1, 2, and 3 nuclear facilities, (b) major modifications to DOE HC 1, 2, and 3 nuclear facilities, and (c) other modifications to DOE HC 1, 2, and 3 nuclear facilities that are managed under the requirements of DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets.* The activities and processes in this Standard may be applied to new facilities and to modifications to those facilities not listed above, for example, hazardous non-nuclear facilities.

1.3 BACKGROUND

DOE-STD-1189-2008, *Integration of Safety into the Design Process*, was developed to fulfill the objectives of project management as stated by the Deputy Secretary of Energy in a December 5, 2005 memorandum, *Integrating Safety into Design and Construction*, to DOE elements:

> *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.*

This revision reflects lessons learned and experience since the original issuance of DOE-STD-1189-2008. It also reflects the definition of 90% design completion as set out in Secretary Moniz's June 8, 2015 memorandum, *Project Management Policies and Principles*, as reflected in DOE O 413.3B.

1.4 OVERVIEW OF THE STANDARD

Section 2 describes the terminology used in the Standard, including acronyms and abbreviations, requirement and recommendation statements, and definitions.

Section 3 describes the project management processes and responsibilities for ensuring proper implementation of the safety-in-design concept.

Section 4 describes the design process and criteria to ensure that safety is integrated into design.

Section 5 describes the process for determining whether a facility modification is a “major modification” and the application of the graded approach for major modifications.

Section 6 provides key references.

Appendices are provided on the following topics: (A) Overview of the Safety-in-Design process, (B) Safety Design Strategy, (C) Conceptual Safety Design Report, (D) Preliminary Documented Safety Analysis, (E) Safety Programs and Other Important Project Interfaces, (F) Major Modification Determination Examples, (G) Analysis of Potential Design Upgrades, and (H) Interface Between Safety-in-Design and Project Management.

2.0 TERMINOLOGY

2.1 ACRONYMS AND ABBREVIATIONS

ALARA	As Low As Reasonably Achievable
CD	Critical Decision
CDR	Conceptual Design Report
CFR	Code of Federal Regulations
CIPT	Contractor Integrated Project Team
CM	Configuration Management
COR	Code of Record
CSDR	Conceptual Safety Design Report
CSE	Cognizant System Engineer
DBA	Design Basis Accident
DOE	Department of Energy
DSA	Documented Safety Analysis
FHA	Fire Hazards Analysis
FPD	Federal Project Director
G	Guide
GFE	Government Furnished Equipment
HC	Hazard Category
HDBK	Handbook
IPT	(Federal) Integrated Project Team
NEPA	National Environmental Policy Act
NPH	Natural Phenomena Hazards
O	Order
PDSA	Preliminary Documented Safety Analysis
QA	Quality Assurance
QAP	Quality Assurance Program
R&OA	Risk and Opportunity Assessment
RMP	Risk Management Plan
SAC	Specific Administrative Control
SDIT	Safety Design Integration Team
SDS	Safety Design Strategy
SER	Safety Evaluation Report
SME	Subject Matter Expert
SMP	Safety Management Program
SSCs	Structures, Systems, and Components
STD	Standard
TRL	Technology Readiness Level
TSR	Technical Safety Requirement

2.2 SHALL, SHOULD, AND MAY

The word “shall” denotes a requirement; the word “should” denotes a recommendation; and the word “may” denotes permission, neither a requirement nor a recommendation.

2.3 DEFINITIONS

Code of Record (COR): The COR is a set of design and operational requirements, including Federal and state laws, in effect at the time a facility or item of equipment is designed and accepted by DOE. The COR is (i) initiated during the conceptual design phase, placed under configuration control to ensure it is updated to include more detailed design requirements as they are developed during preliminary design, (ii) controlled during final design and construction with a process for reviewing and evaluating new and revised requirements to determine their impact on project safety, cost, and schedule before a decision is taken to revise the COR, and (iii) maintained and controlled through facility decommissioning. The COR may be defined in contracts, Standards, or Requirements Identification Documents (or their equivalent), or project-specific documents.

Configuration Management: A disciplined process that involves both management and technical direction to establish and maintain alignment of project documentation, design requirements, and the physical configuration of the nuclear facility.

Design Organization: The organization with the responsibility and authority for the design of a capital asset being acquired or major modification to an existing asset (typically, the contractor or contractor team holding the design contract). The design organization may obtain help and support from other organizations, but retains overall responsibility and authority for the design. In some cases, DOE may be the design organization.

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

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

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

Major Modifications: Modifications that "substantially change the existing safety basis for the facility." [10 C.F.R. § 830.3]

Safety Structures, Systems, and Components: Both safety class structures, systems, and components and safety significant structures, systems, and components. [10 C.F.R. § 830.3]

Systems Engineering: A proven, disciplined approach that supports management in clearly defining the mission or problem; managing system functions and requirements; identifying and managing risk; establishing bases for informed decision-making; and verifying products and services meet customer needs. [DOE G 413.3-1]

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

3.0 PROJECT MANAGEMENT

This section sets forth the project management processes and responsibilities for ensuring proper implementation of the safety-in-design concept required by DOE directives. This section identifies DOE directives that provide project management requirements, and identifies requirements for the Safety Design Strategy (SDS), a project management document that provides a roadmap for integration of safety into design. This section also provides roles and responsibilities of project organizations, and top-level requirements for configuration management. Appendix A, "Overview of the Safety-in-Design Process," further describes the process established in this section.

3.1 DOE ORDER BASIS

The DOE Orders forming the basis for this Standard are: DOE O 420.1C, Chg.1, *Facility Safety*, and DOE O 413.3B. This Standard provides (a) requirements in addition to those in the cited Orders, and (b) guidance and acceptable methods for meeting Order requirements.

3.2 PROJECT MANAGEMENT PROCESS

DOE's program and project management system, described in DOE O 413.3B, establishes a required management process for the acquisition of capital assets. Integration of safety into design in all phases of a project is a critical element of this process. Line managers are responsible for successfully developing, executing, and managing projects within the approved performance baseline. Appendix B of DOE O 413.3B describes specific project management responsibilities for all levels of DOE line management.

Project management for projects with a total project cost below the DOE O 413.3B threshold are managed consistent with DOE O 430.1B, Chg. 2, *Real Property Asset Management*. For such projects, the requirements in this Standard should be graded based on the scope and complexity of the project.

3.3 SAFETY DESIGN STRATEGY

An SDS shall be developed for all projects within the scope of this Standard. For DOE O 413.3B projects, the Order requires that the contractor organization develop an SDS for DOE approval at the conceptual design stage of the project. The SDS for these projects should be developed on a graded approach that considers the degree of interface with nuclear safety SSCs. The Order states the following in regard to the purpose of the SDS:

> *The SDS provides preliminary information on the scope of anticipated significant hazards and the general strategy for addressing those hazards. The SDS is updated throughout subsequent project phases and should contain enough detail to guide design on overarching design criteria, establish major safety structures, systems, and components, and identify significant project risks associated with the proposed facility relative to safety.*

The SDS reflects and is guided by safety expectations for the project as communicated by the responsible DOE Program Office. The SDS shall address the following aspects of safety integration:

- The guiding philosophies or assumptions to be used to develop the design, including significant inputs and assumptions, potential impacts of new technology, and project constraints as they might affect safety design decisions.
- The safety-in-design and safety goal considerations for the project, including such matters as hazardous materials associated with the facility, preliminary hazard categorization, commitment to DOE O 420.1C, Chg. 1 (design criteria, functional requirements, and design basis); and high-cost design attributes and approaches affecting project risk (such as use of new and non-standard methods).
- The approach to developing the overall safety basis for the project, including the types of analyses to be conducted, documents to be developed through the project cycle, transition from preliminary design to final design (including identification of any hold points on design activities until DOE review of preliminary design results is complete), and any tailoring approaches selected.
- Key safety decisions for major processes and systems including risk and opportunity management approaches.
- Key safety documents to be used during the design development phase, to support design development activities and to document the Preliminary Safety and Design Results.
- The Quality Assurance Program (QAP) and implementation strategy.
- The Configuration Management (CM) program and implementation strategy.
- For Major Modifications, the interface with the existing facility's safety basis and operations.
- The potential need for a Design Upgrade Analysis (see Appendix G).
- Any tailoring or graded approaches used for the requirements of this Standard.
- Facility-level commitments and requirements developed by the various design disciplines such as structural and electrical.

For modifications to DOE HC 1, 2, and 3 nuclear facilities that are not major modifications but are managed under DOE O 413.3B, the SDS should document the type and scope of the hazard/accident analysis, describe the supporting safety documentation and Documented Safety Analysis (DSA) amendment or revision to be prepared, and should explain the process to develop and review and approve these documents. For such modifications, a Conceptual Safety Design Report (CSDR) and a Preliminary Documented Safety Analysis (PDSA) may not be necessary. No SDS is required for modifications that do not require any new or revised hazard controls and do not require a new or revised hazard analysis/accident analysis.

The SDS should be provided to DOE for review and approval prior to submission of other safety documentation required at the conceptual design stage. This is particularly important for large, complex projects.

In developing an SDS, it is a good practice to review lessons learned from previous projects. See Appendix B of this Standard for further guidance on the SDS.

3.4 FEDERAL PROJECT DIRECTOR

3.4.1 Management Role

Appendix B of DOE O 413.3B assigns the central project management role to the Federal Project Director (FPD): "The FPD is accountable to the Project Management Executive, Program Secretarial Officer or delegated authority, as appropriate, for the successful execution of the project."

The FPD is given these management responsibilities:

- Prepare and maintain the (Federal) Integrated Project Team (IPT) charter and operating guidance and ensure that the IPT is properly staffed;
- Define and oversee the roles and responsibilities of each IPT member;
- Lead the IPT and provide broad project guidance;
- Delegate appropriate decision-making authority to the IPT members; and
- Approve the IPT charter for non-major system projects.

The FPD (or assigned project manager for projects not covered by DOE O 413.3B) provides leadership and sets the expectation of effective coordination between the safety and design organizations. Frequent and frank discussions among technical professionals working on the design and safety analysis are essential for implementation of the safety-in-design integration process. Other senior project managers should monitor interactions between the safety and design organizations.

Some projects (such as projects not covered by DOE O 413.3B) may not identify an FPD. In such cases, the responsibilities assigned to the FPD by this Standard should be carried out by the responsible approving authority.

3.4.2 Safety Responsibilities

DOE O 413.3B assigns to the FPD the task of ensuring "that safety is fully integrated into design and construction for Hazard Category 1, 2, and 3 nuclear facilities." The Order also requires that the FPD "ensure that design, construction, environmental, sustainability, safety, security, health and quality efforts performed comply with the contract, public law, regulations, and Executive Orders."

The FPD is also responsible for implementation of a systems engineering approach to the design development process. Systems engineering encompasses engineering, design, construction, testing, operation, and maintenance aspects of design development. Its use will ensure that safety issues and resolutions are well thought out for effective integration into the design details. DOE G 413.3-1, *Managing Design and Construction Using Systems Engineering for Use with DOE O 413.3A*, provides additional information on the systems engineering approach.

The FPD approves or concurs in the following safety-in-design documents:

- SDS,
- Risk & Opportunity Assessment (R&OA),
- Safety review letter on the CSDR, and
- Safety Evaluation Report (SER) on the PDSA.

3.5 FEDERAL INTEGRATED PROJECT TEAM

The IPT, including subject matter experts (SMEs) from both DOE and the contractor design organization, is initially established by the appropriate Program Manager or Head of Field Organization. DOE O 413.3B and DOE G 413.3-18A, *Integrated Project Team: Guide for Formation and Implementation*, elaborate on the roles, responsibilities, and necessary technical expertise of an IPT. Specifically with respect to integration of safety into design, the IPT performs the following tasks:

- Maintain close coordination with the Contractor Integrated Project Team (CIPT) for timely resolution of safety-in-design issues;
- Identify, define, and manage to completion the project's environmental, safety, health, security, risk, and QA requirements;
- Support resolution of review findings and issues related to safety and design (including those identified by the Defense Nuclear Facilities Safety Board (DNFSB));[1] and
- Ensure safety is effectively integrated into design and construction in a timely manner.

For projects not covered by DOE O 413.3B, the FPD or assigned project manager should establish an IPT with a size and composition based on the complexity of the project. The IPT should include a DOE nuclear safety professional, when merited by the scope and complexity of the project. The IPT shall interface and coordinate with the CIPT (see Section 3.6) and with the Safety Design Integration Team (SDIT) (see Section. 3.7), to ensure that integration of safety into project design is accomplished in a timely and effective manner.

The IPT is responsible for reviewing the following safety-in-design documents:

- SDS,
- R&OA,
- CSDR,
- PDSA, and
- SER on the PDSA, DSA, and Technical Safety Requirement (TSRs).

[1] For details regarding the DNFSB interface, see DOE M 140.1-1B, *Interface with the Defense Nuclear Facilities Safety Board*, 2001.

3.6 CONTRACTOR INTEGRATED PROJECT TEAM

The contractor managing the project shall establish a CIPT to accomplish the responsibilities described below. Normally, the contractor's Project Manager serves as the team leader and the contractor's Safety Lead serves as a team member. CIPT members should represent the competencies relevant to the project, including systems engineering. This range of expertise permits the CIPT to provide an important forum for discussion and resolution of design, safety, and project issues. If separate safety and/or design engineering organizations are supporting the contractor, a representative of these organizations should be included on the CIPT. For a large, complex project, the CIPT is functionally parallel to the IPT. The FPD and contractors maintain close coordination using the IPT and CIPT as communication tools.

The CIPT (a) ensures safety is effectively integrated into design and construction in a timely manner, (b) monitors performance of safety and design tasks and completion of safety and design deliverables to ensure that they are integrated and in sync, and (c) takes action, including informing the IPT, if safety and design task integration presents risks to successful completion of the project.

The CIPT also maintains close coordination with the SDIT (see next section), which is intimately involved with the safety analysis, design, construction, and operational planning details. The SDIT is the ultimate source of project information related to safety-in-design activities. The CIPT's assigned responsibilities parallel those of the IPT. The CIPT assists the IPT in resolving design issues.

3.7 SAFETY DESIGN INTEGRATION TEAM

An SDIT shall be established for all projects that fall under this Standard, unless the DOE-approved SDS provides an alternate approach.

The SDIT shall be a part of the organization responsible for the design (typically, the contractor organization). The principal tasks of the SDIT are to (a) support the IPT/CIPT to ensure the integration of safety into the design process, including development of the SDS, (b) identify and analyze the hazards in the facility,[2] (c) ensure that the selected controls are adequate to perform the safety function, (d) ensure that the requirements of project interfaces (e.g., security needs) are addressed, and (e) ensure that selected controls are consistent with control selection hierarchy and represent cost effective solutions to safety challenges. (See DOE O 420.1C and DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis,* for further guidance). The SDIT should be established and commence operations no later the commencement of conceptual design. Because an SDS should be developed in the earliest stages of the project cycle, the SDIT should develop a working draft as its first task.

[2] In the case of a major modification, the SDIT examines hazards within the scope of the modification project.

The SDIT is responsible for preparing the following safety-in-design documents, as directed by the CIPT:

- SDS,
- R&OA,
- CSDR,
- PDSA, and
- DSA and TSRs (assisted by operations personnel).

The SDIT should use R&OAs as a communication and decision-making tool for highlighting safety-in-design assumptions, risks, and decisions (see Appendix C for further details). The SDIT shall communicate and coordinate with the IPT (or applicable federal authority) and the CIPT to ensure that integration of safety into the project design is accomplished in a timely and effective manner.

The SDIT should consist of (a) a core technical team and (b) additional SMEs who may be called upon to accomplish specific tasks. The overall team composition depends on complexity of the design being developed. The core team should consist of safety personnel (contractor safety lead), engineering and design personnel responsible for the process or facility, operations and maintenance personnel, and the management of the design organization.

In rare cases, which meet one of the following criteria, the SDIT duties may be performed by the CIPT, or by another approach, as described in the approved SDS.

- The project is small such that the IPT and the CIPT can coordinate effectively all safety-in-design related issues, leaving no uncertainties in communication protocols;
- Hazards are well-defined and hazards mitigation strategies are well-defined and have been proven effective; or
- Design solutions, including those to meet safety-in-design requirements, are well-defined and have been proven effective.

In these situations, use of a separate, stand-alone SDIT is still strongly recommended to provide adequate focus on and integration of important technical tasks.

3.8 CONFIGURATION MANAGEMENT

3.8.1 Configuration Management Plan

DOE's approach to this subject is set forth in DOE-STD-1073-2016, *Configuration Management*, which is endorsed by DOE O 413.3B and DOE O 430.1B, Chg. 2. This Standard provides a disciplined CM process to establish consistency among safety and design requirements, control the physical configuration of a nuclear facility,[3] and manage

[3] This includes controlling configuration during a major modification.

documentation.

The design organization shall prepare and implement a CM plan as an integrated process for all activities that affect safety-in-design integration as the project moves from inception to operation. The CM plan identifies how different levels of CM are phased in as design requirements are established and construction activities are completed and turned over. The CM plan shall (a) specify the process so that the design basis and design requirements are made consistent with the safety analysis process, (b) specify the process for maintaining configuration management of safety basis documents, and (c) describe the basis for any graded approach, if used. The CM plan should be initiated early in the conceptual design process and approved prior to start of preliminary design activities.

3.8.2 Code of Record

The Code of Record (COR) and its supporting documents should be organized in a manner that supports accessibility, traceability, and maintainability. The COR is initiated during the conceptual design phase and is placed under configuration management to ensure it is updated to include more detailed design requirements, or changes to requirements, as they are identified during preliminary and final design. The COR is controlled during final design and construction with a process for reviewing and evaluating new and revised requirements to determine their impact on project safety, cost and schedule before a decision is taken to revise the COR. A database tool is often useful in organizing COR information and its specific applicability to project structure, system, or components (SSCs).

3.8.3 Change Control for the Preliminary Documented Safety Analysis

After the PDSA is issued, not every change in the design baseline will necessitate a PDSA revision. The following criteria should be applied to design baseline changes when determining whether a PDSA revision is necessary.

- The change alters a safety function for a safety structure, system, and component identified in the current PDSA.
- The change alters either the functional classification or the design standard for a safety SSC previously specified in the PDSA configuration baseline.
- The change requires implementation of new or different safety SSCs or specific administrative controls (SACs), or safety management program (SMP) key elements.
- The change significantly alters the process design or its safety basis.
- The change significantly alters the likelihood or consequences of an SSC malfunction.

4.0 INTEGRATION OF SAFETY INTO THE DESIGN

This section sets forth the design process and criteria to ensure that safety SSCs, SACs, and SMPs are integrated into the design in an effective and efficient way. As the design progresses and hazard analyses are performed, the design organization determines appropriate safety features. Failure to incorporate safety features early in the design can result in prohibitively expensive changes and delays later in the design process. A systematic design development process is executed in project phases, using a graded approach:

- Pre-Conceptual – develop the Mission Need Statement based on gap analysis.
- Conceptual – evaluate alternatives for satisfying the Mission Need Statement to identify the preferred alternative for preliminary design.
- Preliminary – initiate the process of converting concepts to a design appropriate for procurement or construction.
- Final – complete the design effort and produce approved design documentation necessary to permit procurement, construction, testing, checkout and turnover to proceed.

For capital asset projects, a tie to the Critical Decisions (CDs) in DOE O 413.3B shall be established in the Project Execution Plan.[4]

Section 4.1 specifies the safety-in-design approach and requirements that need to be used in the design development phases, as described in Sections 4.2 through 4.6 below.

4.1 SAFETY-IN-DESIGN APPROACH

The following safety-in-design approach is used to ensure that safety concepts are well thought out from the pre-conceptual to final design phases of the project and fully integrated into the design at the appropriate time.

4.1.1 Identification of Design and Safety Requirements

DOE O 420.1C, Chg. 1, provides nuclear design criteria and requirements for facility safety and hazards analyses, defense in depth, and safety-in-design integration. Safety SSCs shall be designed and constructed using applicable industry codes and standards and other DOE directives identified in accordance with Attachment 3 to DOE O 420.1C, Chg. 1. For security and safeguards design requirements, the DOE O 470 series is used. The identified requirements are actively managed and safety is integrated into the design using a systems engineering approach. The identified requirements provide a foundation for the COR.

[4] See DOE G 413.3-15, *Department of Energy Guide for Project Execution Plans*.

4.1.2 Major Safety Functions

During design development, the design organization shall identify the safety SSCs and their safety functions as determined by the hazards and accident analyses. Safety function descriptions state the objective of the SSCs in a given accident scenario to prevent or mitigate the consequences of the scenario. Any supporting systems and requirements related to accomplishing safety functions shall also be identified. The safety design basis should explain how supporting systems, adjacent systems, or connecting systems might affect a safety SSC when its function is demanded. These functions are later developed into performance criteria for each SSC.

4.1.3 Inherently Safer Design

The design process shall evaluate and consider inherently safer design concepts that can lead to the removal or reduction of hazards before controls need to be developed. Specifically, this design philosophy entails consideration of the following:

- Minimize: Reducing the amount of hazardous material present at any one time (for example, by using smaller batches).
- Substitute: Replacing one material with another of less hazard (for example, cleaning with water and detergent rather than a flammable solvent).
- Moderate: Reducing the strength of an effect (for example, having a cold liquid instead of a gas at high pressure) or using material in a dilute rather than concentrated form.
- Simplify: Eliminating problems by design rather than adding additional equipment or features to deal with them. Use complex procedures only when necessary.[5]

Inherently safer design concepts can allow facilities to be designed minimizing the need for complex layers of controls that can add project risk and increase operational complexity.

4.1.4 Hierarchy of Controls

After hazardous material minimization/elimination and application of inherently safer design concepts where practical, a control strategy shall be (a) selected to prevent or mitigate releases of hazardous materials and to provide defense in depth, and (b) based on the following order of preference:[6]

[5] For the origin and meaning of this preference structure, see for example Bollinger, R.E., et al., *Inherently Safer Chemical Processes: A Life Cycle Approach*, D.A. Crowl, Ed., American Institute of Chemical Engineers, New York, NY (1996), and Khan, Faisal and Amyotte, Paul, "How to Make Inherent Safety Practice a Reality," Canadian Journal of Chemical Engineering, 81: 2-16 (Feb. 2003).
[6] See DOE-STD-3009-2014 and DOE G 420.1-1A for additional details on implementation.

- SSCs are preferred over administrative controls.
- Passive SSCs are preferred over active SSCs.
- Preventive controls are preferred over mitigative controls.
- Controls closest to the hazard may provide protection to the largest population of potential receptors, including workers and the public.
- Controls that are effective for multiple hazards can be resource-effective.

4.1.5 Conservatism

When a safety-in-design strategy is uncertain and/or immature at an early stage of design, design margins and assumptions shall be conservative. Use of conservative assumptions, however, should be tempered by weighing risks and opportunities, because some assumptions cannot be relaxed at a later date without significant impact on cost and schedule. In cases where extra conservatism is added because the design is immature, this conservatism should be documented so that it can be reevaluated later as the design matures. The degree of conservatism can be relaxed and the provisional set of SSCs may be refined when justified by evolving design information.

4.1.6 Risk and Opportunity Assessment

The safety-in-design integration process shall incorporate use of a Risk and Opportunity Assessment (R&OA) tool for tracking and assessing the risks/opportunities associated with safety and design features affecting project cost, schedule and contingencies.[7]

4.1.7 Stakeholder Issues

Specific issues that have been raised by outside stakeholders, such as local, state, and public interest groups, should be addressed at the appropriate stage of the project. The R&OA may be used for this purpose.

4.1.8 Use of Integrated Safety Management Guiding Principles

To ensure effective and efficient integration of safety into the design, a systematic approach requiring implementation of the core functions should be implemented in the design process. Important guiding principles involved in this process and addressed in this Standard are (a) identification of safety standards and requirements and (b) 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.

[7] See DOE G 413.3-7A, *Risk Management Guide*, for additional guidance.

4.2 PRE-CONCEPTUAL DESIGN PHASE

During the pre-conceptual design development phase for DOE O 413.3B projects, the DOE Program Office identifies and analyzes any shortfall in its current capabilities when viewed in light of its strategic mission. This analysis forms the basis of the Mission Need Statement, the vehicle for formally establishing a project to address the capability deficiency. The mission need determines the overall scope and objectives of the project.

4.2.1 Capability Analysis

The capability analysis provides the basis for the Mission Need Statement. It determines whether a new facility or a modification to an existing facility would best satisfy the mission need. The Program Office is responsible for performing the capability analysis and may direct contractor tasks, including performing the following activities to support this analysis:

- Identification of material inputs and outputs, together with the process technology options, to permit a credible initial assessment of the hazards posed by each proposed process;[8]
- Preparation of a qualitative assessment of the physical and programmatic risks associated with various available alternatives (i.e., new facility, modification, or no change); and
- Preliminary determination of safety functions for major systems and hazard controls, based on a qualitative hazard analyses.

4.2.2 Mission Need Statement

Based on the results of the capability analysis, the Program Office drafts the Mission Need Statement. The Statement should:

- Describe safety-in-design information affecting the mission need, commensurate with information available at the pre-conceptual phase;
- Identify capability gaps and translate them into functional requirements that cannot be met through other than material means;
- Describe the general parameters of the solution;
- Explain the benefits of the solution; and
- State why the solution is critical to the overall accomplishment of DOE's mission.

4.2.3 Expectations of DOE

DOE will provide expectations for execution of safety-in-design efforts. DOE O 413.3B requires that the SDS developed in the conceptual design phase be based on those DOE expectations.

[8] Generally, a simple process model that shows the material inputs and outputs will satisfy this purpose.

4.3 CONCEPTUAL DESIGN PHASE

During the conceptual design phase, alternatives for satisfying the mission need are evaluated in detail to identify the preferred alternative for preliminary design. The scope of the alternatives analysis should be comprehensive enough to ensure that the selected alternative is best suited for safety-in-design integration, technology readiness, type of facility, site location, security, constructability, and operability. The alternatives analysis shall consider inherently safer design concepts.

The design organization shall identify the functional and performance requirements of major safety systems in a timely manner to ensure that safety becomes an integral part of the design. DOE-HDBK-1132-99, *Design Considerations*, provides safety-in-design considerations for major systems such as:

- Confinement systems,
- Fire protection systems,
- Facility layout and design,
- Process equipment and piping systems,
- Mechanical systems,
- Electrical, instrumentation, and control systems, and
- Handling of special nuclear material.

4.3.1 Hazards Analysis at the Conceptual Design Phase

A qualitative evaluation of the potential facility hazards shall be performed for the available alternatives to assist in identifying a preferred option (and possibly a back-up alternative). A more detailed facility-level hazards analysis shall be performed for the preferred alternative. This hazards analysis (a) describes the initial major hazards and other risk areas that could affect project cost and schedule and (b) identifies significant hazard scenarios and the initial suite of facility design basis accidents (DBAs). This preliminary assessment of anticipated hazards provides an initial inventory of nuclear as well as hazardous material as a basis for preliminary hazard categorization of the facility. This hazard analysis should evaluate inherently safer design concepts to eliminate and reduce hazards where possible. The hazards analysis shall factor in the results of a preliminary security vulnerability assessment for each design alternative.

4.3.2 Fire Hazards Analysis

A Fire Hazards Analysis (FHA) shall be developed for the preferred alternative. The FHA at this phase will reflect the scope of the design for selection of the preferred alternative. Section 4.1 of DOE-STD-1066-2016, *Fire Protection*, provides additional guidance on the integration of the FHA into the design process.

4.3.3 Facility-Level Accident Analysis

Accident analysis entails characterization of a limited set of accidents, referred to as DBAs, and the determination of consequences and hazard controls associated with these events (see DOE-STD-3009-2014 for additional discussion). Accident analyses for the preferred alternative, where the conclusions could impact project cost and schedule, shall be performed to identify the major facility safety functions needed.

4.3.4 Identification of Important Safety Functions and Major Safety SSCs

Important facility safety functions, including major safety SSCs, shall be addressed during the conceptual design phase for the preferred alternative. Such functions include radioactive material confinement, fire protection, life safety, emergency power, natural phenomena hazards (NPH) design, and security features. The interface of major safety and security functions shall be examined to identify any conflicts, constraints, or cross-purposes.

Hazards control strategies for significant hazard scenarios and DBAs shall be clearly identified in the hazards analysis. The control strategies should include (a) classification of major safety SSCs and their initial safety functions and (b) NPH design categories for major SSCs.[9]

4.3.5 Conservative Design Margins

To ensure that the initial cost estimates are realistic, the hazards analysis and the selection of major safety SSCs should be conservative. Initial selection of major safety SSCs and their design margins, therefore, should account for a wide range of uncertainties in hazards analyses and technology readiness.

4.3.6 Required Documentation

The following documents shall be developed by the completion of the conceptual design phase: SDS (see Appendix B), Conceptual Design Report (CDR) for DOE O 413.3B projects only, CSDR (see Appendix C), QAP, National Environmental Policy Act (NEPA) Strategy, Environmental Compliance Strategy, Checkout/Testing/Commissioning Plan, and the COR. The SDS, the CDR, and the CSDR should document the basis for preferred alternative selection, technology readiness status, assumptions, safety-in-design risks, and opportunities.

[9] The design information available at this phase will be limited and may involve several design alternatives, but this effort is needed to identify a preliminary set of major safety SSCs. Identifying and classifying the major safety SSCs, both safety class and safety significant, which are major contributors to project cost and schedule, is a fundamental part of the safety-in-design process.

4.3.7 DOE Review of the CSDR

In accordance with DOE-STD-1104-2016, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents,* DOE reviews the CSDR and documents the review in a safety review letter. The purpose of this review is to confirm that the preliminary safety positions adopted during conceptual design constitute an appropriately conservative basis for preliminary design. These safety positions include:

- Hazard categorization (HC-1, 2, or 3) of the facility;
- Preliminary identification and analysis of the facility hazards and DBAs;
- An assessment, based on significant hazard scenarios and DBAs, of the need for safety class and safety significant hazards controls;
- Consideration of inherently safer design concepts, and application of the hierarchy of controls;
- Preliminary assessment of the applicable NPH design criteria; and
- Approach to meeting the safety design criteria of DOE O 420.1C, Chg. 1, or approved exemptions and equivalencies.

4.4 PRELIMINARY DESIGN PHASE

During the preliminary design phase, the hazards and accident analyses are completed at the facility level, and facility level safety functions and safety SSCs are identified. Satisfactory completion of preliminary design includes technology readiness of major SSCs and no significant uncertainties such that the detailed design can proceed. An important aspect of the preliminary design phase is obtaining DOE review and approval of Preliminary Safety and Design Results.

4.4.1 Hazards and Accident Analyses

The hazards analysis initiated during the conceptual design phase for the preferred alternative forms the basis for the project's PDSA, which will address the hazards analyses, accident analyses, and selection of safety controls. The hazards analysis will evolve from a facility-level analysis to a system level hazards analysis as design detail becomes available. As the project design progresses, more detailed hazards analysis is performed to identify "process-related" hazards and the need for appropriate controls. As the hazards analysis is refined, the selection of controls, safety functions, and classifications developed during the conceptual design phase will 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 can have significant impacts on overall project cost and schedule.) The hazards analysis shall include consideration of inherently safer design concepts to remove and reduce hazards where possible. The hazards analysis also identifies whether the planned facility contains chemical hazards that necessitate hazard or accident analysis and possible identification of safety significant SSCs. The potential impact of updates to the security vulnerability assessment (based upon the

developing design of proposed security features) should be considered with respect to hazards and hazard controls.

4.4.2 SSC Selection and Classification

The initial selection and classification of safety SSCs identified during the conceptual design phase shall be further refined as the design and safety and hazards analyses mature. SSCs shall be classified as safety class, safety significant, or other hazard controls. Other hazard controls often play an important role in safety by providing protection from identified hazards, supporting safety related controls, and providing defense-in-depth.

4.4.3 Fire Hazards Analysis

The FHA developed for the conceptual design phase for the preferred alternative is further refined using facility and process level information. Additional analysis of fire hazards is performed as needed to guide design implementation of fire protection requirements.

4.4.4 Technology Readiness Assessment

DOE O 413.3B requires a technology readiness assessment to be conducted for the preferred alternative and development of a Technology Maturation Plan, as appropriate (see DOE G 413.3-4A for additional guidance). DOE O 413.3B establishes targets for Technology Readiness Level (TRL) scores at various stages of design.

4.4.5 Preliminary Safety and Design Results

The following Preliminary Safety and Design Results shall be produced during the preliminary design phase:

- Site Description.
  - Site information of the type that can affect safety-in-design, such as location of nearby facilities and external hazards, meteorological information for dispersion analyses, and natural phenomena (e.g., seismic, wind) data.
- Facility Description.
  - Facility structure type and layout;
  - Process descriptions (includes details on basic process parameters, hazardous materials, process equipment in sufficient detail to support accident assessment and the safety analysis);
  - Confinement systems; and
  - Other major systems and support systems.
- Hazard and Accident Analysis.
  - Summary of facility-level and process systems hazards and accidents analyses, hazard categorization, and results of hazards evaluation;
  - Hazard evaluation tables or data sheets for each hazard scenario, describing: brief unmitigated hazard scenario description and assumptions; likelihood of the hazard

scenario; consequences of the hazard scenario; safety functions and preventive features; mitigated consequences; available controls; and
  - FHA.
- Description of Safety SSCs and SACs.
  - Control description with safety function and its relationship to the hazard and accident analysis,
  - Functional requirements, and
  - Performance criteria judged to require TSR coverage.
- Summary of Key Design Activities.
  - Description of any remaining TRL activities; and
  - Description of any other studies needed to address specific details of the design, such as validation of key assumptions, equipment section, and design optimization.

Commensurate with the design completion, these Preliminary Safety and Design Results shall demonstrate the adequacy of the hazards analyses and the selection, classification, and hierarchy of controls. Although completion of component-level design at this stage is not expected, it is prudent to complete component-level design and determine the critical characteristics for acceptance during the preliminary design on those safety SSC items slated for long-lead procurement. These Preliminary Safety and Design Results shall be internally consistent and under configuration management in accordance with the CM plan.

The Preliminary Safety and Design Results may be packaged into a single document designated a "Draft PDSA." If packaged as a single document, that document should be formatted consistent with Appendix D of this Standard, although all sections need not be complete at this stage. An alternative to a Draft PDSA at the preliminary design phase may be individual project, design, and/or safety documents that provide the design results above. An important advantage of packaging these results into a single document is that it assures integration and ease of use for final design.

In addition, the following documents shall be developed or updated by the completion of the preliminary design phase:

- SDS (updated as necessary to reflect significant changes or reported to not require updating),
- NEPA documentation to support the selected site,
- QAP, and
- COR (identifying applicable requirements for the design, including applicable codes and standards).

The COR may be in the form of a requirements database.

4.4.6 DOE Review of Preliminary Safety and Design Results

A review and approval of the Preliminary Safety and Design Results is conducted by DOE upon completion of preliminary design (that is, when the Preliminary Safety and Design Results described in Section 4.4.5 are available for review). The review may consist of a single review or a series of reviews, based on when the preliminary design of the facility (or of defined segments of the design) is complete and ready to enter final design. This review is conducted by a DOE-selected team of experts and its results provided to the FPD for review and action as necessary. The size and composition of the team reflects the size and complexity of the project. More than one review may be conducted at the discretion of the FPD; the SDS should define segments when more than one review is planned. The independent review(s) should be scheduled as early as practicable, after completion of preliminary design, to minimize project risk.

The scope of the independent review includes the following:

- Completeness of the Preliminary Safety and Design Results (satisfying Section 4.4.5), and consistency of design with the safety strategy provided in the SDS;
- Resolution of any open conditions of approval identified in the safety review letter for the CSDR;
- Approach to meeting the general design criteria of DOE O 420.1C, Chg. 1, Attachment 3 (or approved exemptions and equivalencies), and identification of appropriate codes and standards, including technical justifications, as necessary;
- Identification and description of a viable design solution (in terms of major safety SSCs) that provides the safety functions called for in the hazard and accident analysis;
  - The unmitigated accident consequence assessment provides adequate basis to assign appropriate functional classification and NPH design categories for major SSCs, and
  - The hazard and accident analysis provides adequate basis to identify the functional requirements and conditions that the major safety SSCs need to address.
- Consideration of inherently safer design concepts (see Section 4.1.3), and application of the hierarchy of controls (see Section 4.1.4);
- Identification and description of the technical studies needed to complete the safety design, including TRL activities; and
- Identification and description of safety design risks and risk mitigation strategies for the final design phase.

The findings of the DOE review of Preliminary Safety and Design Results are approved by the Safety Basis Approval Authority, with the concurrence of the FPD. The design organization shall address and resolve the findings of this review on an agreed-upon schedule. Resolution may occur in parallel with ongoing design efforts.

4.5 FINAL DESIGN PHASE

The goal of the final design phase is to achieve 90 percent design completion, meaning a level capable of supporting procurement, construction, testing, and operation. At this phase, the design organization finalizes the hazards and accident analyses, FHA, security vulnerability assessments, and other supporting analyses for design completion.

4.5.1 90 Percent Design Completion

A design completion of 90 percent shall be achieved at the completion of the final design phase. According to DOE O 413.3B, the following attributes signify 90 percent design completion:

- Complete final drawings and specifications that may be released for bid and/or construction;
- Current and detailed cost estimate;
- Current construction schedule;
- Clearly-defined testing requirements and acceptance criteria for the safety and functionality of all subsystems;
- Independent technical, construction, operation, and environmental reviews of the final drawings and specifications;
- Quality control review that evaluates both technical accuracy and discipline coordination;
- Final design that meets all the requirements stipulated in the COR;
- Final design review, consisting of final validation of comment resolution from previous reviews, and a review of any additional developments since the last review; and
- Checking and verification of any required waivers or exemptions.

In addition, the following documents shall be developed or updated by the completion of the final design phase:

- SDS (updated as necessary to reflect significant changes or reported to not require updating),
- Hazard Analysis,
- FHA,
- Accident analysis, as applicable,
- Security vulnerability assessment,
- R&OA,
- PDSA,
- COR (applicable design requirements including codes and standards), and
- QAP.

See Table 4-1 at the end of this section for an overview of the responsibilities for key nuclear safety design documents at the 90 percent completion stage.

If any open items exist, these items shall be identified and evaluated as representing low technical, cost, and schedule risk to the project.

4.5.2 Procurement Support

Safety design analyses, design requirements, and performance criteria for safety class and safety significant SSCs shall be used to develop the details of procurement specifications in support of construction activities. DOE's approval of the PDSA precedes procurement of materials or components for construction (except for long-lead procurements, addressed below).

4.5.3 Long-Lead Procurement SSCs

Section 830.206 of 10 CFR Part 830 states:

> *DOE may authorize the contractor to perform limited procurement and construction activities without approval of a PDSA if DOE determines that the activities are not detrimental to public health and safety and are in the best interests of DOE.*

Caution should be exercised before proposing for DOE approval any limited procurement and construction activities prior to completion of the final design and approval of the PDSA.

To support the long-lead procurement of SSCs, which is sometimes needed to maintain the project's schedule prior to PDSA approval, the design organization shall submit to the FPD (or responsible approving authority) safety documentation providing the following information:

- Description of the scope of long-lead procurement items,
- Reason for the request and the benefit to DOE,
- Impact (cost and schedule) of not conducting the requested activity,
- Risks and opportunities associated with performing the requested activity,
- For SSCs being procured:
  - Functional classification, if any, and
  - Hazard scenarios/accidents, if any, that the SSCs are being credited to prevent or mitigate.
- For Safety SSCs only:
  - Complete description of the item,
  - Status of design completion, including any support systems and other interfaces,
  - Status of safety analysis (including process-level hazard analysis) and any unverified assumptions,
  - Safety Functions, Functional Requirements, and Performance Criteria,
  - Inspections, tests, and acceptance criteria, as necessary, and
  - Risk associated with release for procurement.

4.5.4 Configuration Management Process

The CM process at the final design stage shall track changes to the design as established in the project CM plan (see Section 3.8).

4.5.5 PDSA Development

The PDSA should be initiated following completion of preliminary design. The PDSA shall be developed using the methodology, criteria, and guidance of DOE-STD-3009-2014, or other equivalent method (see Appendix D for additional guidance on PDSA format and content).

Preliminary TSRs should be developed in concert with PDSA development. By drafting preliminary TSRs at this phase, the project can better identify and address any unique design attributes needed to facilitate surveillance.

4.5.6 DOE Approval of the PDSA

Section 830.206 of 10 CFR Part 830 requires DOE approval of the PDSA before the contractor can procure materials or components or begin construction, except in cases where DOE approves long-lead procurement as described in Section 4.5.3.

4.5.7 Inspections, Tests, and Acceptance Criteria

Inspections, tests, and acceptance criteria shall be developed by the design organization for validating that functional requirements and performance criteria are met for all SSCs important to safety.

4.6 CONSTRUCTION AND TRANSITION TO OPERATIONS

The goals of this phase are to support construction, maintain configuration controls, develop the DSA and TSRs, and support transition to operation (including development of SMPs and support of start-up testing).

4.6.1 100 Percent Design Completion

At the completion of final design, the project will have achieved 90 percent design completion. The design may continue to evolve, as necessary, during construction. The following activities are examples of design activities that will be needed during and after construction to achieve 100 percent design completion:

- Completing design details and installation that do not impact cost estimates or the PDSA;
- Completing as-built documentation;
- Addressing changes based on equipment actually procured;
- Addressing changes based on as-built configuration; and

- Addressing changes based on updated vendor information.

4.6.2 Construction Support and Configuration Controls

Construction of the project design requires close coordination and integration to maintain various interfaces between design documents and physical configuration requirements. Numerous changes to the final design can occur during construction, some of which may affect the assumptions, commitments, or results of the safety analysis. During construction, a CM plan (see Section 3.8) shall be used to ensure that any change to the approved final design is fully evaluated for its impact on the safety design basis. For example, hazard analyses that were completed as part of the PDSA shall be maintained under configuration control such that changes are identified and can be incorporated into the final DSA.

4.6.3 Development of DSA and TSRs

The DSA and TSRs shall be developed based on the approved final design and any changes made during the construction process. The DSA and TSRs can be completed when it is confirmed that facility configuration matches the design documentation.

4.6.4 Required Documentation

The DSA, TSRs, and the COR shall be finalized by the completion of this project phase.

4.6.5 DOE Approval of DSA

Section 830.207 of 10 CFR Part 830 requires DOE approval of the DSA via issuance of a SER.

4.6.6 Checkout/Acceptance, Testing, and Commissioning

Planning for checkout/acceptance, testing, and commissioning is coordinated with the operating organization to facilitate an efficient, timely turnover and ensure functionality of SSCs.

The following activities shall be accomplished in a timely manner for successful turnover of safety SSCs to operation:

- Prepare and approve test procedures, and organize test teams,[10]
- Validate that inspections and tests have been completed and that acceptance criteria are met for SSCs,
- Walk down facilities to identify and correct physical, process, safety, quality, or environmental deficiencies, and

[10] Testing serves to verify that the components, systems, and facilities meet or exceed design requirements and performance parameters and help to train operating personnel in the operation of the equipment, systems, and other components of the completed project.

- Ensure effective knowledge transfer, including transfer of key design basis documents and COR, between the project/design and the operating organizations.[11]

4.6.7 Readiness Reviews

DOE O 425.1D, *Verification of Readiness to Start Up or Restart Nuclear Facilities*, requires that a readiness review be performed prior to commencement of facility operations.

4.6.8 Project Closeout

At the completion of construction and testing activities, project documentation (including as-built documentation) shall be turned over to the operations organization. Any unresolved deficiencies identified in Section 4.6.6 should also be communicated to operations.

4.7 RISK MANAGEMENT PLAN

4.7.1 Overview

DOE O 413.3B requires the project to use a Risk Management Plan (RMP) for managing risks and uncertainties affecting safety-in-design and project objectives. The risk management process includes R&OAs consisting of identification, assessment, and plans for mitigation of risks. Given the potentially significant costs associated with safety decisions, the integration of safety into the design process should include a strong link between the development of safety-in-design and identification of project technical and programmatic risks. DOE G 413.3-7A provides a framework for developing the RMP.

4.7.2 Identification and Management of Risks

Early identification of possible opportunities to address potential risks allows the project to define appropriate cost 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 project's risks and opportunities assessments are intended to be inputs to its RMP and to be managed accordingly.

The risk breakdown structure described in DOE G 413.3-7A should be used to identify safety-in-design development risks and their consequences to the project. Once the risks are identified and prioritized, sound risk mitigation actions should be developed and tracked to completion. The following are examples of safety-in-design risk factors that could have significant cost and schedule effects on the project:

[11] The design organization works closely with the user in developing and presenting specific process and facility training, and continues to provide support to the operations/maintenance staff throughout transition and turnover.

- Technology maturity
- Safety analysis assumptions
- Design margins/degree of conservatism
- Safety classification of major SSCs
- Confinement strategy
- Fire protection
- Security
- Site location and infrastructure
- Facility footprint
- NPH design categories

4.8 SAFETY PROGRAM AND OTHER IMPORTANT PROJECT INTERFACES

This section highlights programs and site support interfaces linked with the safety-in-design process. Because most of these programs and interfaces concern aspects important to design, their consideration should be integrated into the design effort as early as it is practical to do so.

4.8.1 Safety Management Programs

Section 830.204(b)(5) of 10 CFR Part 830 requires defining the characteristics of certain SMPs where applicable: QA, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection. (Identified SMPs are not precluded) Such programs shall be evaluated in light of the proposed design to assure that the design supports program implementation. In some cases, design requirements need to be defined that support SMP implementation. These requirements shall be identified and included in the project design requirements, and addressed in the DSA.

4.8.2 Other Design Interfaces

In addition to SMPs, other interfaces should be considered for potential impact on the project. In some cases the interface has its own controlling regulatory document (for example, worker safety under 10 CFR Part 851), while in other cases these interfaces are integral to providing a cost-effective operational facility that meets safety requirements. Each such interface should be evaluated against the proposed design to assure that the design supports implementation.

4.8.3 List of Potential Interfaces

A list of potential interfaces follows:

- Radiation Protection
- Fire Protection
- Maintenance
- Procedures & Training
- Conduct of Operations
- QA

- Emergency Preparedness
- Waste Management
- Worker Safety and Health Program
- Infrastructure
- Human Factors
- Security
- Environmental Protection
- Hazardous Material
- External Reviews
- System Engineer Program
- Transportation
- Criticality Safety

Appendix E of this Standard provides further guidance on SMPs and other design interfaces.

Table 4-1. Responsibilities for Key Nuclear Safety Documents

Key Nuclear Safety Documents Developed by the Contractor	Responsibility			Interface with Other Documents/Products
	Prepare	Review	Approve	
SDS	SDIT.	IPT and DOE.[12]	FPD and DOE.	The SDS is part of or can be referenced in the Project Execution Plan.
R&OA	SDIT.	IPT and DOE.	FPD.	The R&OA is input to the RMP.
CSDR	SDIT.	IPT and DOE.	DOE, with concurrence by the FPD.	CSDR needs to be consistent with the CDR.
PDSA	SDIT.	IPT and DOE.	DOE in the SER on the PDSA, with concurrence by the FPD.	PDSA needs to be consistent with the Final Design.
DSA and TSRs	SDIT, assisted by operations personnel.	IPT and DOE.	DOE in the SER on the DSA.	The DSA is consistent with the as-built configuration. TSRs are derived from the DSA.

[12] DOE's role as reviewer and approver of safety design basis documents is described in detail in Section 8 of DOE-STD-1104-2016, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents*.

5.0 INTEGRATION OF SAFETY INTO FACILITY MODIFICATIONS

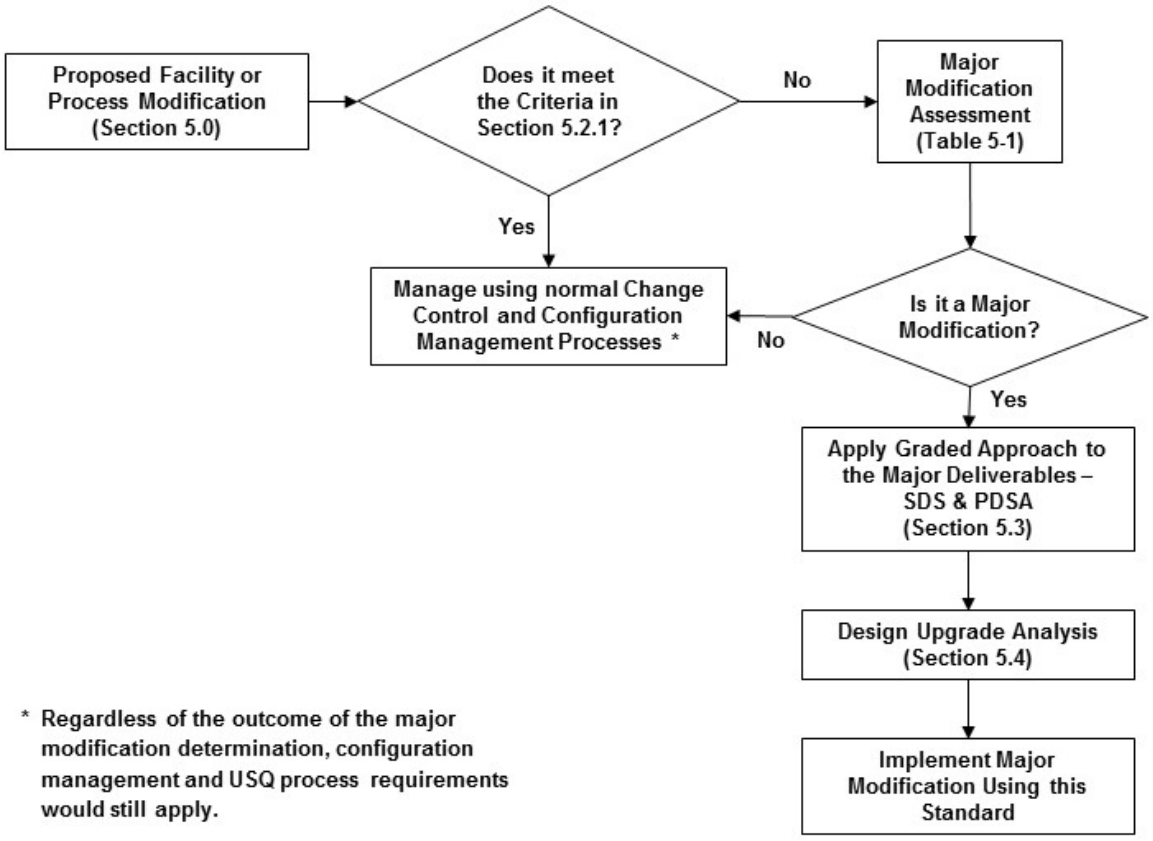
5.1 OVERVIEW

This section sets forth (a) the process for determining whether a facility modification is a "major modification" as defined by 10 CFR Part 830 and (b) the basis for the graded approach in applying requirements associated with a major modification determination. Specifically, this section provides the following:

- An entry process for determining pre-screening of facility modifications,
- The method and assessment criteria whereby a major modification is determined,
- A graded approach for applying DOE safety requirements associated with a major modification determination, and
- The requirement for a design upgrade analysis.

Figure 5-1 below illustrates the process now to be described:

Figure 5-1: Major Modification Determination Process



5.2 MAJOR MODIFICATION DETERMINATION

A major modification determination[13] should be commenced as early in the planning stage for a facility modification as is feasible. However, the scope of the modification should be mature enough to perform a meaningful review and evaluation.

Any facility modification that involves design effort shall be either: (1) evaluated using the criteria in Section 5.2.1 to determine whether the proposed modification needs to be further assessed in accordance with Section 5.2.2; or (2) processed in accordance with Section 5.2.2. An equipment change that does not involve a design effort is not a major modification and does not need to go through this process. Examples of such cases include equipment maintenance and like-for-like replacement of equipment.

Regardless of the outcome of the major modification determination, configuration management and USQ process requirements would still apply.

5.2.1 Criteria for Entering the Major Modification Determination Process

A modification that meets all of the following criteria (also known as a "simple" modification) is not required to enter the major modification determination process:

- The modification involves only hazards that have been evaluated by the existing safety analysis;
- Existing hazard and accident sequences remain applicable, including the frequency, consequence, and probability of malfunction of safety SSCs; and
- Required hazard controls have already been identified and implemented.

Modifications meeting these criteria may be managed using normal change control and CM processes.

5.2.2 Major Modification Assessment

Any proposed modification not meeting the entry criteria of Section 5.2.1 shall be assessed according to the requirements in this section. The six criteria in Table 5-1 below shall be used to evaluate whether a major modification exists. Each criterion addresses a key project characteristic relevant to the requirements associated with a major modification. In applying the evaluation criteria, a single "Yes" answer does not necessarily indicate that a major modification exists. Each criterion shall be assessed individually and then an integrated evaluation performed based on the collective set of individual results. In performing this evaluation, the focus should

[13] The major modification process is not appropriate to use for a new facility. Typically, if the functions and/or processes of the change are to be housed in a separate structure, and are not enveloped within the mission of the existing facility, a proposed change is considered a new facility, rather than a major modification.

be on the extent of the impact on the facility safety basis.

In determining whether an environmental restoration activity constitutes a major modification (and therefore requires a PDSA), emphasis should be placed on the amount of new construction involved, the hazard level and associated hazards, and the safety functions provided by and potentially affected by the new construction. Appendix A of 10 CFR Part 830 states:

> *As a general matter, DOE does not expect preliminary documented safety analyses to be needed for activities that do not involve significant construction such as environmental restoration activities, decontamination and decommissioning activities, specific nuclear explosive operations, or transition surveillance and maintenance activities.*

Appendix F of this Standard provides several examples of major modification determinations.

Table 5-1. Major Modification Assessment Criteria

Major Modification Assessment Criteria	Guidance for Application
1. Add a new building or facility with a material inventory ≥ 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, Chg. 1, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, September 1997, shall be 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 or safety significant safety function or associated SSC?	A change in the footprint of an existing facility requires the identification and evaluation of any potential adverse impacts on safety class or safety significant 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 sets may no longer be valid. The evaluation of any new hazards introduced by the revised or new process should be addressed via Criterion 6.

Major Modification Assessment Criteria	Guidance for Application
4. Use 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 includes 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. 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.
5. Create the need for new or revised safety SSCs?	Consideration is 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 (as applicable) should be addressed for this criterion for the development, review, and approval of new or revised safety analysis and attendant controls.
6. Involve a hazard not previously evaluated in the 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.

5.2.3 DOE Concurrence

Major modification assessments assigned at least one “yes” answer shall be provided to the DOE field element manager or designee, together with supporting technical justification. Major modification assessments that assign “no” to all criteria may be submitted to DOE for information only.

5.3 GRADED APPROACH

Where a major modification is found to exist, a graded approach to the requirements of this Standard may be used. The graded approach shall consist of the following elements:

- An SDS that addresses (1) the application of nuclear safety design criteria, (2) the graded content of the PDSA necessary to support the design of the facility modification, (3) the need for and content of other project-supporting safety documentation in addition to the PDSA (such as a CSDR), and (4) the interface with the existing facility, its operations, and construction activities.

- A PDSA graded in content to include the required provisions from 10 CFR Part 830 without the full format and content of a PDSA supporting a new facility. These required provisions are:
  - The nuclear safety design criteria to be satisfied;[14]
  - A safety analysis that derives aspects of design that are necessary to satisfy the nuclear safety design criteria; and
  - An initial listing of the SMPs to be developed to address operational safety considerations.
- The safety analysis within the PDSA is required by DOE O 420.1C, Chg. 1, to include identification of the following:
  - Safety-class and safety-significant SSCs needed to fulfill the safety functions in order to prevent and/or mitigate identified hazard scenarios and accidents, including natural and man-induced hazards and events;
  - The functional requirements of the safety class and safety significant SSCs; and,
  - SACs needed to fulfill safety functions or protect the base assumptions of the hazard and accident analyses.

5.4 POTENTIAL FOR DESIGN UPGRADES

A design upgrade analysis shall be performed to evaluate the application of nuclear safety design criteria and requirements to the major modification project and to the existing facility. This analysis encompasses new and existing SSCs that provide a safety function credited for the major modification. This analysis should address:

- The applicability of codes and standards to the modification of an existing structure or system,
- The potential need for upgrading sections of the existing facility affected by the modification to meet new design requirements, and
- Interfaces between the new and existing sections of the facility to determine if the application of differing design codes or standards is feasible.

Appendix G of this Standard provides guidance for the development of a design upgrade analysis. This analysis should be included in the SDS in support of the application of nuclear safety design criteria. Proposed deviations from applicable requirements of DOE O 420.1C, Chg. 1, are required to follow the exemption or equivalency process of the Order. The PDSA is required to be approved by DOE before procurement of materials or components for construction can begin.[15]

[14] As provided by DOE O 420.1C.

[15] Limited procurement and construction without approval of the PDSA may be permitted by DOE in accordance with 10 CFR §830.206(b)(2).

5.5 REPURPOSING EXISTING FACILITIES

An existing nuclear or non-nuclear facility may be re-purposed to (a) fulfill a new mission and/or (b) increase the inventory of radioactive material such that a new hazard categorization applies.

A below-HC-3 nuclear or non-nuclear facility redesignated as an HC-3 or HC-2 nuclear facility shall be treated as a new HC-3 or HC-2 nuclear facility under 10 CFR Part 830. An SDS shall be prepared for DOE review and approval containing a plan for developing the DSA and TSRs. Facility modifications necessary to provide adequate safety shall be evaluated in accordance with Section 5 of this Standard and are subject to the design requirements of DOE O 420.1C, Chg. 1.

For an HC-3 facility being redesignated an HC-2 nuclear facility, a major modification determination shall be performed in accordance with Section 5 of this Standard.

6.0 REFERENCES

Users of this Standard are advised to review the list below to determine whether each listed document, a more recent version, or a replacement document is the most pertinent for each application. When alternate documents are used that are not listed here, users are advised to document this decision and its basis.

a. Code of Federal Regulations

(1) 10 CFR Part 830, *Nuclear Safety Management*
(2) 10 CFR Part 835, *Occupational Radiation Protection*
(3) 10 CFR Part 851, *Worker Safety and Health Program*

b. DOE Directives

(1) DOE P 450.4A, *Integrated Safety Management Policy*
(2) DOE O 413.3B, Chg. 2 (PgChg), *Program and Project Management for the Acquisition of Capital Assets*
(3) DOE O 414.1D, *Quality Assurance*
(4) DOE O 420.1C, Chg.1, *Facility Safety*
(5) DOE O 425.1D, *Verification of Readiness to Start Up or Restart Nuclear Facilities*
(6) DOE O 430.1B, Chg. 2, *Real Property Asset Management*
(7) DOE Order 470 Series, *Safeguards and Security Program*

c. DOE Manuals

(1) DOE M 140.1-1B, *Interface with the Defense Nuclear Facilities Safety Board*, 2001.

d. DOE Guides

(1) DOE G 413.3-1, *Managing Design and Construction Using Systems Engineering for Use with DOE O 413.3A*
(2) DOE G 413.3-7A, *Risk Management Guide*
(3) DOE G 413.3-18A, *Integrated Project Team: Guide for Formation and Implementation*

e. DOE Technical Standards

(1) DOE-STD-1020-2016, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities*
(2) DOE-STD-1027-92, Chg. 1, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports, September 1997*
(3) DOE-STD-1066-2016, *Fire Protection*
(4) DOE-STD-1073-2016, *Configuration Management*

(5) DOE-STD-1104-2016, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents*
(6) DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*

f. DOE Handbooks

(1) DOE-HDBK-1132-99, *Design Considerations*

g. DOE Memoranda

(1) Clay Sell, Deputy Secretary of Energy, December 5, 2005, "Integrating Safety into Design and Construction"
(2) Ernest J. Moniz, Secretary of Energy, June 8, 2015, "Project Management Policies and Principles"

APPENDIX A OVERVIEW OF THE SAFETY-IN-DESIGN PROCESS

A.1 PURPOSE

This appendix provides an overview of how safety is integrated into the design of DOE's nuclear facilities using the requirements and guidance of DOE-STD-1189-2016. The appendix stresses the importance of (a) active and competent project management and (b) a disciplined process for implementing the safety-in-design concept.

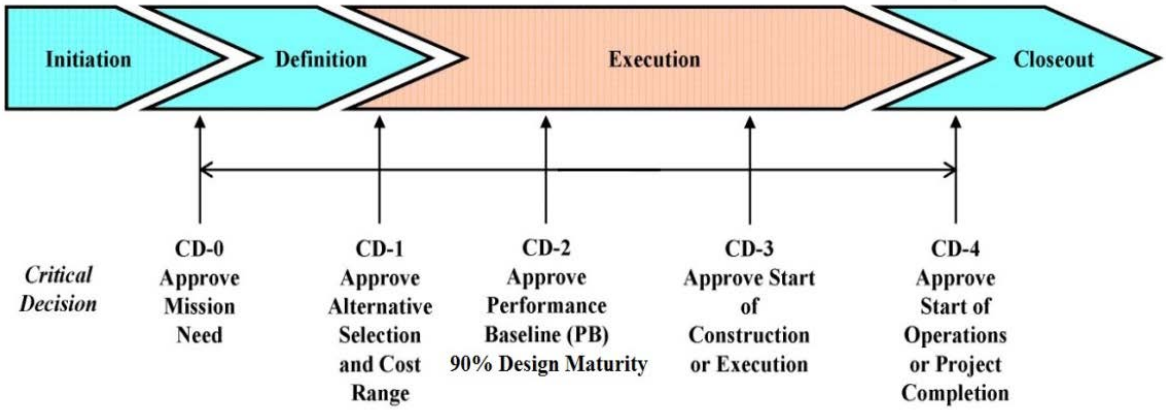
A.2 DOE's ACQUISITION MANAGEMENT SYSTEM

DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, which provides most of the requirements for the acquisition management system, sets out a framework for each phase of a capital acquisition project.

The five phases of the acquisition process are delimited by "Critical Decisions," referred to as CDs. Each CD marks an authorization to increase the commitment of resources to the project and is premised on successful completion of the preceding phase. Execution of a new project or major modification project, according to the Order, is premised on implementing the five project phases in sequence (see Figure A.2-1 below):

- CD-0: development of Mission Need Statement describing a need that cannot be met through other than material means.
- CD-1: development of a conceptual design for alternative selection; the selected alternative and approach is the optimum solution.
- CD-2: development of preliminary and final design; definitive scope, schedule and cost baselines have been developed, and the project is ready for implementation. (Design is 90% complete).
- CD-3: completion of any open items for construction support and release of funds for construction.
- CD-4: approval for start of operation or project completion.

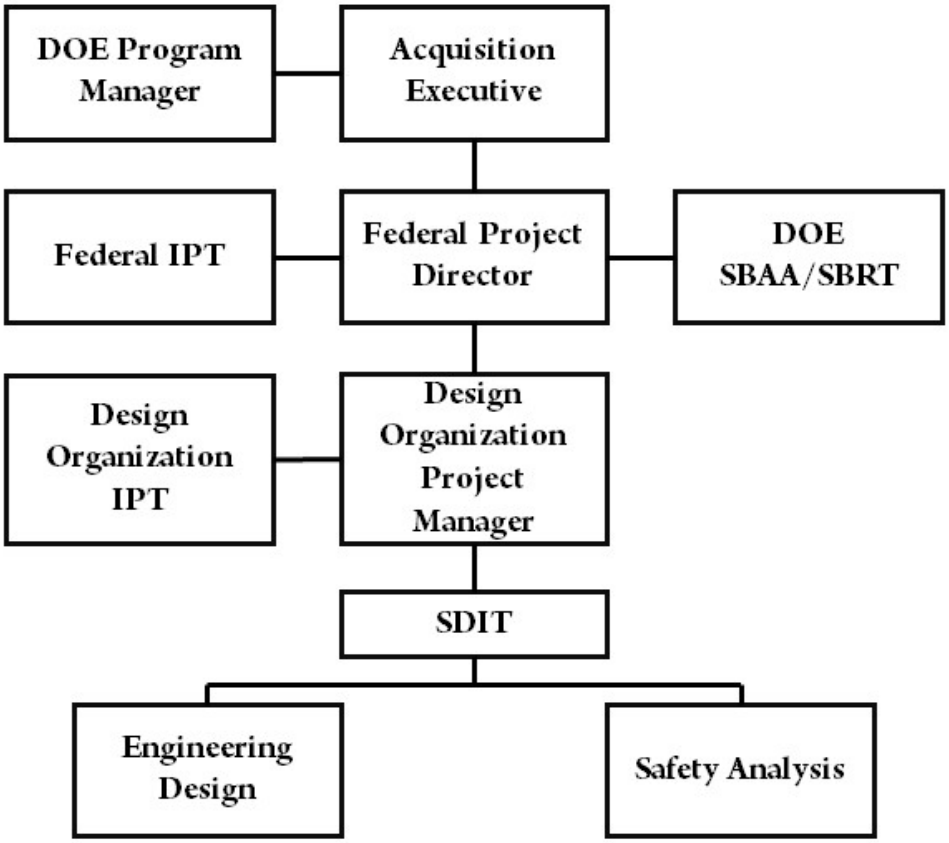
Figure A.2-1: DOE O 413.3B Project Lifecycle



A.3 PROJECT ORGANIZATION AND INTERNAL COMMUNICATIONS

Communication is an essential ingredient for successful implementation of the safety-in-design process. In many cases, capital asset acquisition projects are fairly complex and one-of-a-kind. To succeed, the Contractor Integrated Project Team (CIPT) (a) selects technological systems commensurate with mission needs, (b) fully understands the hazards associated with selected systems, (c) chooses safety structures, systems and components (SSCs) that will protect the public, workers, and environment, and (d) satisfies security needs. Management personnel and subject matter experts (SMEs) work together within the CIPT and Safety Design Integration Team (SDIT) to make risk-informed decisions leading to a successful project outcome (see Figure A.3-1 below). At early stages of the design, lack of information on final approaches to safety suggests that conservative assumptions should be made to avoid costly changes later on. The Risk and Opportunity Assessment (R&OA) approach may be an effective tool for tracking these assumptions and assessing their role in decision-making.

Figure A.3-1: Project Organization

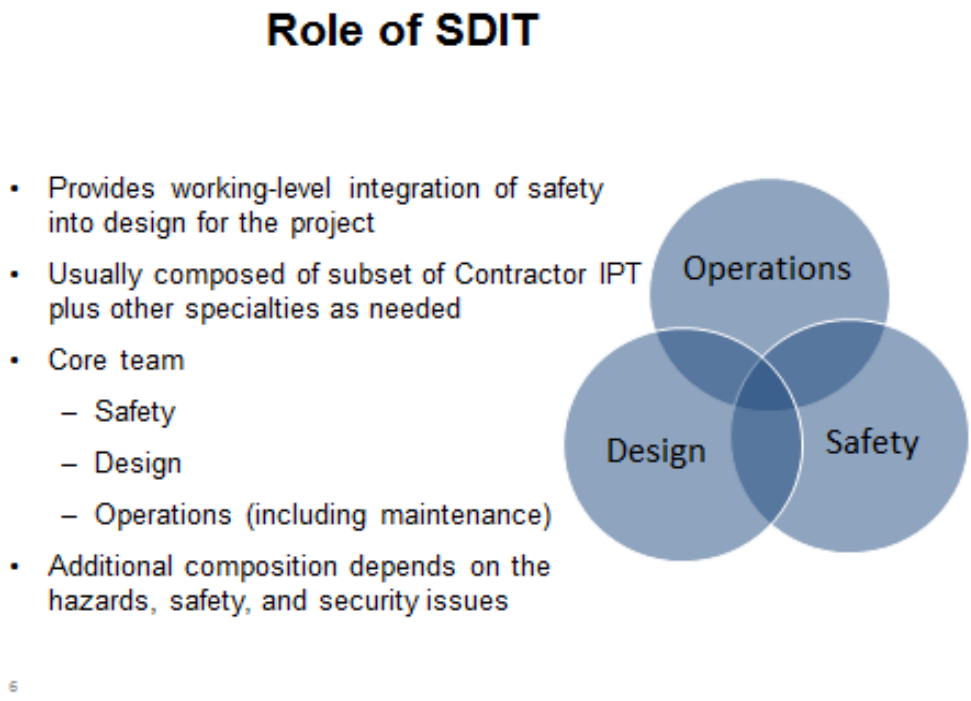


A.4 PROJECT PLANNING AND EXECUTION

As stated in Section A.1 above, DOE O 413.3B requires a certain sequence of project planning and activities be used to establish the performance baseline and cost estimates for the execution of the project. This same sequence serves to ensure cost-effective implementation of the safety-in-design concept. In a broad sense, this concept should be (a) evaluated while the design is being conceptualized, (b) integrated into the design during design development, and (c) implemented during construction.

For a large, complex project, safety design information may not be available during the conceptual and preliminary design phases. Yet the project needs to move ahead using the best available design assumptions and estimates of uncertainties. To assist the Federal Project Director (FPD) and the contractor's management organization, this Standard contemplates reliance on three expert teams: (Federal) Integrated Project Team (IPT), CIPT, and SDIT. These teams comprise SMEs in a range of disciplines who are collectively capable of assessing the design development process, understanding safety-in-design requirements, and assessing the risks, opportunities, and uncertainties associated with important project decisions. The teams serve as the eyes and ears for the FPD and the contractor's management organization. (See Figure A.4-1 below regarding the role played by the SDIT.)

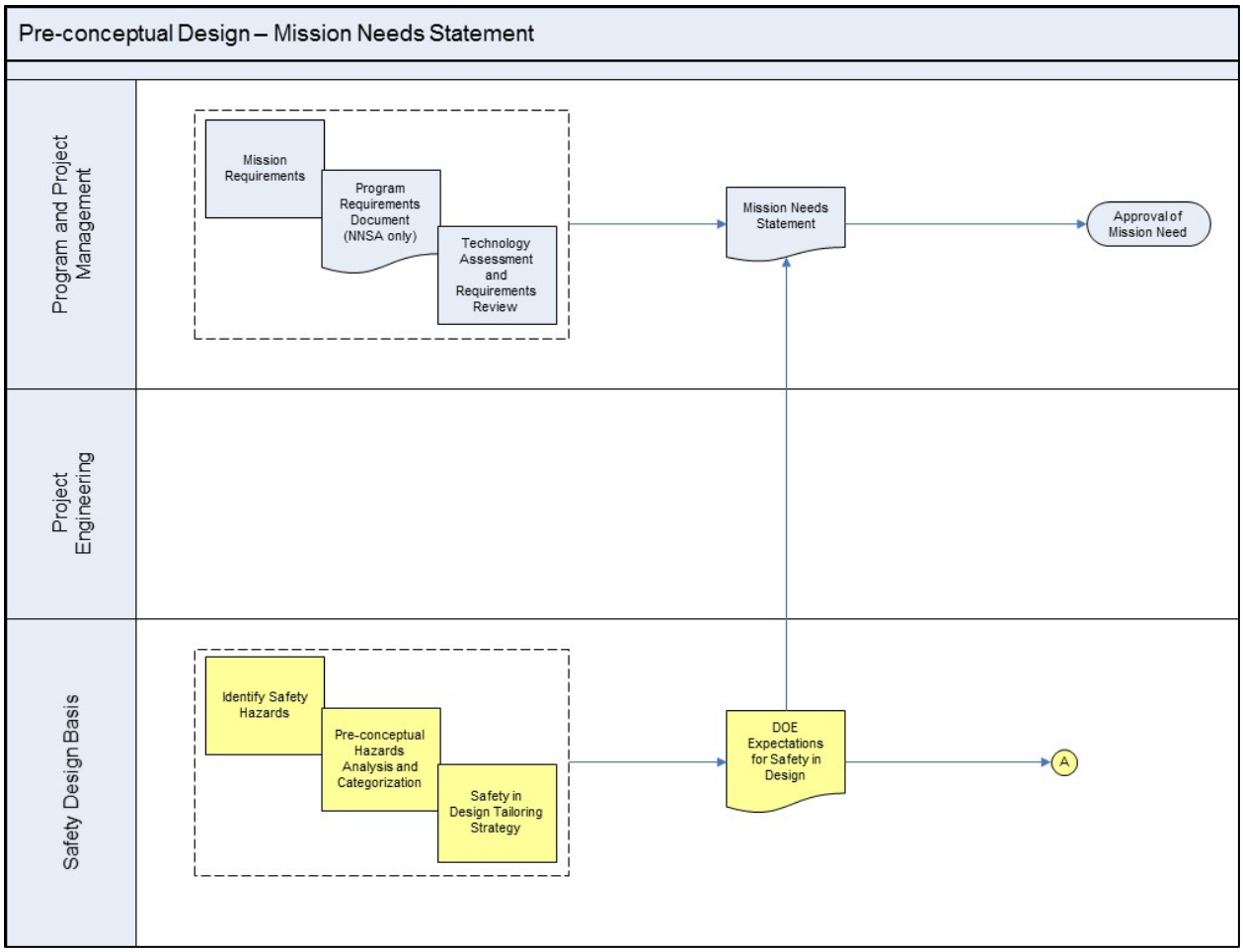
Figure A.4-1: Role of the SDIT



A.4.1 Pre-Conceptual Design Phase

During the pre-conceptual phase, an analysis of alternatives is performed to explore whether a new facility or a modification to an existing facility would best satisfy the mission need. Potential costs, benefits, and significant hazards are addressed to the extent required to determine the program gap and therefore the mission need. Figure A.4.1-1 below illustrates how project management and safety basis activities interact during the pre-conceptual design phase.[16]

Figure A.4.1-1: Pre-Conceptual Design Phase (CD-0)



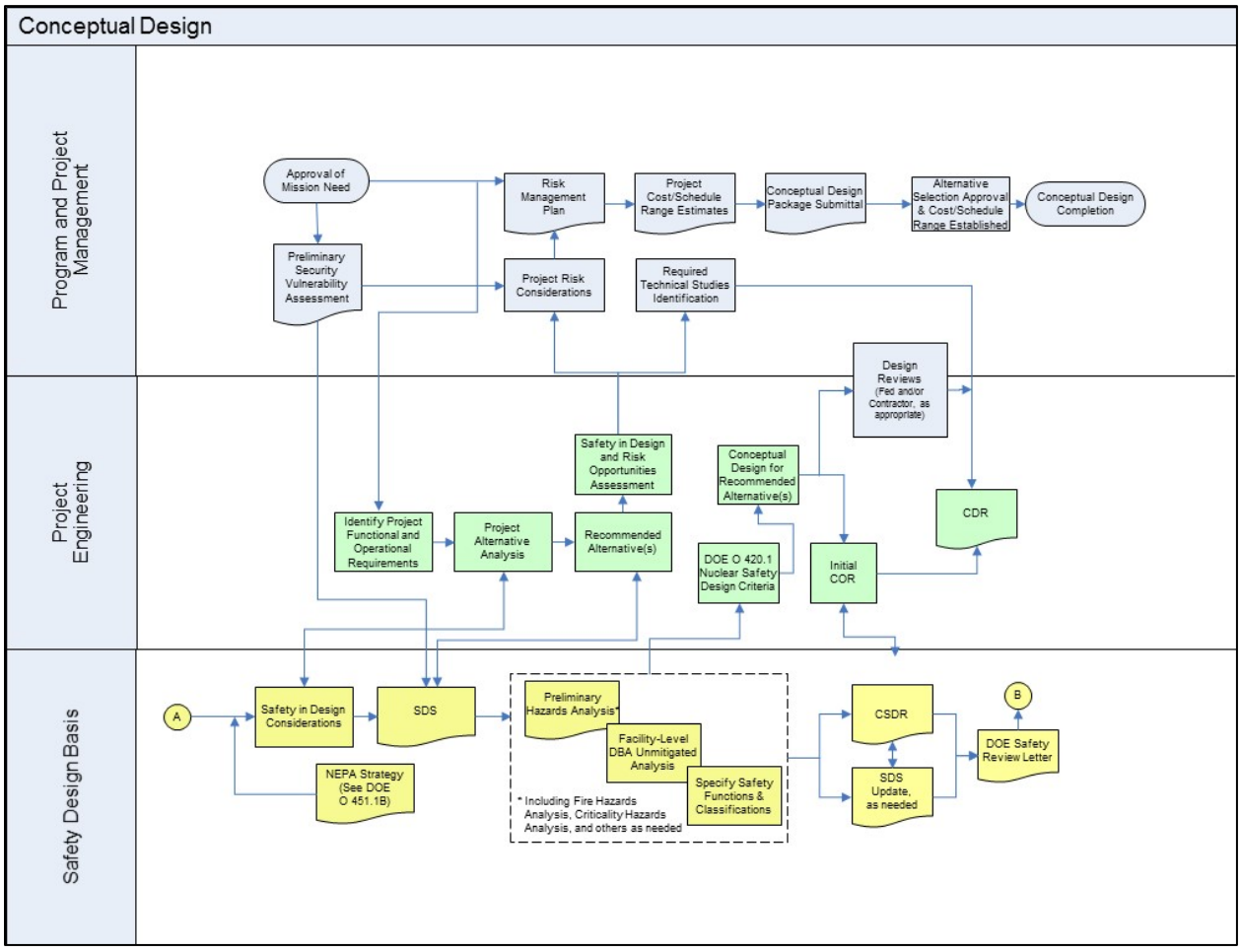
[16] See Appendix H for expanded flow diagrams showing the interface between safety in design and project management activities specified in DOE O 413.3B, Chg. 2.

A.4.2 Conceptual Design Phase

The conceptual design phase is devoted to evaluating alternative design concepts, preparing an SDS, and providing a conservative safety design basis for the preferred design concept. The SDS is prepared by the SDIT (or by the Project Safety Lead in the absence of an SDIT) based on written DOE safety expectations. It is approved by the DOE Safety Basis Approval Authority and by the FPD.

Once a preferred alternative has been selected, the identification of necessary SSCs begins. Safety design requirements are found in DOE O 420.1C, Chg. 1. The focus of safety work at this stage is to: (1) establish and document a preliminary inventory of hazardous materials; (2) establish and document the preliminary hazard categorization of the facility; (3) identify and analyze (as needed) primary facility hazards and facility-level accidents, and (4) provide an initial determination, based on the Hazards Analysis, of safety class and safety significant SSCs.

Figure A.4.1-2: Conceptual Design Phase – Selection of Preferred Alternative



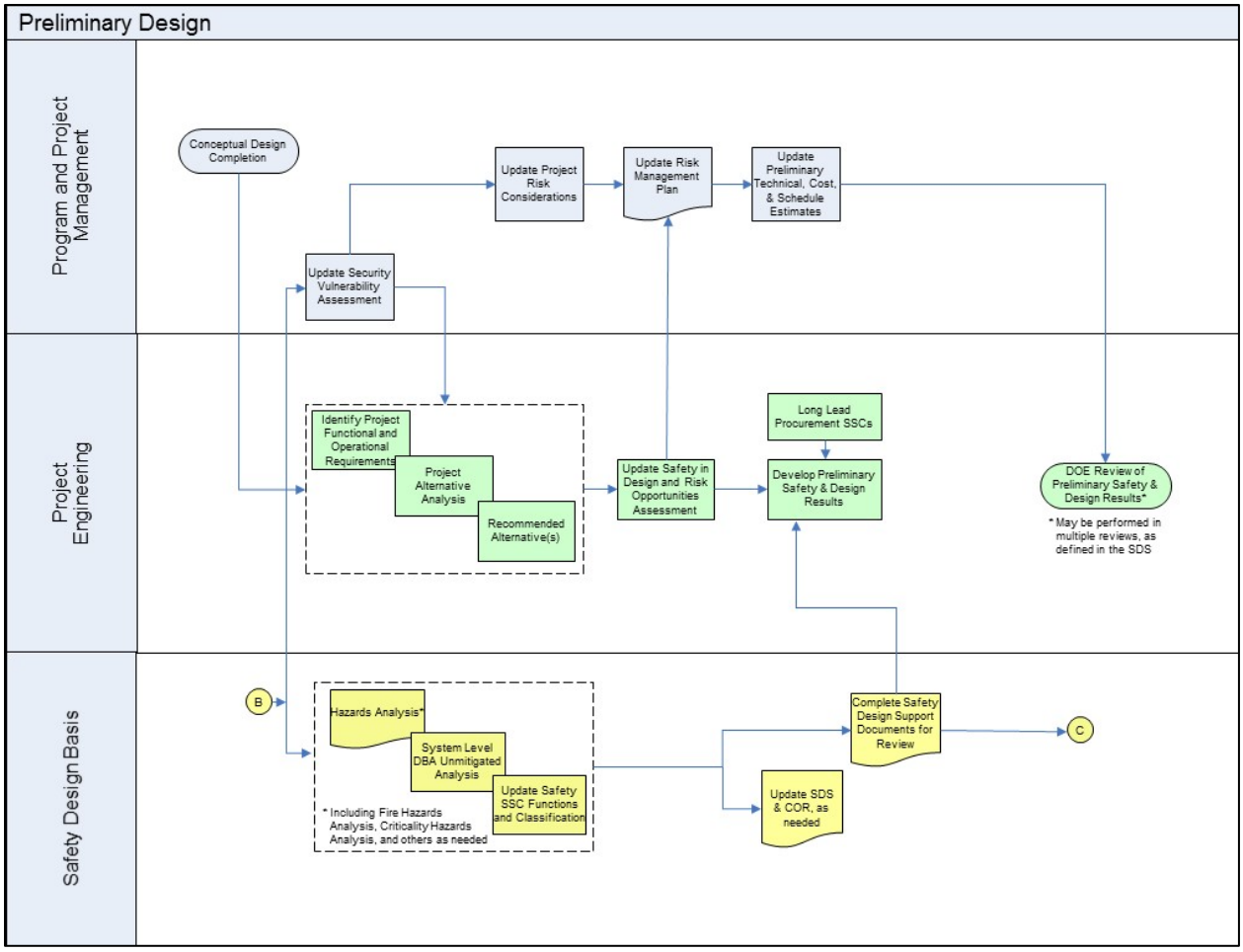
1. Acronyms: Code of Record (COR); Conceptual Design Report (CDR); National Environmental Policy Act (NEPA); Safety Design Strategy (SDS); Design Basis Accident (DBA); Conceptual Safety Design Report (CSDR)

A.4.3 Preliminary and Final Design Phase

The preliminary design phase is devoted to a more rigorous evaluation of the conceptual design. The hazards analysis evolves from a facility-level analysis to a system-level analysis as more design detail becomes available. As it is refined, the selection of controls, safety functions, and SSC classifications made during the conceptual design phase will be revisited. 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.

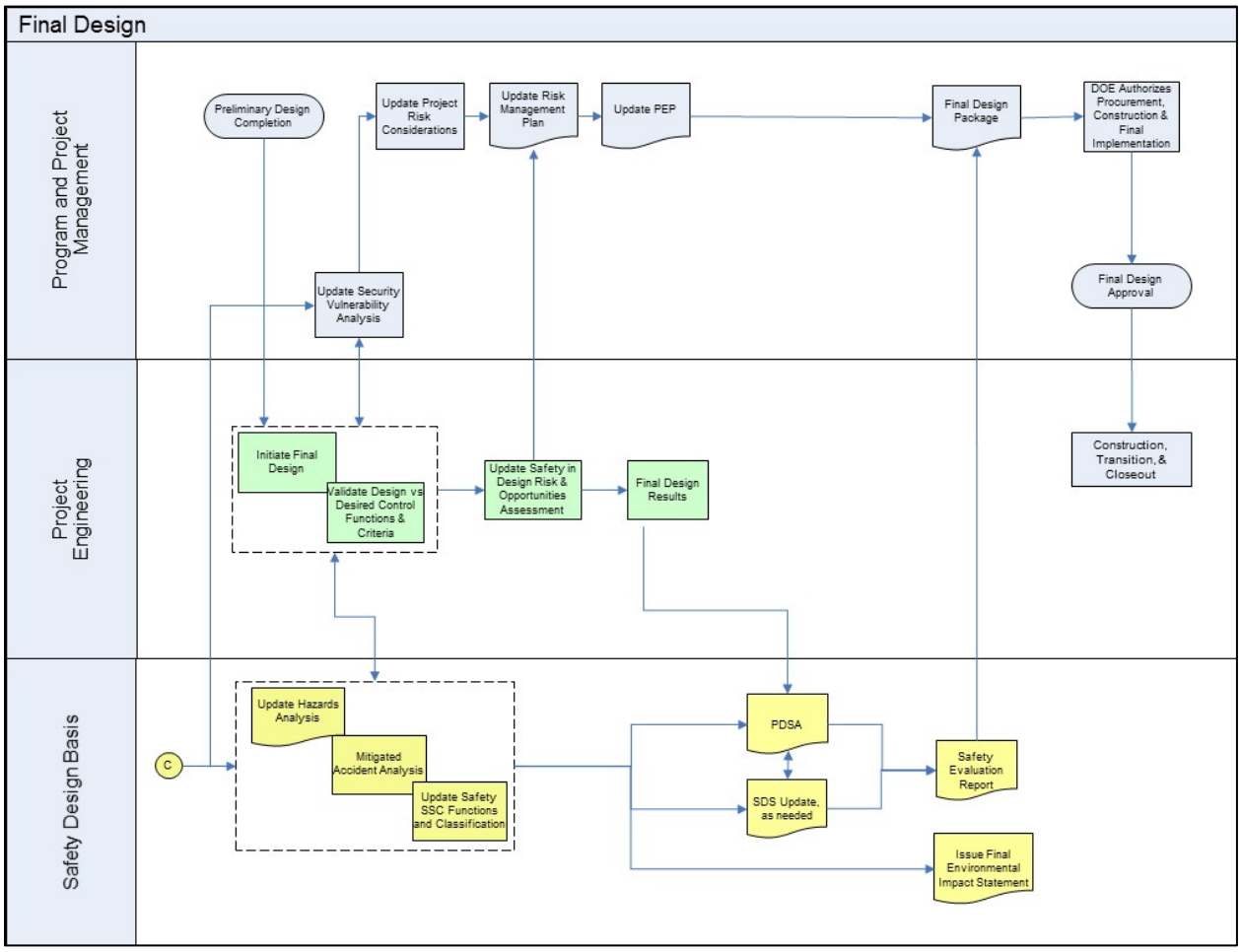
Decisions made during the preliminary design phase provide the basis for detailed design and construction. Major course changes after this phase can have significant impacts on overall project cost and schedule. Hence, all relevant contractor and DOE safety personnel will participate in design reviews. The approach for demonstrating how the preliminary design will satisfy the nuclear safety design criteria of DOE O 420.1C, Chg. 1, should be developed during this phase. (See Figures A.4.1-3 and A.4.1-4 below.)

Figure A.4.1-3: Preliminary Design Phase



1. Acronyms: Structures, Systems, and Components (SSCs)

Figure A.4.1-4: Final Design Phase (CD-2)



1. Acronyms: Project Execution Plan (PEP); Preliminary Documented Safety Analysis (PDSA)

A.4.4 Construction, Transition, and Closeout

During construction, the CM plan ensures that any change to the approved final design is fully evaluated for its impact on the safety design basis. The final Documented Safety Analyses (DSAs), including the Technical Safety Requirements (TSRs) are developed based on the approved final design and any changes made during the construction process. The DSA is completed when it can be confirmed that facility configuration matches the design documentation, safety design basis documentation, and the operating procedures for that configuration.

APPENDIX B SAFETY DESIGN STRATEGY

B.1 OVERVIEW AND PURPOSE

The Safety Design Strategy (SDS) is a tool to guide project design, document safety planning, and provide approving authorities sufficient information on which to make decisions. It provides a single source for the safety policies, philosophies, major safety and security requirements, and safety goals for the project. The SDS describes the major hazards anticipated in the facility and how those hazards will be addressed employing SSCs. Any risks associated with the use of new technology or unproved assumptions should be identified. In addition, the SDS identifies major safety documentation deliverables to be provided within each project phase.

The SDS is used to (a) guide project safety and design integration, document safety documentation development planning, (b) provide approving authorities sufficient information on which to make decisions, (c) document and gain approval on alternative approaches to providing required safety documents, such as the Conceptual Safety Design Report (CSDR) or Preliminary Documented Safety Analysis (PDSA), (d) establish expectations for major modifications where the PDSA may only contain limited information beyond what is already captured in the approved Documented Safety Analysis (DSA) for the facility, and (e) describe any graded approach used and its basis.

B.2 EARLY STAGES OF THE PROJECT

The SDS provides the preliminary information to gauge the scope of significant hazards and the general strategy for addressing those hazards. DOE's expectations for safety-in-design are developed in support of mission need. An initial SDS is prepared at the conceptual design stage. The SDS is then updated if any of the major safety decisions related to project cost or safety risk are changed or as needed for each succeeding phase through project completion.

Early in project planning and design, the SDS identifies the required hazards analysis effort and supports the safety basis documents to be developed. For certain projects, safety assumptions and criteria may be known when DOE approves the mission need or major modification at the beginning of conceptual design. These assumptions and criteria will be in the SDS and used for developing the conceptual design and CSDR.

System Design Descriptions (SDDs) should also be initiated early in the design process. The content of SDDs is set forth in DOE-STD-3024-2011, *Content of System Design Descriptions*.

B.3 FINAL DESIGN AND BEYOND

As the project moves from preliminary design into final design, significant design effort may still be needed to complete the design. At this stage, the SDS lays out the safety-in-design elements required for the completion of the project, to assure successful implementation of the decisions made up to that point in the project. At the construction stage, the SDS may require updating if significant changes to the safety design are made.

B.4 FORMAT AND CONTENT

Section 1: Introduction

This section introduces the SDS for the project. It describes the technical scope of the document and outlines how the material will be presented.

Section 2: 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. Details may include mission, proposed locations, description of major facilities/processes or changes to existing facilities/ processes, and major hazards. Aspects that may be relevant to the overall safety strategy, such as storage capabilities of hazardous materials, waste streams and processes, and support systems, are also covered. Reference to other controlled project documents for detailed information is appropriate.

Section 3: Process Assumptions

This section provides a listing of major process assumptions that are critical to design and the safety design basis. This section addresses:

- The process used to (1) establish the design criteria, the design functional requirements, and design basis, (2) integrate design criteria, requirements, and basis, and (3) mature the design criteria, requirements, and basis throughout the design process.
- The approach to developing the overall safety basis for the project, including the types of analyses to be conducted, documents to be developed through the project cycle, and tailoring approaches selected.
- Key safety documents to be used during the design development phase, to support design development activities and to document the Preliminary Safety and Design Results.
- Transition from preliminary design to final design, including identification of any hold points on design activities until DOE review of Preliminary Safety and Design Results is complete.
- The QA plan and implementation strategy.
- The Configuration Management (CM) plan and implementation strategy.
- For Major Modifications, the interface with the existing facility's safety basis and operations.
- Commitments and requirements developed by the various design disciplines such as structural and electrical.

Section 4: Safety System Support Interfaces

This section provides a listing of major facility or major modification interfaces that are critical to design and the safety design basis. The list includes support and infrastructure systems required for safety system operation.

Section 5: Safety Strategy

This section, the technical core of the SDS, presents the overall safety strategy for the project, including the following:

- The guiding philosophies or assumptions to be used to develop the design, including significant inputs and assumptions, potential impacts of new technology, and project constraints as they might affect safety design decisions.
- The safety-in-design and safety goal considerations for the project, including such matters as hazardous materials associated with the facility, preliminary hazard categorization, commitment to DOE O 420.1C, Chg. 1, and its design requirements; or approved exemptions and equivalencies.
- Air Dispersion Modeling Protocol if used. (See Section 3.2.4.2 of DOE-STD-3009-2014.)
- The need for a design upgrade analysis for major modification projects (Section 5.4 and Appendix G).

Section 6: Safety Guidance and Requirements

This section identifies the safety design criteria to be applied to the project. Applicable rules, orders, standards, guides, handbooks, and consensus codes are listed. Reference to a controlled project requirements document is an acceptable approach. A commitment to the DOE O 420.1C design requirements or alternatives for DOE approval is needed in this section.

Section 7: Hazard Identification

This section discusses the major hazards inherent in the project and the possible risks those hazards may pose. While all hazards should be addressed, special emphasis is placed on hazards that could require the use of safety class or safety significant controls.

Section 8: Key Safety Decisions

This section identifies and describes key safety decisions that have significant cost and schedule implications for the project. Examples are:

- Hazard minimization and use of inherently safe designs;
- Seismic and other natural phenomena design categorization;
- Criticality accident prevention strategy;
- Confinement strategy; and
- Fire prevention and mitigation strategy.

Section 9: Risks and Opportunities - Project Safety Decisions

This section describes risks and opportunities connected to major safety strategy decisions. Factors that relate to these risks and opportunities, such as an application of new technology, are identified. New and non-standard methods, and the associated risks in using these methods, should be clearly identified.

Section 10: Safety Analysis Approach and Plan

This section describes the safety analysis process and deliverables planned for the project. This section describes whether and when preliminary TSRs will be developed and provided for review. Deliverables expected to be completed, submitted, and approved are described for all project phases (and correlated to the project's Critical Decision milestones). Integration with other safety discipline efforts is pertinent to describing the project interfaces and synergy. Tailored project approaches are specifically identified.

Safety design basis development are described sufficiently to facilitate concurrence by approving authorities. The specific safe harbor methodology (e.g., DOE-STD-3009-2014) is identified. Any tailoring approaches selected for satisfying the DOE O 413.3B requirements for safety documentation are described. The required safety documents summarized in Table 4-1 for each design phase are developed for all new and major modifications to existing Hazard Category 1, 2, and 3 nuclear facilities, except in instances where a tailoring strategy is outlined in the SDS and approved by the Safety Basis Approval Authority and FPD.

Section 11: Safety Design Integration Team (SDIT) – Interfaces and Integration

This section describes the strategy for establishing and implementing an SDIT within the project. The discussion addresses the primary interfaces within the project team that are specifically aimed at facilitating coordination of design functions.

APPENDIX C CONCEPTUAL SAFETY DESIGN REPORT

C.1 INTRODUCTION

DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, requires a Conceptual Safety Design Report (CSDR) as a part of the approval package for conceptual design for the preferred alternative. 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 CSDR includes the following:

- Preliminary hazard categorization (HC-1, 2, or 3) of the facility;
- Preliminary identification of facility design basis accidents (DBAs);
- Assessment of the need for safety class and safety significant facility-level hazard controls based on hazards analyses and accident analyses;
- Preliminary assessment of the appropriate natural phenomena hazards (NPH) design basis (e.g., seismic design category and limit state) for the facility structure and major hazard controls; and
- Positions taken with respect to compliance with the safety design criteria of DOE O 420.1C, Chg. 1, *Facility Safety*, or approved exemptions and equivalencies.

The CSDR follows the guidance similar to that for the Documented Safety Analysis (DSA) provided in DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*, as appropriate. Since the CSDR is prepared using preliminary information and assumptions, it provides additional supporting information in support of the preferred alternative. This additional supporting information is generally not carried through in the Preliminary Documented Safety Analysis (PDSA) for the final design.

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 subject matter experts (SMEs) who will be responsible for safety review for the project.

However, part of the CSDR review should assess the implementation of the principles of the hierarchy of 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 major safety systems selected provide an adequate basis for proceeding to the preliminary design stage.

DOE's review of the CSDR confirms that the preliminary safety positions adopted during conceptual design constitute an appropriately conservative basis to proceed to preliminary design.

C.2 RISK AND OPPORTUNITY ASSESSMENT

The Risk and Opportunity Assessment (R&OA) 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 strategies for each risk element has bounded the risk for proceeding with the project. The R&OA is essential to enable the project risks to be understood by the project team and by federal project authorization executives.

Projects are required by DOE O 413.3B to prepare Risk Management Plans (RMPs) to define the roadmap to executing the project within a risk and opportunity environment. DOE O 413.3B 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 413.3B expectations.

Developing the R&OA 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 R&OA of the conceptual design package is the foundation for demonstrating the adequacy of the safety design approach documented in the 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 SMEs, 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.

In developing input for the R&OA, all risks that could affect the safety-in-design strategies delineated for HC 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 SDS 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 should 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 413.3B. 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 should be discussed in the CSDR.

Where risks and opportunities are identified, appropriate strategies should 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 C-1 provides examples of factors that may be considered in identifying and developing risks and opportunities.

Table C-1. Sample Considerations for Risk and Opportunity Analysis.

Technology or Initiator	Risk	Opportunity
New Technology (With Alternatives)	• Cost and manpower spent on alternatives • Not making the decision on technology on time • May require specially trained personnel to operate and maintain new technology	• Potential process improvement or safety risk reduction
New Technology (Without Alternatives)	• Performance below expectations • Potential increase in previously undefined failure modes • Rework and redesign, and associated cost and schedule impact • May require specially trained personnel to operate and maintain new technology	• Potential process improvement or safety risk reduction
Large Scale-up of Design Approach from Laboratory to Full-Size	• Performance below expectations • Potential for previously undefined hazards and event scenarios • Rework and redesign, and associated cost and schedule impact	• Cost of building intermediate-size facilities is avoided if scale-up is a success • Programmatic implementation without delay of intermediate-size facilities
Interfaces with processes outside of facility control • Security requirements • Process support systems • Availability of safety-related equipment that can satisfy requirements • Interfaces with existing facility processes or infrastructure	• Potential increase in failure modes • Rework and redesign • Project delays • Increased costs to upgrade existing systems or infrastructure	• May be performed in parallel with project to achieve early implementation
Complex Design, Construction, Operation, and Support Needs	• Potential increase in failure modes • Rework and redesign • Project delays due to increased time and verifications required to achieve facility completion	• If complexity can be managed, the design may prove a safer and cost effective solution to a DOE complex need
Schedule Pressures	• Mitigation of hazards identified late in the project by either design or operations is typically costly, impacts schedules, and is difficult to integrate into the project	• Devote extra time and resources at the alternative selection phase to ensure most practical option is chosen • Address potential issues early to permit efficient project execution

Technology or Initiator	Risk	Opportunity
Unanticipated Safety Concerns by Stakeholders	• Delay in schedule, increases in costs, disputes with oversight bodies over suitable solutions	• Stakeholder interactions and communication early and often in the project minimizes surprises
Front-Loading of Design Conservatism	Extra margins can prove to be excessive at a design stage with increased costs and often cannot be reversed after analysis and design have been completed	Appropriate margins can help overcome unanticipated safety challenges during design
Accident Analysis Methodology for New or Unique Applications	Changes driven by new requirements or by oversight bodies can invalidate parts of the design, leading to higher costs and extended schedule	Use of a conservative analysis approach during conceptual design can accommodate changes in accident analysis without major project impact
Natural Phenomena Hazards (NPH) Design	Use of increased NPH performance parameters increases cost	Careful use of increased NPH performance parameters increases design robustness and may provide for design changes or upgrades later in facility life
Fire Protection Design	Use of safety class/safety significant fire protection systems adds cost and complexity to a design that may later prove unjustified	Use of safety class/safety significant fire protection systems and may provide for design changes or upgrades later in facility life
Unresolved Safety and Design Issues	Schedule and cost delays if action is not taken at the right time	Active management of safety and design issues may provide more efficient project completion

C.3 CSDR FORMAT AND CONTENT GUIDE

Executive Summary

1. INTRODUCTION

a. Facility Background and Mission

Suggested format and content:

- 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 affecting the extent of safety-in-design approaches documented in the CSDR. (Examples: short facility life cycle, anticipated future change in facility mission, approved DOE exemptions.)

b. Site Description

Suggested format and content:

- Provide a description of the facility location, including the physical and institutional boundaries, relationship and interfaces with nearby facilities.
- Provide a description of the facility layout and significant external structure, system, and component (SSC) interfaces (e.g., utility connections) as they pertain to the hazard analysis.
- If multiple sites are under consideration, describe each of them.

2. CONCEPTUAL DESIGN DESCRIPTION

a. Facility Structure

Suggested format and content:

- Provide information necessary to perform facility-level accident analyses.
- Necessary information includes basic floor plans, material-at-risk locations within the structure, general dimensions, and dimensions significant to the hazard analysis activities.
- Supply information to support an overall understanding general arrangement of the facility in relation to hazards analyzed in later sections of the CSDR.

b. Process Description

Suggested format and content:

- Describe the individual processes within the facility to support understanding of postulated facility-level material-at-risk release events and safety-in-design strategies.
- Include details as necessary on: basic process parameters, types and quantities of hazardous materials, energy sources, process equipment, basic flow diagrams, operational considerations, major interfaces, and relationships between SSCs.
- Information is expected only at the level of conceptual design, as described in Section 4.3 of this Standard. The intent is to supply information sufficient to understand facility-level material-at-risk release events.

3. PRELIMINARY HAZARD CATEGORIZATION

a. Hazardous Material Inventories

Suggested format and content:

- 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 hazards analysis.
- The attributes of hazards identified in this section are the basis for subsequent hazard evaluation and accident analysis in future project stages.

The inventory estimate should 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 information should be in sufficient detail to support a facility-level hazards analysis. The hazards analysis can then support the definition of (a) facility-level DBAs or bounding accidents associated with the inventory locations (e.g., tanks, storage, process vessels) and (b) the associated preliminary lists of safety class and safety significant SSCs.

For the purposes of preliminary facility hazard categorization (before final design), the use of Type B containers to exclude material-at-risk 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

Suggested format and content:

- Compare the radionuclide and fissile material inventories with the threshold quantities in Table A.1 of DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23*, and identify the preliminary hazard categorization.
- When segmentation is proposed, identify segment boundaries and hazard inventories and justify the independence of the segments. Also identify the individual segment preliminary hazard categorizations.

As required by 10 CFR §830.202, the preliminary hazard categorization is done in compliance with DOE-STD-1027-92. The information compiled in the preliminary inventory of hazardous materials is used for this purpose. Any issues that are likely to change the final hazard categorization (such as an inconsistency with Table A.1 of DOE-STD-1027-92) should be identified and discussed.

4. DESIGN BASIS ACCIDENTS

a. Facility-Level DBAs

Suggested format and content:

- Provide a summary table identifying postulated hazardous material release events, including events involving risk to both the public and workers. 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 hazards analysis activities.

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

b. Unmitigated Accident Analyses

Suggested format and content for each DBA:

- Identify the release category by individual title, category (e.g., operational, natural phenomena, external) and general type (e.g., fire, explosion).
- Describe the source-term determination for the event category. Discuss all parameters used to derive the source term, including the material-at-risk (as derived from the hazard

identification), the damage ratio and the airborne release fraction. The degree of conservatism in the calculation needs to be consistent with DOE-STD-3009-2014.
- Present the results of the DBA analysis, both to the collocated worker at 100 m and to the public, according to the guidance of DOE-STD-3009-2014.
- Compare the DBA results to guidance for safety system classification and NPH design criteria of DOE-STD-1020-2016 and the criteria for chemical hazards of DOE-STD-3009-2014.

c. Preliminary Selection and Classification of Safety SSCs

Suggested format and content for each DBA:

- Preliminary identification of facility-level safety functions; and, if proposed, the associated safety class and safety significant SSCs and their necessary support systems;
- Requirements for the identified safety functions and, if proposed, for the associated safety SSCs; and
- Applicable structural design basis associated with each system (NPH design criteria).

Based on unmitigated analyses of the facility DBAs, candidate preventive and mitigative safety SSCs can be identified and classified, according to the guidance of DOE-STD-3009-2014.

This section also provides:

- A discussion of safety functions and design criteria for selected safety SSCs; for example, the required safety functions for the confinement ventilation system, fire protection, and electrical power and distribution SSCs.
- 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.

5. SECURITY HAZARDS AND DESIGN IMPLICATIONS

DOE's Order 470 series (Safeguards and Security Program) contains security requirements that may affect the design and safety aspects of some facilities. These directives should be reviewed as part of the design process. This section of the CSDR may have to be classified, in whole or in part. Normally it is possible to describe in general terms the types of conflicts involved and methods of solution employed.

NUCLEAR SAFETY DESIGN CRITERIA

a. Approach for Compliance with Design Criteria

Suggested format and content:

- List applicable nuclear safety design criteria of DOE O 420.1C, Chg. 1, and provide a brief summary of the implementation approach being taken in the project for each design-related criterion. The implementation guides for DOE O 420.1C, Chg. 1, should be consulted in this effort.
- Programmatic criteria are not expected to be discussed.
- Discuss topics such as ALARA[17] and decontamination/decommissioning plans, which will be needed for the final DSA (though not directly related to the conceptual design).

b. Exceptions to Design Criteria

Suggested format and content:

- For any exception to the nuclear safety design criteria in DOE O 420.1C, Chg. 1, provide and justify the project's alternative criterion.

6. OTHER CONSIDERATIONS

a. Planned Studies or Analyses

Suggested format and content:

- Describe technical studies essential for development or validation of the safety design basis.
- These studies may be necessary to confirm key assumptions or process component equipment selections.

[17] ALARA: "as low as reasonably achievable."

b. Safety-in-Design Risks and Opportunities

Suggested format and content:

- Summarize the safety-in-design risks and opportunities. This summary should 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/detection;
- Confinement ventilation;
- Emergency power;
- Nuclear criticality design features and alarms;
- NPH design (e.g., 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 D PRELIMINARY DOCUMENTED SAFETY ANALYSIS

D.1 TECHNICAL CONTENT

The Preliminary Documented Safety Analysis (PDSA) is the key safety document developed, updated, and maintained while the design progresses from preliminary to final design phase. The PDSA should update the information in the Conceptual Safety Design Report (CSDR).

The PDSA addresses the following safety-in-design aspects for the final design phase:

- Site information of the type that can affect safety-in-design, such as location of nearby facilities and external hazards, meteorological information for dispersion analyses, and natural phenomena data (e.g., seismic, wind);
- Facility and process descriptions (including facility structure types and layout), process descriptions and flow sheets, and summary system descriptions for safety structures, systems, and components (SSCs), consistent with the level of design;
- Summary of the hazards analysis, accident analysis, and fire hazards analysis (FHA);
- Functional requirements, performance criteria, and performance evaluation for safety class and safety significant SSCs and specific administrative controls (SACs);
- Measures to prevent inadvertent criticality accidents;
- Design aspects affecting implementation of safety management plans (SMPs,); and
- How the safety design criteria of DOE O 420.1C, Chg. 1, *Facility Safety*, are met, including any proposed exemptions or alternate approaches.

The PDSA demonstrates the adequacy of the design from the safety perspective. Demonstrating safety design adequacy for final design is focused on demonstrating that the safety design requirements specified at the end of final 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 Documented Safety Analysis (DSA) is developed for the transition to operation.

The PDSA follows the same formatting and guidance as that for the DSA cited in DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*. If a different safe harbor is applicable to the project or modification; or a graded approach for the PDSA is used (e.g., for major modification project), the Safety Design Strategy (SDS) should establish the expectation, and the format of the PDSA as appropriate.

At the completion of final design phase, the PDSA is released for DOE review and approval to

support construction.

D.2 PDSA FORMAT

The format of the PDSA should be consistent with DOE-STD-3009-2014.

D.3 DEVELOPMENT OF PDSA

The PDSA is developed from the Preliminary Safety and Design Results. The following table shows a mapping from the Preliminary Safety and Design Results to the PDSA contents.

Table D-1. Development of PDSA.

Preliminary Safety and Design Results (Section 4.4.5)	STD 3009-2014 DSA Format
• **Site Description.** - Site information of the type that can affect safety-in-design, such as location of nearby facilities and external hazards, meteorological information for dispersion analyses, and natural phenomena (e.g., seismic, wind) data.	**Ch 1: Site Characteristics**: 1.1 Introduction 1.2 Requirements 1.3 Site Description 1.4 Environmental Description 1.5 Natural Event Accident Initiators 1.6 Man-made External Accident Initiators 1.7 Nearby Facilities 1.8 Validity of Existing Environmental Analyses
• **Facility Description.** - Facility structure type and layout; - Process descriptions (includes details on basic process parameters, hazardous materials, process equipment in sufficient detail to support accident assessment and the safety analysis); - Confinement systems; and - Other major systems and support systems.	**Ch 2: Facility Description** 2.1 Introduction 2.2 Requirements 2.3 Facility Overview 2.4 Facility Structure 2.5 Process Description 2.6 Confinement Systems 2.7 Safety Support Systems 2.8 Utility Distribution Systems 2.9 Auxiliary Systems and Support Facilities
• **Hazard and Accident Analysis.** - Summary of facility-level hazards and accidents analyses, hazard categorization, and results of hazards evaluation; - Hazard evaluation tables or data sheets for each hazard scenario, describing: brief unmitigated hazard scenario description and assumptions; likelihood of the hazard scenario; consequences of the hazard scenario; safety functions and preventive features; mitigated consequences; available controls; - PHA; and	**Ch 3: Hazard and Accident Analysis, and Control Selection** 3.1 Introduction 3.2 Requirements 3.3 Hazard Analysis 3.4 Accident Analysis 3.5 BDBAs and BEBAs 3.6 Planned Design and Operational Safety Improvements

Preliminary Safety and Design Results (Section 4.4.5)	STD 3009-2014 DSA Format
- FHA.	
• **Description of Safety SSCs and SACs.** - Control description with safety function and its relationship to the hazard and accident analysis, - Functional requirements, and - Performance criteria judged to require TSR coverage.	**Ch 4: Safety Structures, Systems, and Components** 4.1 Introduction 4.2 Requirements 4.3 Safety Class SSCs 4.4 Safety Significant SSCs 4.5 Specific Administrative Controls (SACs)
• Development of preliminary TSRs.	Ch 5: Derivation of Technical Safety Requirements
	Ch 6: Prevention of Inadvertent Criticality
	Ch 7: Safety Management Programs
• **Summary of Key Design Activities.** - Description of any remaining Technology Readiness Level (TRL) activities; and - Description of any other studies needed to address specific details of the design, such as validation of key assumptions, equipment section, and design optimization	

D.4 GRADED APPROACH TO PDSA DEVELOPMENT

A graded approach to PDSA development is intended to ensure that the PDSA is sufficient for the needs of the project without providing unnecessary information or analyses. As stated in 10 CFR §830.3, the graded approach adjusts the magnitude of the preparation effort to the characteristics of the subject facility based on:

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

APPENDIX E SAFETY PROGRAMS AND OTHER IMPORTANT PROJECT INTERFACES

As stated in Section 4.8 of this Standard, a project or facility depends on full implementation of safety management programs (SMPs) and evaluation of project interfaces. The safety-in-design process identifies instances where credit is taken for the availability and capability of SMPs and for design interfaces. The basis for taking credit in these situations should be documented in the Preliminary Documented Safety Analysis (PDSA) and ultimately in the Documented Safety Analysis (DSA). This appendix highlights those interfacing SMPs that will be addressed in Chapter 7 of the DSA and other project interfaces that should be accounted for during design development activities.

For new facilities to be built at existing DOE sites where SMPs have already been established, much of the interface with the DSA may be similar to that for existing facilities. Exceptions may occur where new classes of hazards or control approaches are introduced. The existing program is assessed against the proposed design and control requirements from the new design to assure that the design and potentially modified SMPs are in alignment.

For new sites, however, the development of SMPs should be a focus of management attention early in the project life cycle. These programs mature as the facility heads toward operational capability. In addition to SMPs, other design interfaces such the worker safety and health program (mandated by 10 CFR Part 851, *Worker Safety and Health Program*) need to be evaluated for potential impact on the facility design. These interfaces will be implemented during facility design development phases.

Further discussion of these interfaces is provided below.

E.1 RADIATION PROTECTION

Radiological controls to achieve "As Low as Reasonably Achievable" (ALARA) worker doses represent a fundamental design philosophy required by 10 CFR Part 835, *Design and Control and Facility Design and Modifications*. Subpart K of 10 CFR Part 835, provides key inputs into the design process. DOE O 458.1 Admin Chg 3, *Radiation Protection of the Public and the Environment*, and DOE G 441.1-1C, *Radiation Protection Programs Guide for Use with Title 10, Code of Federal Regulations, Part 835, Occupational Radiation Protection*, provide additional guidance for design.

Radiological hazards will generally be mitigated by the use of confinement or shielding strategies to minimize worker exposure. These strategies will evolve to design requirements through the project life cycle. It is often beneficial in projects with significant shielding needs to establish ALARA design goals along with the ALARA strategy for areas where workers could be present. This guides design of the shielding as well as providing input to potential operational restrictions. In addition, detection or monitoring equipment is generally required to protect workers, the public, and the environment.

E.2 FIRE PROTECTION

The site fire protection program plays an important role in facility safety design. At an early design phase, fire protection SMEs and safety analysts should work together to evaluate fire hazards and scenarios that will drive safety functional classification of fire protection structures, systems, and components (SSCs). The design is developed using a complete and technically-supported Fire Hazards Analysis (FHA).

Fire protection SSCs can represent a significant cost to the overall project and present special interface challenges between fire protection subject matter experts (SMEs), design, and safety analysis disciplines. Hence, a full understanding of the implications of fire protection SSC and specific administrative control (SAC) selection, along with any credit taken for the site's fire protection SMP, is necessary to effectively implement such a strategy during detailed design.

The FHA and its conclusions should be addressed in the facility Conceptual Safety Design Report (CSDR) and PDSA in a manner that reflects all relevant fire safety objectives that could affect the facility safety basis.

DOE-STD-1066-2016, *Fire Protection,* provides requirements and guidance applicable to the design process.

E.3 MAINTENANCE

The maintenance functional area, a part of site SMPs, involves significant interfaces with other functional areas as well as with the processes for identification of facility material deficiencies. Maintenance program includes monitoring and maintenance of SSCs to support safe and reliable facility operations. At an early design phase, the design organization should coordinate with SMEs from operation and maintenance and address design features that are essential for reliable and efficient maintenance and operations. Unique design features for maintaining the reliability of safety SSCs should be documented in the DSA.

E.4 PROCEDURES, TRAINING, AND QUALIFICATION

Safety-in-design objectives can only be achieved through safe operation of the facility, which requires trained operators and well-documented procedures. 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 Technical Safety Requirements (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 SACs, 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 should be incorporated into the procedures and training programs. 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.

E.5 CONDUCT OF OPERATIONS

The purpose of a conduct of operations program is to ensure that management systems are designed to anticipate and mitigate the consequences of human failures. The program provides detailed performance expectations and requirements for procedure administration and compliance, communications, training, and facility operations. Conduct of operations input to the conceptual, preliminary, and final design process is primarily addressed by having SME support for the design team. The primary source for the requirements applicable to this functional area is DOE O 422.1, Chg. 2, *Conduct of Operations*.

E.6 QUALITY ASSURANCE

An effective Quality Assurance (QA) program can greatly strengthen the ability to achieve the goals of safety-in-design, by identifying problems early in the design when it is most cost-effective to make corrections. For nuclear facilities, the Quality Assurance Program (QAP) is mandated by 10 CFR Part 830. Detailed program requirements are found in DOE O 414.1D, *Quality Assurance*.

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;
- 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, including procurement of safety SSCs;
- 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;
- Establishing Commercial Grade Dedication for the safety SSCs, if necessary;
- 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; and
- Periodically meeting with vendors to ensure safety components can in fact be constructed and function consistent with design specifications without unconsidered exceptions.

The project's 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.

E.7 EMERGENCY PREPAREDNESS

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.

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. EMP SMEs and project safety analysts should work together to define and analyze these scenarios.

Useful references for this topic are DOE O 151.1C, *Comprehensive Emergency Management System*, DOE-HDBK-1163-2003, *Integration of Multiple Hazard Analysis Requirements and Activities*, 40 CFR Part 68, *Chemical Accident Prevention Provisions*, and 29 CFR §1910.19, *Special Provisions for Air Contaminants*.

E.8 WASTE MANAGEMENT

Facility process systems should be designed to minimize (a) waste production, (b) the quantity of toxic and hazardous chemicals and material acquired, used, or disposed of, and (c) mixing of radioactive and non-radioactive 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) should be examined to reduce management costs of these waste streams. Management strategies for these waste streams including storage and treatment and disposal systems are 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.

DOE O 435.1, Chg. 1, *Radioactive Waste Management*, provides additional information and acceptable methods for meeting the requirements. Other methods may be used but should ensure an adequate level of safety commensurate with the hazards associated with the work and be consistent with the radioactive waste management basis. Applicable requirements from Federal and State regulations may also apply (for example, RCRA, CERCLA, CAA) which may be presented in the Environmental Protection section of the DSA.

E.9 WORKER SAFETY AND HEALTH PROGRAM

DOE's rule-governed worker safety and health program appears in 10 CFR Part 851. The objectives of this rule are to:

- 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 (a) all applicable requirements of this rule; and (b) with the worker safety and health program for that workplace.

Two areas of this rule of particular relevance to safety-in-design are fire protection and pressure safety. The rule invokes National Fire Protection Association code requirements for fire protection and the American Society of Mechanical Engineers' Boiler and Pressure Vessel code for pressure safety.

Applicability of worker safety 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 the Hazardous Materials Program, Occupational Safety (which includes fire protection), Emergency Preparedness, Management, Organization, and Industrial Safety.

E.10 INFRASTRUCTURE

Infrastructure needs and existing capabilities or constraints should be identified 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,
- Interfacing facility (modifications), and
- SMPs.

Of particular interest is the identification of any constraints that may hinder project planning and execution. Equipment compatibility constraints can arise when interfaces with an aged infrastructure are required. 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. A commonly-encountered issue is the ability of the existing water supply to support 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 (such as toxic or explosive gases) to 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 PDSA.

E.11 HUMAN FACTORS

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.

In the context of safety bases development, human factors consist of the following:

- Designing facilities, systems, equipment, and tools so they are sensitive to the capabilities, limitations, and needs of humans;
- Ensuring that an operator can perform the items required under a SAC in the timeframes assumed in the safety analysis; and
- Human reliability analyses that quantify the contribution of human error to the facility risk.

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

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.

E.12 SECURITY

Some measure of physical security is needed for most DOE facilities. In certain cases, however, security needs may have a substantial impact on the design and the ultimate cost of the project.

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 should be coordinated

with the design as it relates to safety in a two 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 accidents, 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 ought to 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 ought to 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.

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 ought to 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, a Vulnerability Assessment, and participation in the hazard analysis effort.

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.

E.13 ENVIRONMENTAL PROTECTION

In accordance with DOE O 413.3B, the National Environmental Policy Act (NEPA) strategy and analysis are prepared during conceptual design. Final NEPA documents, including a Record of Decision or Finding of No Significant Impact, need to be issued prior start of final design. The design organization should coordinate with DOE's 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.

The design organization 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. Other requirements (relating, for example, to protection of endangered species, and protection of historic and cultural resources) 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 436.1, *Departmental Sustainability*, outlines requirements and responsibilities to ensure that DOE carries out its missions in a sustainable manner and achieves the sustainability goals established in its Strategic Sustainability Performance Plan. Among other things, the Order requires that each site develop and commit to implementing an annual Site Sustainability Plan (SSP) that identifies its respective contribution toward meeting the Department's sustainability goals. Under the Order, DOE sites are required to use Environmental Management Systems (EMSs) as a platform for SSP implementation. In conformance with the Order, the environmental aspects of any projects should be reflected in the site's EMS prior to operation.

E.14 HAZARDOUS MATERIAL

The program for hazardous material protection should incorporate the ALARA approach, the elements to provide hazardous material exposure control, and facility protection instrumentation. Decisions made during conceptual and preliminary design can either minimize or exacerbate the risks of handling hazardous material. 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 methods, 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.

Hazardous materials, typically those 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 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-1139-2006, *Chemical Management* (Volume 2 of 3), "Chemical Safety and Lifecycle Management."

E.15 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 (10 CFR Parts 830 and 835). The principal DOE external reviews will cover the CSDR, PDSA, DSA, and TSRs. However, the interaction between DOE and the contractor within the (Federal) Integrated Project Team (IPT) and Safety Design Integration Team (SDIT) maintains an open line of communication so that issues may be raised by stakeholders before or after these formal reviews.

Periodic formal project reviews, particularly those at the major project approval stages, are required by DOE O 413.3B. 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 Facilities Safety Board (DNFSB) evaluates the effectiveness of DOE regulatory oversight activities and the safety of defense nuclear facility design, construction, operations, and decommissioning. The DNFSB has stationed members of its technical staff at a number of DOE's defense nuclear sites. These staff members can, and typically will, participate in reviews of the project at any stage. The DNFSB also conducts its own review of the proposed facility design, including the safety design basis development and construction, when determining the adequacy of nuclear safety approach 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 statutes such as the Resource Conservation and Recovery Act, Clean Air Act, and Clean Water Act. Typically, required 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.

E.16 COGNIZANT SYSTEM ENGINEER PROGRAM

DOE O 420.1C, Chg. 1, requires that Cognizant System Engineers (CSEs) be made responsible for "active safety class and safety significant SSCs as defined in the facility's DOE-approved safety basis documentation, or 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. CSE program requirements are also aimed at supporting operations and maintenance.

In preparation for the operational phase, it will be important to identify CSEs 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. CSEs should be involved in the planning for and conduct of system testing to allow detailed operational understanding. The CSEs 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 CSE preparation will help

facilitate a smooth transition to routine operation and maintenance following approval for operations.

E.17 TRANSPORTATION

The safety-in-design process during the conceptual design phase should consider packaging and transportation requirements. DOE directives in the Order 460 series provide regulatory requirements and guidance for packaging and transportation of hazardous materials. The design organization should consult SMEs to ensure facility design can support the requirements for packaging and transportation.

E.18 CRITICALITY SAFETY

Nuclear criticality safety 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, criticality safety controls can also result in safety significant functional classification of SSCs and, potentially, TSR controls. As a result, the criticality safety function will be represented on the project team and will be closely linked to the safety analysis effort from the earliest stages of project development. Criticality safety evaluations are 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, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Non-Reactor Nuclear Facilities.*

APPENDIX F MAJOR MODIFICATION DETERMINATION EXAMPLES

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 $10M.*		
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?	*No. 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 safety class (SC) or safety significant (SS) safety function or associated structure, system and component (SSC)?	*No. The steam reforming process will be housed in a section of an existing building which has not previously been used. 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?	*Yes. The project will introduce a process which is used 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	Use new technology or Government Furnished Equipment (GFE) not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*Yes. Steam reforming is not new technology and no GFE equipment is used 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, Tennessee and other DOE and commercial locations. Steam reforming is used 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 SSCs?	*Yes. Safety basis controls for the facility will require modification, and this will likely include new or revised safety SSC. However, steam reforming is used 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 Documented Safety Analysis (DSA)?	*Yes. Although steam reforming is used 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: *Four of the six criteria (Criteria 3, 4, 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 a significant impact to the facility safety basis. 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 hazards analysis 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 hazards analysis 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 ≥ HC 3 inventory limits or increase the HC of an existing facility?	*No. The project 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 safety class or safety significant safety function or SSC?	*Yes. 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?	*No. Although the new mixing system could potentially be viewed as new process, for the purposes of this evaluation it is 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	Use new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*Yes. The project will use a mixing technology that has not previously been formally reviewed / approved by DOE for mixing radioactive waste inside of a large radioactive waste tank. However, 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. Full scale mock-up testing performed to date using simulant has yielded promising results. 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 SSCs?	*Yes. The project will require new or revised safety SSCs 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 significant in scope. Due to the complexity of the project, any 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?	*Yes. 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: *Four of the six criteria (criteria 2, 4, 5, and 6) were tripped in this PDSA evaluation. The assessment of each of these four criteria identified a high degree of risk inherent in the application of the new mixing technology as proposed by this project. 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.*		

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 material-at-risk 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?	*No. 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 safety class or safety significant safety function or associated SSC?	*No . 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 safety class or safety significant safety functions or associated SSCs. 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?	*No. 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	Use new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*No. The addition of a new loading dock will not use 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 SSCs?	*No. The addition of a new loading dock does not create the need for new or revised safety SSCs 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?	*No. 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.*		

EXAMPLE 4

Major Modification Evaluation		
Project Information *A proposed project will add a new operation to an existing HC-2 facility to package transuranic (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 hazards analysis (reference), these hazards are well characterized and the associated hazard controls needed are encompassed by the safety SSC and safety management programs (SMPs) 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?	*No. The material to be processed by the new packaging operations is bounded by the material-at-risk 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 safety class or safety significant safety function or associated SSC?	*No. 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 safety significant 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?	*Yes. 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	Use new technology or GFE not currently in use or not previously formally reviewed /approved by DOE for the affected facility?	*Yes. 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 SSCs?	*Yes. 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 SMPs 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?	*Yes. The addition of a new TRU waste processing operation will involve hazards not previously evaluated in the DSA for this facility. However, 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 Unreviewed Safety Question (USQ) determination was positive, indicating that DOE approval is required in revising the existing Safety basis to add the new waste processing operation. Accordingly, the overall determination is that this project is a major modification. The impact of the two "No" answers and other mitigating factors (low project risk and well understood hazards) can be accommodated by use of the graded approach described in Section 5.3 of the Standard.*		

EXAMPLE 5

Major Modification Evaluation		
Project Information *The project will modify the physical plant as process functions are moved from one building to another within the current buildings complex associated with the existing nuclear facility. The project does not result in a change to process functions and associated hazards analyzed for the process operations being relocated. This project should not result in an increase in risk associated with facility operations in a different location. Additionally it does not change the types of controls currently addressed in the Safety Basis. New controls may be added as a result of a new hazard analysis. At a minimum, the project does change the locations (buildings) where activities discussed in the safety basis are performed and would require a description change. Based on this, a determination is warranted.*		
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?	*Yes. The project does not add any new buildings nor does it increase radiological material inventories. Inventories in the existing building will be re-distributed to buildings already present in the facility. The project does re-categorize existing buildings, described in the existing safety basis, from Other Industrial Categorization to HC-2. However, in so doing, existing Building will eventually be downgraded from HC-2 to below HC-3. It is recognized there will be a transition period where radiological inventories will be present in both the recategorized building and the existing HC-2 building. It is also to be recognized additional project activities outside the project will be needed to deactivate the vacated building. However, the sum total of the radiological inventories in both buildings will not increase over that presently analyzed in the safety basis during any time period. The net result is that there is no change in the hazard categorization of the facilities.*
2	Change the footprint of an existing HC 1, 2, or 3 facility with the potential to adversely impact any credited safety function?	*No. The project will not change the footprint of any existing process buildings within the facilities which will adversely affect any SC/SS safety function of associated SSC. The project does recategorize an existing building from less than HC-3 to HC-2. As hazardous operations are moved from the current building to their new location in the other building, SSCs and their associated Safety Function already discussed in the safety basis will be transferred with them. As such, the location where Safety Functions are implemented may change but no new functions are anticipated.*

Major Modification Evaluation		
3	Change an existing process or add a new process resulting in a Safety Basis change requiring DOE approval?	*Yes. The project will not add any new processes. Existing processes and operations will be relocated to other facilities/buildings. As a result, changes will be made to the descriptive material indicating the location where the processes and operations are performed. The project will not change the Safety Functions associated with the processes described in the Safety Basis. While Safety Functions will be moved to new locations, the Safety Functions will not change. A change to the DOE approved Safety basis will be required to reflect the new location of the Safety Functions.*
4	Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	*No. The project will not utilize new technology or GFE. The project will apply proven technologies in process measurement, equipment manipulation, or product testing. These technologies are not expected to impact the overall safety of the facility.*
5	Create the need for new or revised Safety Basis controls (hardware or administrative)?	*Yes. The project will at a minimum duplicate and/or relocate safety SSCs. However it will not change the Safety Function associated with the hazard analysis described in the current Safety Basis. These Safety Functions presently in place will be required in the new location. Additional controls or enhancements to existing controls may be required due to a new hazard analysis and using latest codes and standards. This will be used to minimize the use of administrative controls as a means of performing the Safety Function. As an example, hoods and gloveboxes installed or modified as part of the project will be compliant with NFPA 80l for fire suppression. This allows elimination of Specific Administrative Control (SAC) on combustible materials in the hoods currently implemented because of non-compliance with NFPA 801. As a result a simplified approach to safety will be achieved.*
6	Involve a hazard not previously evaluated in the DSA?	*No. Hazards within the Facilities are analyzed in the current Hazard Analysis. These hazards resulted in events as examined in the DSA including: Fires, Explosion Plus Fire, Explosions, Loss of Confinement, Tornado and High Winds Event, Seismic Event, External Severe Impact, Stack Collapse, and External Fire. The project does not change the processes performed, or the methods in which they are performed. Therefore it is not anticipated any new hazards or events will result.*
Summary and Recommendation: *While the project will result in changes to "where" operations will occur, it will not result in changes to the core Process Operations and Safety Functions of SSCs as approved in the existing safety basis. Descriptive changes will be required in the safety basis to reflect this. Additional controls or enhancements to existing controls may be required due to a new hazard analysis and using the latest codes and standards. However, these changes are not expected to be substantial. The project will not increase the radiological inventories in the Facilities nor will it add any new technologies which could add risk to operations. Many of the current Safety Basis controls associated with the hazards previously analyzed are not expected to change. Safety Basis controls such as Air Monitors, Fire Suppression, Robust Containers, Empty Container Verification, etc. while being implemented in a different area of the facility are expected to be identical. In summary, while the process areas may change no different hazards or types of events are expected to be added by the project. As such the project does not constitute a Major Modification.*		

APPENDIX G ANALYSIS OF POTENTIAL DESIGN UPGRADES

G.1 INTRODUCTION

This Appendix provides guidance on how to analyze whether design upgrades should be undertaken for an existing facility undergoing a major modification. This issue is raised because criteria to be used for the project's safety structures, systems, and components (SSCs) will be based on DOE's orders and standards in effect when conceptual design work is begun, while the existing facility's safety SSCs will have been designed and constructed using criteria in effect years or even decades before. In some cases, conflicts in criteria will be minor and can be shown to have no safety impact.

In other cases (for example, a significant change in the design basis earthquake for the site), the difference has a substantial impact on functional and performance requirements for safety SSCs that will interface when the modification is completed. In these latter cases, the existing facility's safety SSCs may need to be upgraded to meet the functional and performance requirements for the modification project.

G.2 IDENTIFICATION OF DESIGN CRITERIA CONFLICTS

The analysis begins by identifying interfacing safety SSCs. Examples of such SSCs might include structural members, piping systems, electrical systems, ventilation systems, and fire protection systems. For each such interfacing SSC, the project's design organization should (1) research and identify, to the extent possible, the Code of Record (COR),[18] (2) identify the COR that will apply to design of the major modification, and (3) identify the interfacing existing SSC interfaces where a substantial conflict in CORs will likely lead to incompatible designs and inconsistent safety requirements. For each case of item (3), in which the existing safety SSC would not be able to meet the functional and performance characteristics demanded by the COR for the major modification, an analysis of the conflict between the existing and new systems will be needed to achieve a practical, safe design consistent with DOE's safety basis requirements.

G.3 ANALYSIS OF CONFLICTS

The following factors may be used in evaluating the functional and performance gaps for the interfacing existing SSCs of interest, and for identifying alternatives to resolve them:

[18] As defined in Order 413.3B.

- Material condition and maintenance history of the interfacing existing SSCs;
- Potential operational or other benefits in upgrading the interfacing existing SSCs to current criteria;
- Alternative methods such as specific administrative controls (SACs) or safety management programs (SMPs) to achieve an upgrade rather than replacing or modifying existing SSCs;
- Cost of upgrades measured against likely safety and operational benefits;
- Potential cost savings (e.g., reduced maintenance and surveillance) of replacing old equipment with new equipment; and
- Impact of the "hierarchy of controls" on the upgrade decision.

Other factors in addition to those listed may be considered. No specific weight is assigned to the factors listed, as they are interrelated and vary in importance according to the design criteria issue under study. To the extent practicable, quantitative assessments should be made with respect to costs, risks, and schedule impacts.

G.4 REPORT OF ANALYSIS RESULTS

When the analysis described in Section G.3 is completed, and recommended options identified, the results of the study should be inserted in a separate section of the project's SDS document. The following details should be provided:

- General description of the significant COR conflicts between the major modification and the existing facility;
- For each type of conflict, the design and safety criteria that govern the major modification and those that govern the existing facility (if known);
- For each interfacing existing SSC subjected to a gap analysis:
  - technical options considered to resolve the conflict;
  - the preferred technical option, with justification;
  - a cost-benefit analysis of the preferred option; and
  - whether exemptions/equivalencies will be needed to implement the preferred option.

Wherever relevant, the report should describe costs, schedule impacts, and technical feasibility.

APPENDIX H INTERFACE BETWEEN SAFETY-IN-DESIGN AND PROJECT MANAGEMENT

This Appendix expands the flow diagrams in Appendix A of this Standard to show the interface between safety in design and project management activities specified in DOE O 413.3B, Chg. 2, *Program and Project Management for the Acquisition of Capital Assets*. Some terms used in these diagrams are not defined or used in the main text of this Standard. Landscape format is used to improve readability.

Figure H-1 Acronyms: Safety Basis Approval Authority (SBAA); Federal Project Director (FPD); Independent Cost Review (ICR); Project Management Risk Committee (PMRC); Energy Systems Acquisition Advisory Board (ESAAB).

Figure H-2 Acronyms: Integrated Safety Management (ISM); Chief of Nuclear Safety (CNS); Chief of Defense Nuclear Safety (CDNS); Independent Project Review (IPR); Federal Integrated Project Team (IPT); Code of Record (COR); Conceptual Design Report (CDR); National Environmental Policy Act (NEPA); Safety Design Strategy (SDS); Design Basis Accident (DBA); Conceptual Safety Design Report (CSDR).

Figures H-2 and H-3 Note: The DNFSB is presented in this figure for information only (i.e., not a requirement of this Standard) and to illustrate the process DOE and DNFSB use to interface on issue resolution, methods for tracking safety issues, communication protocol, and escalation methods for resolution and closure of safety issues during the Conceptual design phase.

Figure H-3 Acronyms: Technical Independent Review (TIPR); Structures, Systems, and Components (SSCs).

Figure H-4 Acronyms: Project Execution Plan (PEP); Preliminary Documented Safety Analysis (PDSA).

Figure H-1: Pre-conceptual Design (Expanded)

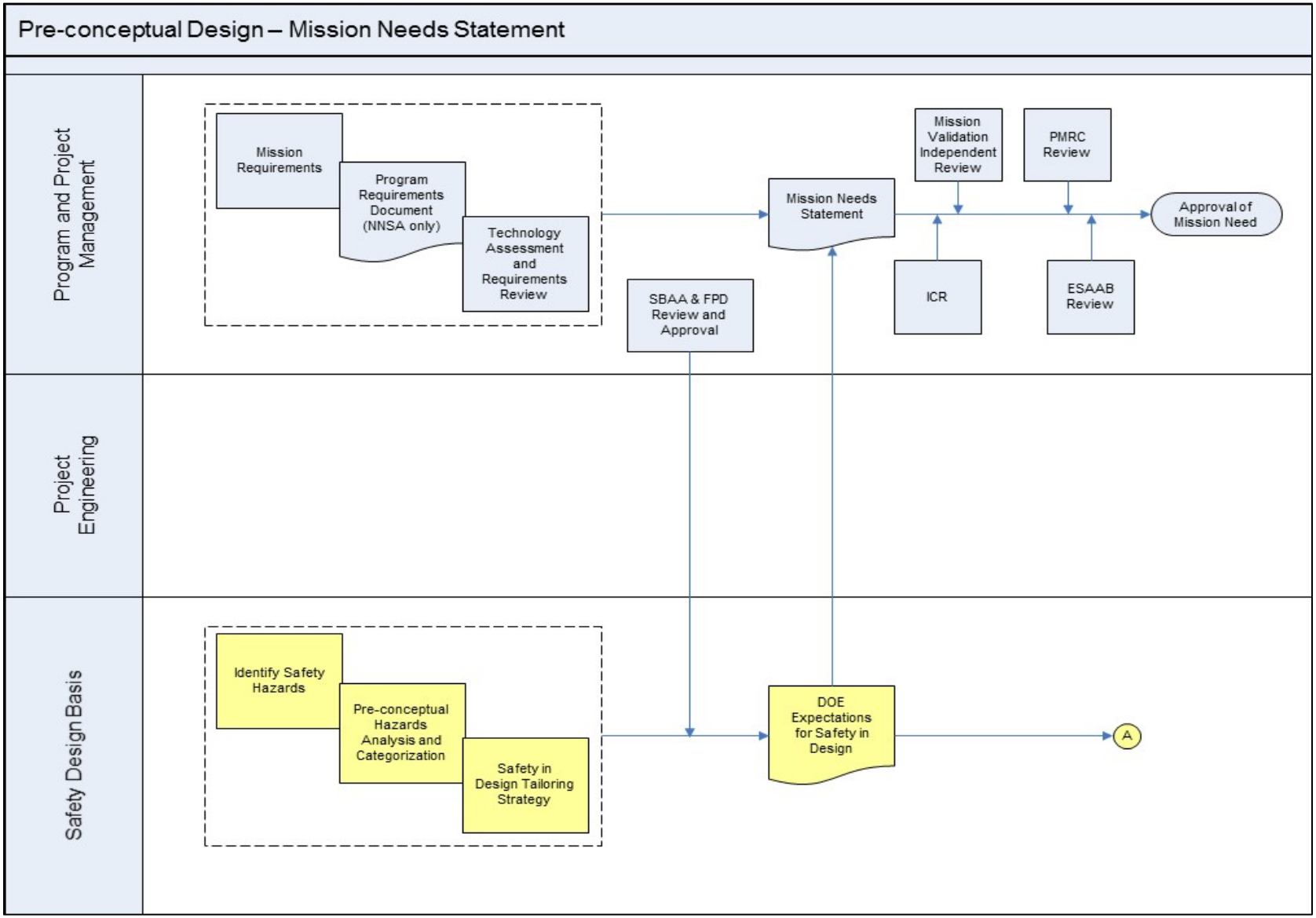


Figure H-2: Conceptual Design (Expanded)

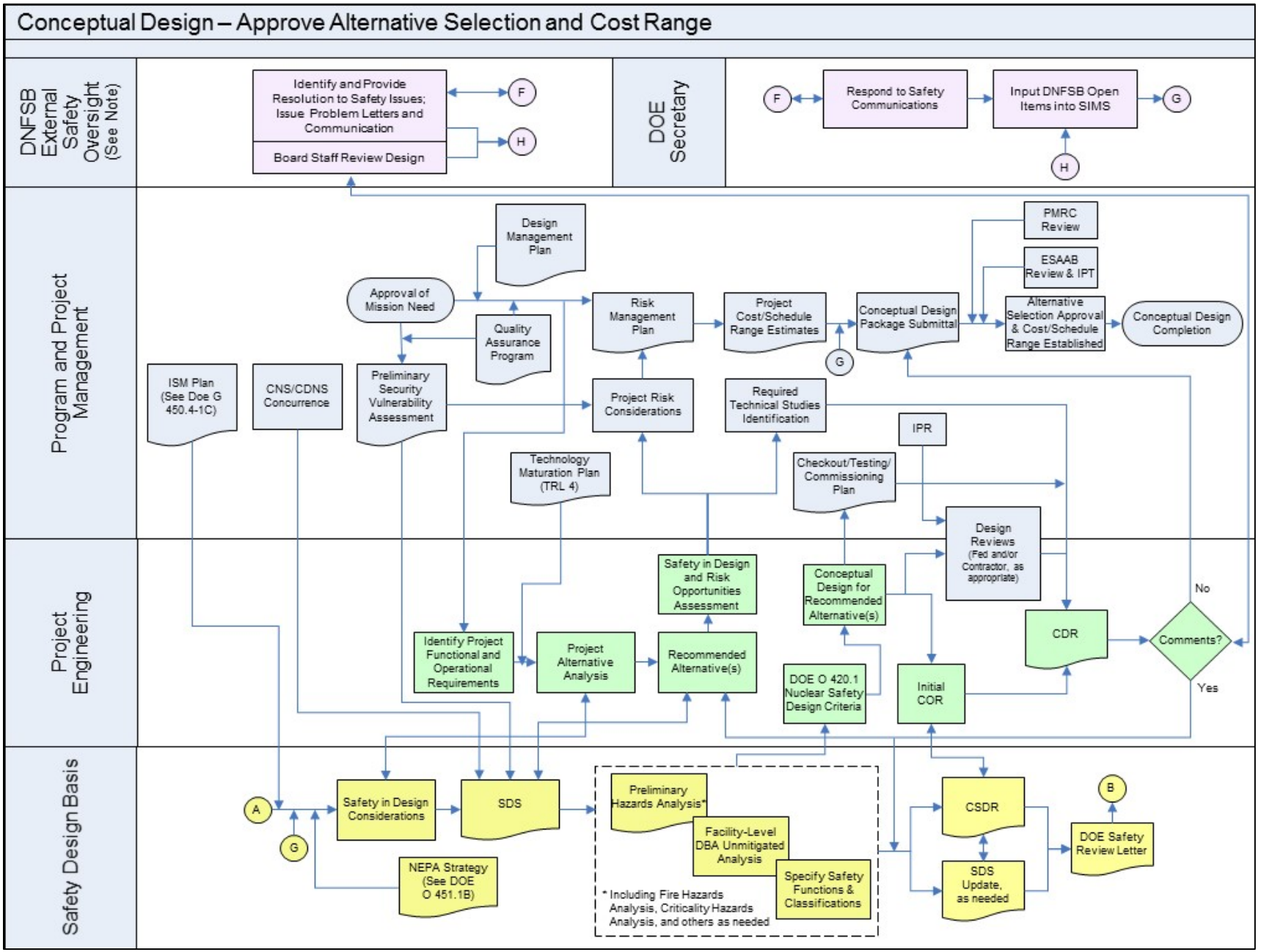

Conceptual Design – Approve Alternative Selection and Cost Range
DNFSB External Safety Oversight (See Note)
Identify and Provide Resolution to Safety Issues; Issue Problem Letters and Communication
Board Staff Review Design
DOE Secretary
Respond to Safety Communications
Input DNFSB Open Items into SIMS
Program and Project Management
Design Management Plan
Approval of Mission Need
Quality Assurance Program
Risk Management Plan
Project Cost/Schedule Range Estimates
Conceptual Design Package Submittal
PMRC Review
ESAAB Review & IPT
Alternative Selection Approval & Cost/Schedule Range Established
Conceptual Design Completion
ISM Plan (See Doe G 450.4-1C)
CNS/CDNS Concurrence
Preliminary Security Vulnerability Assessment
Project Risk Considerations
Required Technical Studies Identification
IPR
Technology Maturation Plan (TRL 4)
Checkout/Testing/ Commissioning Plan
Design Reviews (Fed and/or Contractor, as appropriate)
Project Engineering
Safety in Design and Risk Opportunities Assessment
Conceptual Design for Recommended Alternative(s)
CDR
Comments?
No
Yes
Identify Project Functional and Operational Requirements
Project Alternative Analysis
Recommended Alternative(s)
DOE O 420.1 Nuclear Safety Design Criteria
Initial COR
Safety Design Basis
Safety in Design Considerations
SDS
NEPA Strategy (See DOE O 451.1B)
Preliminary Hazards Analysis*
Facility-Level DBA Unmitigated Analysis
Specify Safety Functions & Classifications
* Including Fire Hazards Analysis, Criticality Hazards Analysis, and others as needed
CSDR
SDS Update, as needed
DOE Safety Review Letter

Figure H-3: Preliminary Design (Expanded)

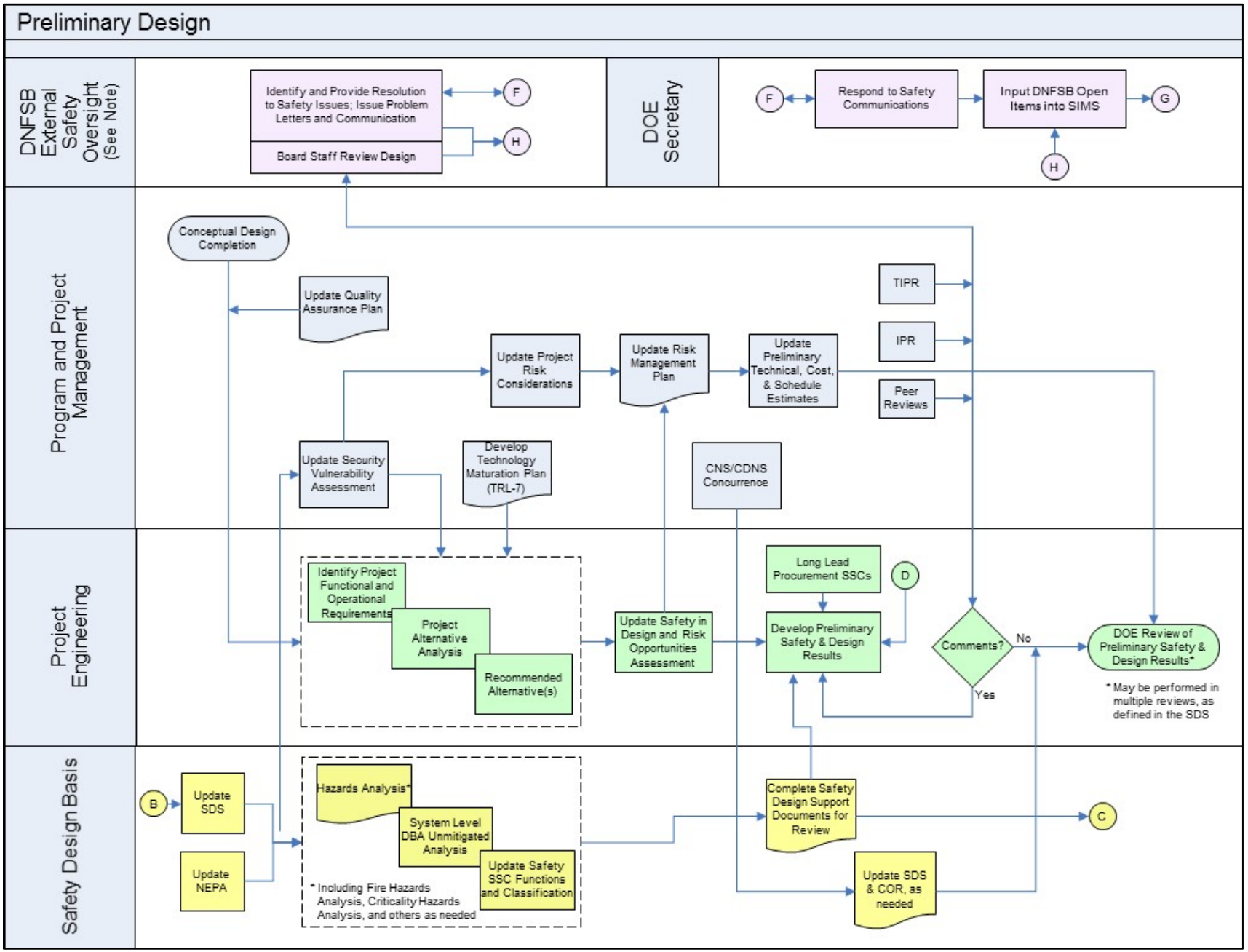
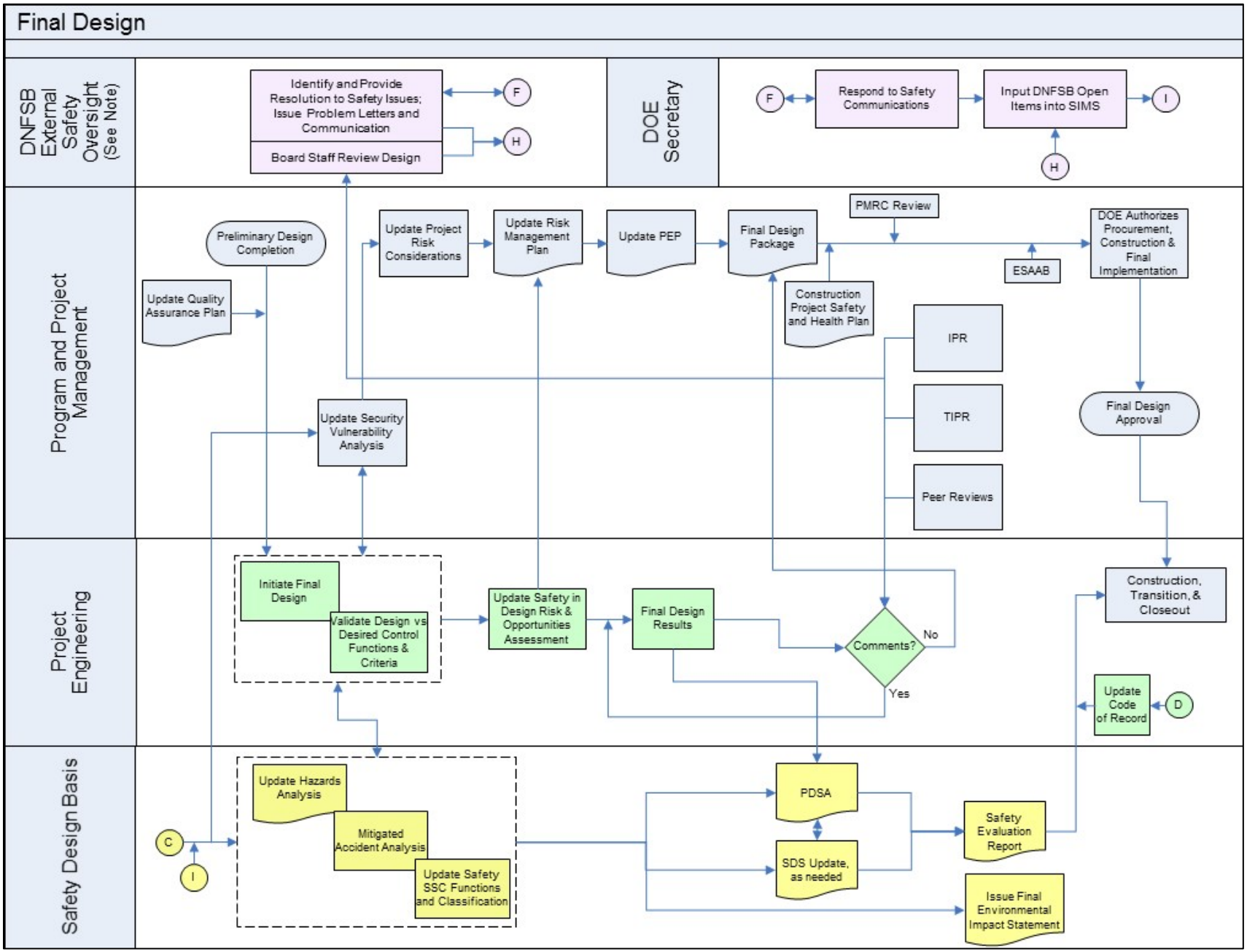

Preliminary Design
DNFSB External Safety Oversight (See Note)
Identify and Provide Resolution to Safety Issues; Issue Problem Letters and Communication
Board Staff Review Design
F
H
DOE Secretary
F
Respond to Safety Communications
Input DNFSB Open Items into SIMS
G
H
Program and Project Management
Conceptual Design Completion
Update Quality Assurance Plan
Update Project Risk Considerations
Update Risk Management Plan
Update Preliminary Technical, Cost, & Schedule Estimates
TIPR
IPR
Peer Reviews
Update Security Vulnerability Assessment
Develop Technology Maturation Plan (TRL-7)
CNS/CDNS Concurrence
Project Engineering
Identify Project Functional and Operational Requirements
Project Alternative Analysis
Recommended Alternative(s)
Update Safety in Design and Risk Opportunities Assessment
Long Lead Procurement SSCs
D
Develop Preliminary Safety & Design Results
Comments?
No
Yes
DOE Review of Preliminary Safety & Design Results*
* May be performed in multiple reviews, as defined in the SDS
Safety Design Basis
B
Update SDS
Update NEPA
Hazards Analysis*
System Level DBA Unmitigated Analysis
Update Safety SSC Functions and Classification
* Including Fire Hazards Analysis, Criticality Hazards Analysis, and others as needed
Complete Safety Design Support Documents for Review
C
Update SDS & COR, as needed

Figure H-4: Final Design (Expanded)


Final Design
DNFSB External Safety Oversight (See Note)
Identify and Provide Resolution to Safety Issues; Issue Problem Letters and Communication
Board Staff Review Design
F
H
DOE Secretary
F
Respond to Safety Communications
Input DNFSB Open Items into SIMS
I
H
Program and Project Management
Preliminary Design Completion
Update Quality Assurance Plan
Update Project Risk Considerations
Update Risk Management Plan
Update PEP
Final Design Package
PMRC Review
ESAAB
DOE Authorizes Procurement, Construction & Final Implementation
Construction Project Safety and Health Plan
IPR
TIPR
Peer Reviews
Update Security Vulnerability Analysis
Final Design Approval
Project Engineering
Initiate Final Design
Validate Design vs Desired Control Functions & Criteria
Update Safety in Design Risk & Opportunities Assessment
Final Design Results
Comments?
No
Yes
Construction, Transition, & Closeout
Update Code of Record
D
Safety Design Basis
C
I
Update Hazards Analysis
Mitigated Accident Analysis
Update Safety SSC Functions and Classification
PDSA
SDS Update, as needed
Safety Evaluation Report
Issue Final Environmental Impact Statement