DOE-STD-1189, *Integration of Safety into the Design Process*

An overview of the REVCOM Draft Standard

Brad Evans, Pacific Northwest National Laboratory

Jerry Bueck, OMICRON/NSTec Nevada Test Site

INFORMATION RELEASE PNNL-SA-55345

Purpose

- This Standard provides the Department's expectations for incorporating safety-in-design into new or major modifications to DOE hazard category 1, 2, and 3 nuclear facilities
- The Standard implements the safety-in-design philosophies listed in DOE Order 413.3A, *Project Management*, and incorporates the facility safety criteria listed in DOE O 420.1B, *Facility Safety*, as a key foundation for safety-in-design determinations.

Purpose (cont'd.)

- The requirements provided in the above DOE Orders and the expectations in this Standard ensure
  - identification of hazards early in the project and
  - the use of an integrated team approach to design safety into the facility.

Applicability

- This Standard applies to the design and construction of the following
  - New DOE hazard category 1, 2, and 3 nuclear facilities;
  - Major modifications to DOE hazard category 1, 2, and 3 nuclear facilities (as defined by 10 CFR Part 830); and
  - Other modifications to DOE hazard category 1, 2, and 3 nuclear facilities managed under the requirements of DOE O 413.3A.

Key Concepts (1 & 2)

- The importance of the Integrated Project Team (IPT), supported by the design contractor, including a Safety Design Integration Team (SDIT).
- The development of a Safety Design Strategy (SDS) that provides a roadmap for addressing important safety issues in the design and in the development of key safety documentation. The SDS should be initiated during the preconceptual design stage and updated and refined through the conceptual design stage.

Key Concepts (3 & 4)

- The development, in the conceptual design stage, of facility-level Design Basis Accidents (DBA) that provide the necessary input to the identification and classification of important safety functions.
- The development of objective radiological criteria for safety and design classification of SSCs. These criteria relate to public and collocated worker safety design considerations.

Key Concepts (5 & 6)

- The identification and application of nuclear safety design criteria as provided by DOE O 420.1B and its associated guides.
- The development of guidance for the preparation of a Conceptual Safety Design Report (CSDR), a Preliminary Safety Design Report (PSDR), and the Preliminary Documented Safety Analysis (PDSA). These reports must be approved by DOE as part of the project approvals to proceed to the next design or construction phase.

Key Concepts (7)

- The definition of a Risk and Opportunities document that recognizes the risks of proceeding at early stages of design (especially conceptual design) on the basis of incomplete knowledge or assumptions regarding safety issues and the opportunities that may arise during preliminary and final design to reduce costs through alternative or refined design concepts or better knowledge regarding the uncertainties.

Guiding Principles (1)

- DOE Order 420.1B, *Facility Safety*, must be utilized and addressed in all design activities. Design teams should be able to clearly articulate strategies in the design that address DOE O 420.1B expectations and include them in the design/safety basis information.

Guiding Principles (2)
Control Selection Strategy

- Control selection strategy to address hazardous material release events should be based on the following at all stages of design development.
  - Minimization of hazardous materials (material at risk) is the first priority.
  - Safety structures, systems, and components (SSC) are preferred over Administrative Controls.
  - Passive SSCs are preferred over active SSCs.

Guiding Principles (2)
Control Selection Strategy (cont'd)

- Preventative controls are preferred over mitigative controls.
- Safety SSCs are preferred over personal protective equipment.
- Controls closest to the hazard may provide protection to the largest population of potential receptors, including workers and the public.
- Controls that are effective for multiple hazards can be resource effective.

Guiding Principles (3 & 4)

- Design standards incorporated into the DOE O 420.1B guides are to be followed unless specific exceptions are taken to the codes listed and approved by DOE.
- The risk and opportunity analysis must include consideration of the safety-in-design approaches selected to address project contingencies and must include appropriate mitigation strategies for the safety-in-design approaches selected.

Guiding Principles (5 & 6)

- Early project decisions on a technical approach should be conservative to establish appropriate cost and schedule baselines for the project.
- The Critical Decision (CD) packages must portray safety-item selections, bases, risks, and opportunities, with proposed mitigation strategies and cost and contingencies, to enable informed risk decision making by the project approval authorities regarding the project technical basis and cost.

Guiding Principles (7 & 8)

- The project team must include appropriate expertise and be established early in the project cycle.
- Safety personnel must be used from the onset of project planning to help ensure that appropriate hazards and techniques for hazard management are considered.

Guiding Principles (9)

- Important safety functions, including facility building confinement, confinement ventilation approach and systems, fire protection strategies and systems, security requirements, life- safety considerations, emergency power systems, and associated seismic design criteria should be addressed as early as possible in the project.

Guiding Principles (10)

- Details may not be available in early project stages to identify all hazards and needed safety controls. The safety design team should strive to ensure sufficient process definition is available, particularly at the conceptual and preliminary design stages, to enable major safety cost drivers to be included in the design documentations along with their associated safety functions and design criteria.

Guiding Principles (11 & 12)

- All stakeholders are important to the process. Stakeholder issues should be identified early and resolved.
- The project is expected to evolve over time, and the project safety basis and design basis are also expected to evolve. The expectation is that within this evolution process, unanticipated issues will be minimized.

Guiding Principles (13)

- To ensure that the project/facility configuration can be managed appropriately, the basis for decisions related to safety should be clearly documented. This includes decisions related to controls selection, MAR, process options, inputs, assumptions, and similar decisions.

DOE-STD-1189 Content

Safety Design Guiding Principles

1. Introduction
2. Project Integration and Planning

2.1 Contractor Integrated Project Team

2.2 Safety-in-Design Integration Team

2.3 Safety Design Strategy

2.4 Safety Interface with Project Management

3. Safety Considerations for the Design Process

3.1 Initiation Phase

3.2 Conceptual Design Phase

3.3 Preliminary Design Phase

3.4 Final Design Phase

4. Hazard and Accident Analyses

4.1 Initiation Phase – Preconceptual Planning

4.2 Conceptual Design Phase

4.3 Preliminary Design Phase

4.4 Final Design

5. Nuclear Safety Design Criteria
6. Safety Reports

6.1 Safety Input to the Conceptual Design Report

6.2 Conceptual Safety Design Report

6.3 Preliminary Safety Design Report (and PDSA)

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

7. Transition/Closeout Phase

7.1 Introduction

7.2 Development of Documented Safety Analysis

7.3 Checkout/Acceptance, Testing and Commissioning

7.4 Readiness Reviews

8. Safety Program And Other Important Project Interfaces

DOE-STD-1189 Content (cont'd.)

9. Additional Safety Integration Considerations for Projects
9.1 Integration of Safety into Facility Modifications
9.2 Construction Projects within Operating Facilities
9.3 Government Furnished Equipment

APPENDIX A Safety System Design Criteria
A.1 Seismic Design Basis
A.2 Safety Classification of SSCs
A.3 Existing Facilities and Major Modifications of Existing Facilities

APPENDIX B Chemical Hazard Evaluation

APPENDIX C Facility Worker Hazard Evaluation

APPENDIX D Additional Functional Classification Considerations

APPENDIX E Safety Design Strategy

APPENDIX F Safety-in-design Relationship with the Risk Management Plan

APPENDIX G Hazards Analysis Table Development

APPENDIX H Conceptual Safety Design Report

APPENDIX I Preliminary and Final Design Stage Safety Documentation
I.1 Introduction
I.2 PSDR/PDSA Format and Content Guide

APPENDIX J Major Modification Determination Examples

Safety and Design Integration
DOE-STD-1189

Integrated Project Team and Safety Design Integration Team

- DOE O 413.3A (and its predecessor) require DOE to form an Integrated Project Team (IPT) to manage projects when needed. Nuclear projects typically require an IPT.
- DOE-STD-1189 includes a recommendation for a Safety Design Integration Team (SDIT)

DOE M 413.3-1 on IPT

- Integrated Project Team membership should comprise representatives from all the business and technical disciplines, such as legal, financial, contracting, safety, environmental health, and others, necessary for successful execution of the project
- Project team composition changes as project progresses

Contractor IPT?

- DOE addresses the DOE organization with limited discussion for the contractor.
- Typically the contractor develops a project team with similar membership to DOE.
- DOE-STD-1189 encourages the formation of the contractor IPT.

What is the Contractor Integrated Project Team?

- Similar makeup to DOE IPT
- Human drivers who ensure integration of mission need, safety analysis, and design
- Diversity of expertise is essential
- Project process understanding very helpful
- Strong upper management commitment to supporting IPT members
- Need consistency and longevity of team members to help avoid problems
- Team formed after approval of CD-0

Typical Contractor Nuclear Facility IPT Representation

- Facility owner/operator
- Funding organization
- Project management
- Health, Safety, and Radiation Protection
- Nuclear safety
- Engineering
- Waste management
- Procurement
- Safeguards and Security (as needed)
- Quality assurance
- Computing, communications and networking
- DOE representative

What is the SDIT?

- Team formed to support the IPT
- Usually composed of subset of IPT plus other specialties as needed
- Used to help ensure integration of safety into design
- Core team
  - Safety
  - Design
  - Operations
- Additional composition depends on the hazards and safety issues

SDIT Objectives

- Identify and analyze hazards in the facility
- Help ensure that controls
  - Are adequate to serve their safety function
  - Don’t create undue burden on operators
  - Can be designed to meet safety function
  - Fit within project cost and schedule
- Timely communications with and support to IPT

Summary

- Successful projects are driven by dedicated and qualified people
- DOE requires formation of an IPT for certain projects
- The contractor often has its own IPT
- To support integrating safety into design, DOE-STD-1189 recommends forming a SDIT to focus on safety issues

Safety Design Strategy (SDS)

Purpose

- The SDS is a tool to guide design, document the safety analysis approach, and establish concurrence on major safety decisions related to project cost and schedule.
- The goal of the SDS is to set the tone for, and maintain the alignment of, the safety basis and design basis during the early evolution of the project.

Objectives

- The SDS provides a single source for project safety policies, philosophies, major safety requirements, and safety goals to guide the design process.
- The SDS provides the preliminary information to gauge the scope of significant hazards and the general strategy for addressing those hazards

Objectives (cont'd)

- To ensure appropriate attention and buy-in by project approval authorities, the SDS should contain enough detail to guide design on overarching design criteria, establish major safety structures, systems, and components (SSC), and identify significant project risks associated with the proposed facility relative to safety.

Objectives (cont’d)

- Concurrence on these topics with approving authorities, while acknowledging associated risks, establishes a critical baseline for project execution.

Timing

- An SDS should be developed in the earliest stages of the project cycle, initially at CD-0, and updated as needed for each succeeding phase of the project
- For projects that may not follow the traditional project cycle, the SDS provides a vehicle to describe how requirements for safety documentation will be tailored to that particular project approach while satisfying the intent of DOE O 413.3A

Elements

1. The guiding philosophies or assumptions to be used to develop the design
2. The safety-in-design and safety goal considerations for the project
3. The approach to developing the overall safety basis for the project

Tailoring

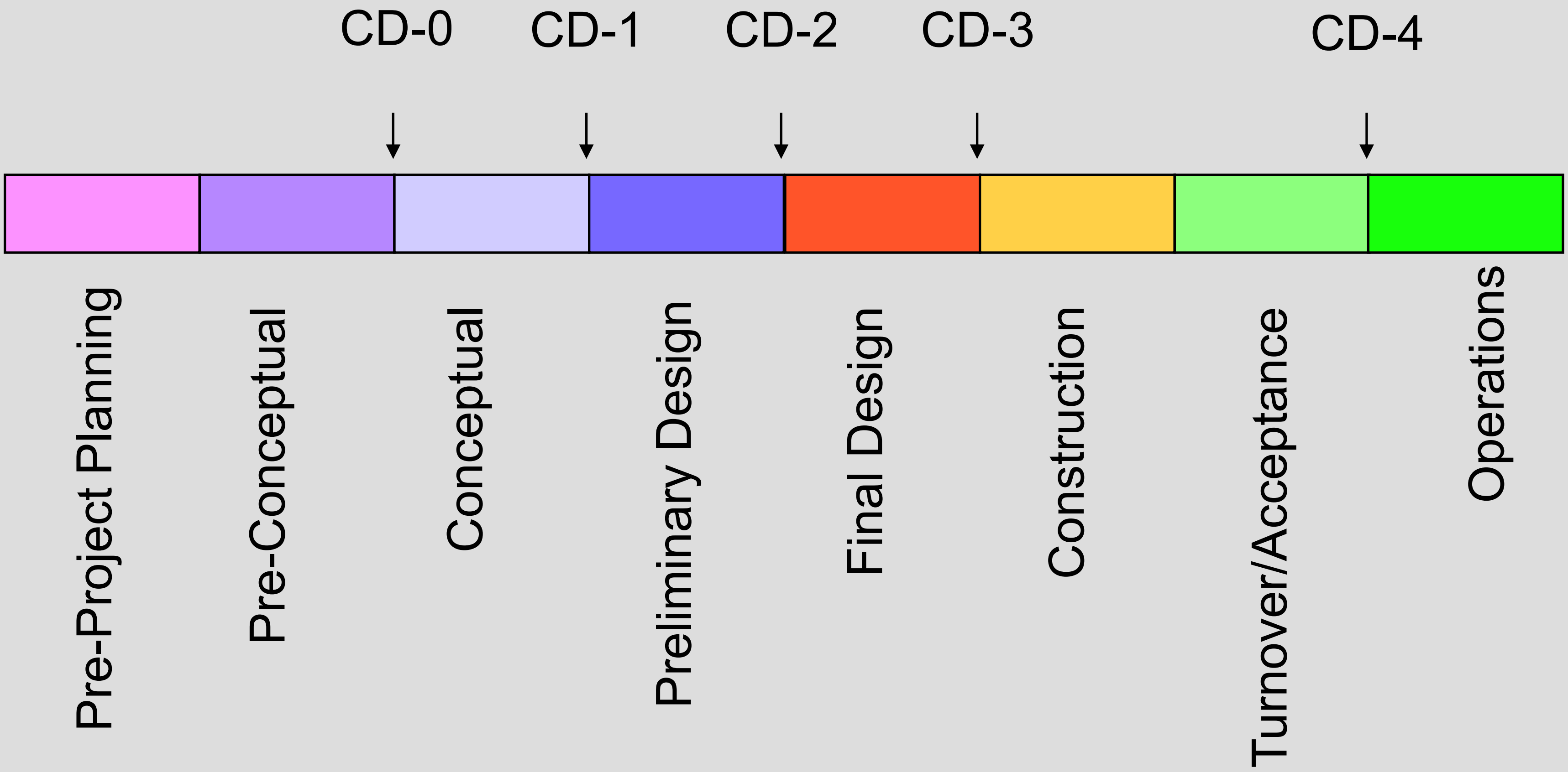
- DOE O 413.3A allows tailoring of the CD process for projects based on “risk, size, and complexity.
  - The tailoring approach for the CD process is typically described in a “tailoring strategy” or as part of the PEP.
  - Tailoring of the safety basis development steps and documents for a project is also permitted based on the level of risk posed by the facility chemical and radiological hazards, the complexity of the processing operations, and the scope of the hazards analysis required for the project.
  - The SDS should provide supporting documentation on the type and scope of the hazard/accident analysis and safety documents for a project

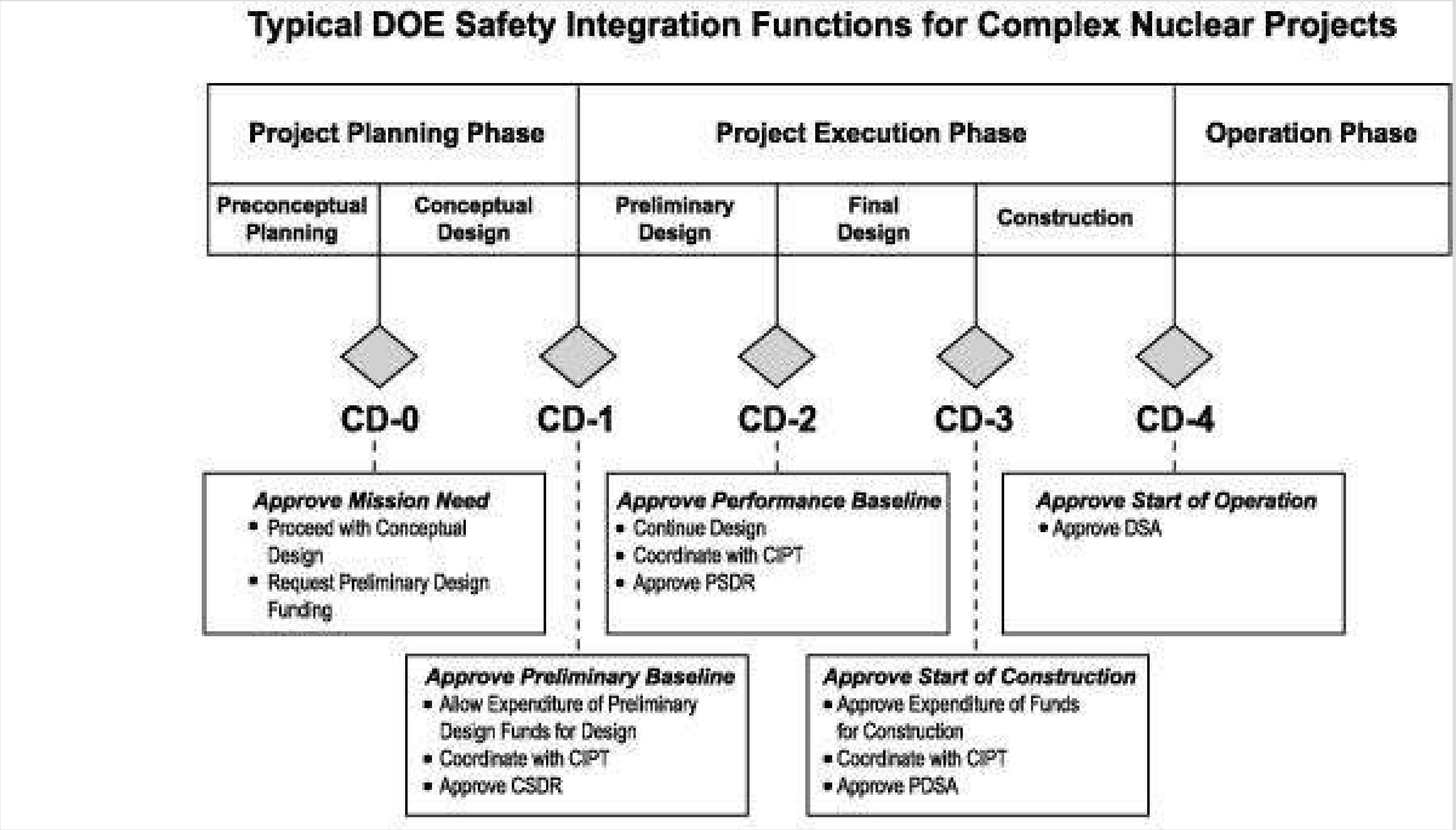
SDS Format and Content

- Described in Appendix E of STD-1189
- Depth of treatment is based on tailoring and project needs for the phase of the project
- The SDS should be as detailed as needed to communicate the strategy for successfully integrating safety and design and producing safety basis documentation that will be approved to allow either entry into the next critical decision or into operation

Safety in Design
for a
Greenfield Project by O 413.3A
Project Phase

Project Lifecycle

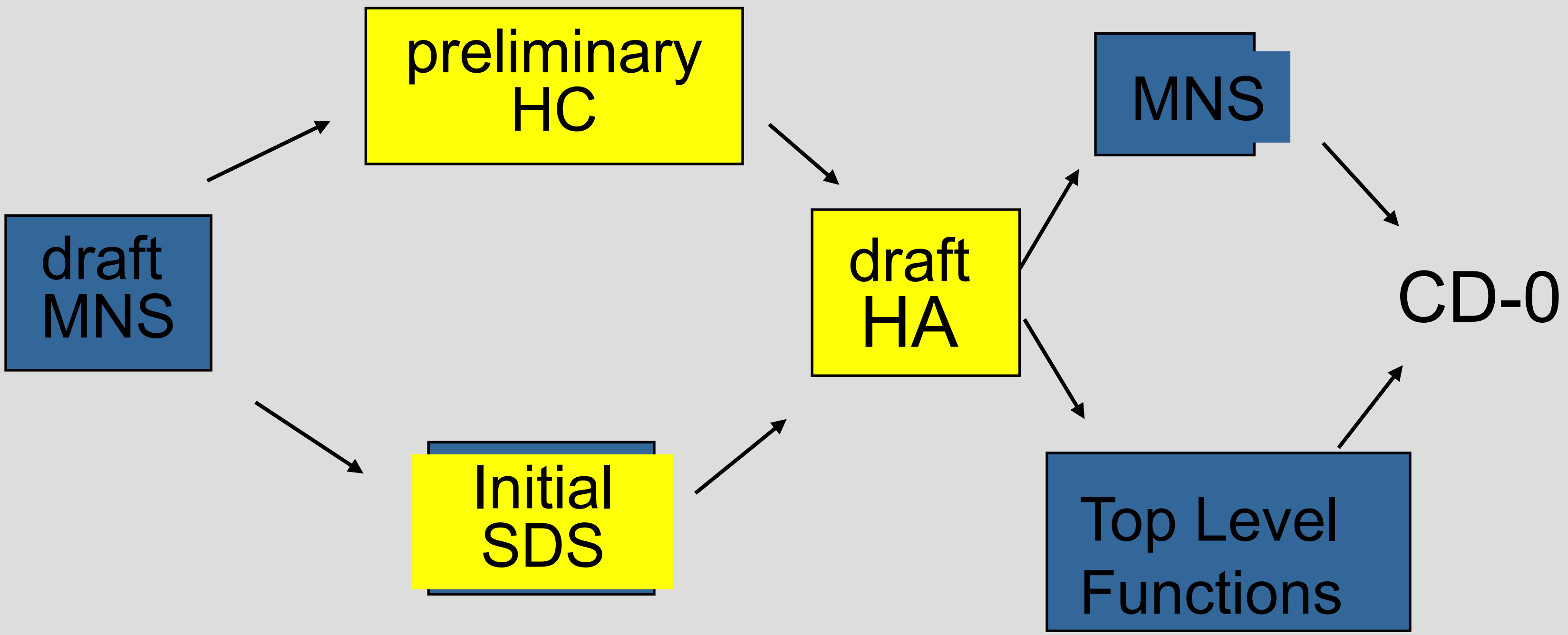



Typical DOE Safety Integration Functions for Complex Nuclear Projects
Project Planning Phase
Project Execution Phase
Operation Phase
Preconceptual Planning
Conceptual Design
Preliminary Design
Final Design
Construction
CD-0
CD-1
CD-2
CD-3
CD-4
Approve Mission Need
• Proceed with Conceptual Design
• Request Preliminary Design Funding
Approve Performance Baseline
• Continue Design
• Coordinate with CIPT
• Approve PSDR
Approve Start of Operation
• Approve DSA
Approve Preliminary Baseline
• Allow Expenditure of Preliminary Design Funds for Design
• Coordinate with CIPT
• Approve CSDR
Approve Start of Construction
• Approve Expenditure of Funds for Construction
• Coordinate with CIPT
• Approve PDSA

Preconceptual Phase

- Objective is to obtain DOE agreement that a material solution to a mission related problem exists
- Results in development of Mission Need which becomes a baseline document in project if CD-0 is granted
- Limited or no design and analysis required

The Path to CD-0



Safety Activities in Preconceptual Design Phase

- Chapter 3 of 1189 provides guidance
- Identify top level hazards (may be associated with particular approaches)
- Preliminary HC determination
- Project safety lead assigned to establish continuity

Additional Safety Activities

- Preconceptual Hazards Analysis
- Upper level safety functions and performance requirements needed to support mission
- Initial draft of Safety Design Strategy (SDS)

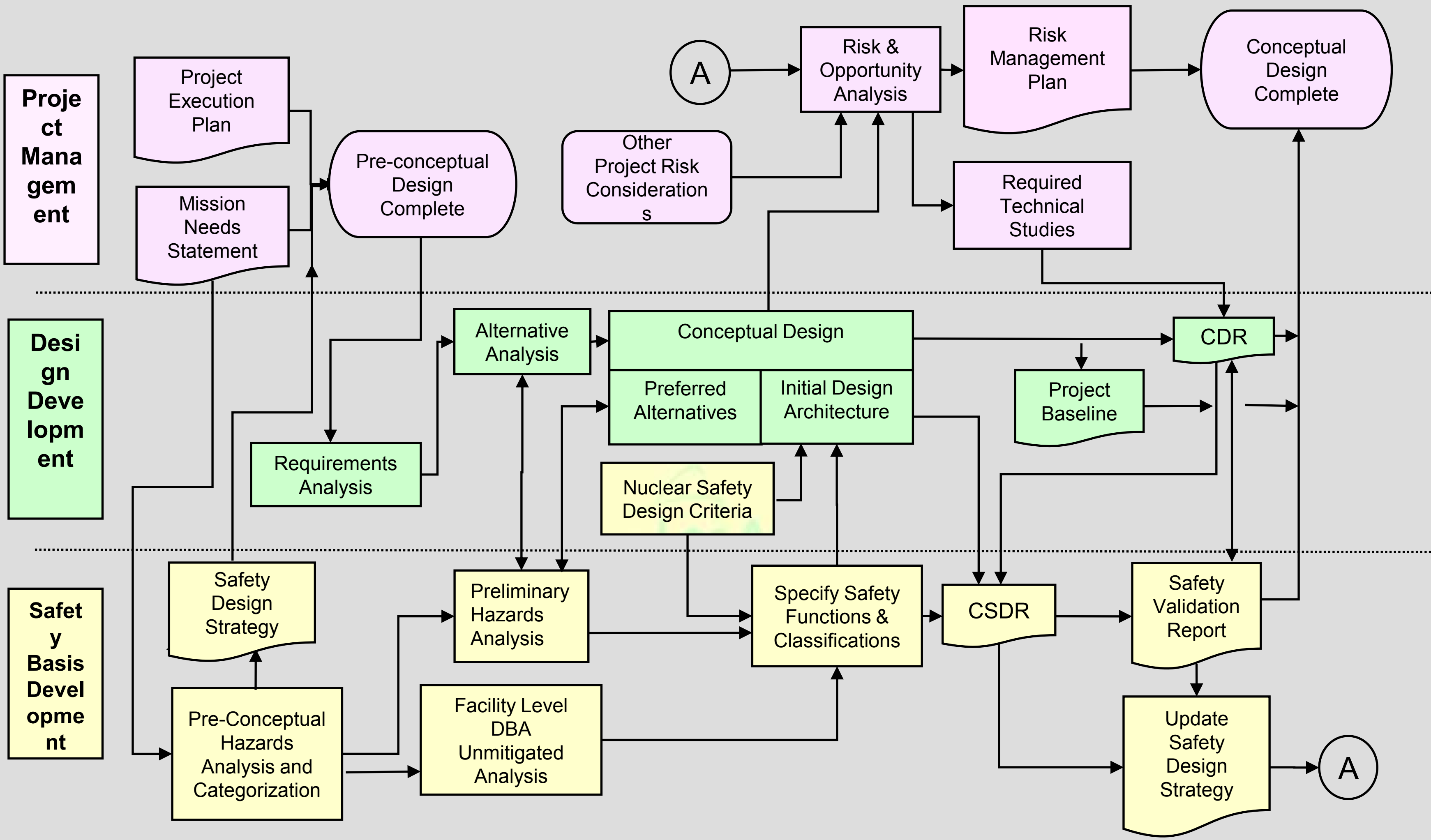
What's Else is New?

- More safety activities addressed in 1189 than in DOE O 413.3
- 1189 discusses design activities, such as alternatives studies, that are currently not addressed in DOE O 413.3
- 1189 recognizes that level of safety info should be consistent with design and project related info

Conceptual Design Phase

- This phase begins after DOE grants CD-0
- Contractors are authorized to spend money on conceptual design activities
- Objectives of conceptual design include
  - Define a preferred alternative (design) solution to Mission Need problem
  - Establish a cost and schedule range
  - Demonstrate understanding of safety issues

Conceptual Design Process Flow



Key Nuclear Safety Activities

- IPT formed (both DOE and Contractor)
- SDIT formed
- PHA developed to define safety functions
- Facility level DBAs identified and assessed
  - Bounding consequences
  - Used to establish functional classification
- SDS updated (or developed if not addressed in pre-conceptual)

More Nuclear Safety Activities

- Conceptual Safety Design Report (CSDR) developed
- Safety input to Risk and Opportunity Analysis
- Conceptual design SSCs that perform required safety functions identified
  - Significant cost drivers
  - Helps demonstrate that conceptual design is credible
  - Helps understand potential technical risks

Safety Design Strategy (SDS)

- Discussed earlier in presentation
- Key document to establish approach to nuclear safety for project
- Evolves with project
- Three main topical areas
  - Guiding philosophies and assumptions
  - Safety goals and approaches for key safety design objectives
  - Approach to development of safety documentation

Preliminary Hazards Analysis (PHA)

- Facility level hazards analysis
- Helps define needed safety functions
- Helps to define DBAs and uses DBAs as input (iterative process)
- Input to CSDR
- A detailed analysis of the CDR design not expected or required
- Question??
  - Based on design solution or
  - Based on required activities to meet Mission Need?

DBAs

- Design basis accidents postulated based on facility level upsets
- Unmitigated consequences assessed to help establish both needed safety function and safety classification of that function
- These accidents need not have the potential for public impact, they are to help define safety functional and design requirements
- DBAs refined and expanded upon in later stages of project

Conceptual Safety Design Report (CSDR)

- New requirement from DOE O 413.3A
- Establishes the facility preliminary hazard category
- Preliminary identification of facility DBAs
- Assess the need for SC and SS facility level controls (based on the DBAs)
- Preliminary assessment of appropriate seismic design criteria
- Commitment to nuclear safety design criteria
- Format for CSDR in Appendix H of 1189

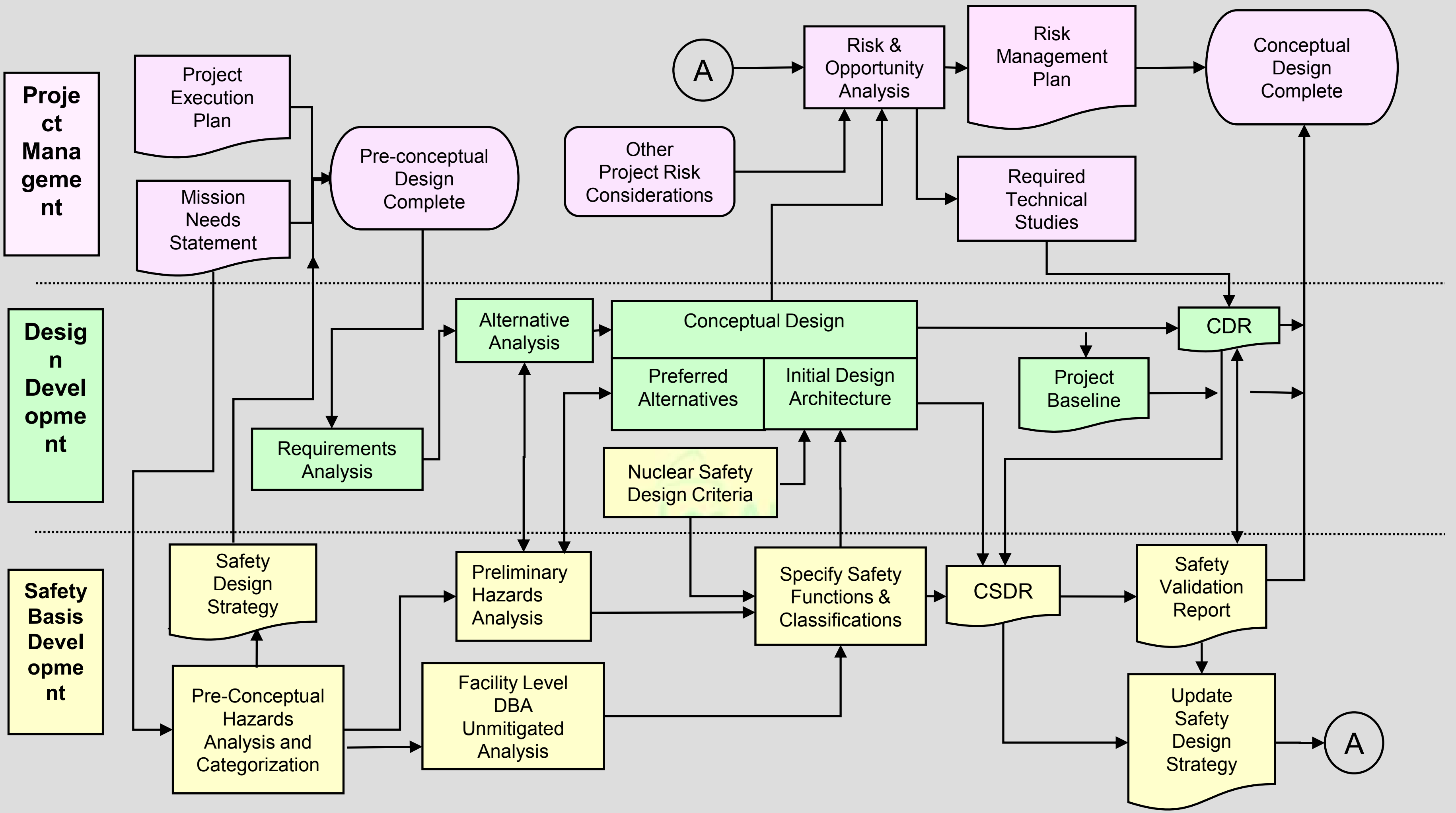
Safety Validation Report

- DOE prepares the SVR to show approval of the CSDR
- Confirms that positions taken in the CDR and documented in the CSDR are appropriately conservative to proceed to preliminary design
- DOE-STD-1104 being revised to address SVR

Final Words on the Safety Analysis

- The safety analysis should accomplish two general objectives
  - Derive the necessary safety functions that any facility must meet to accomplish the defined mission
  - Show that the CDR is a credible way to meet those functions
- Design choice based hazard controls must be segregated from intrinsic hazard controls as they may be designed away in subsequent design phases.

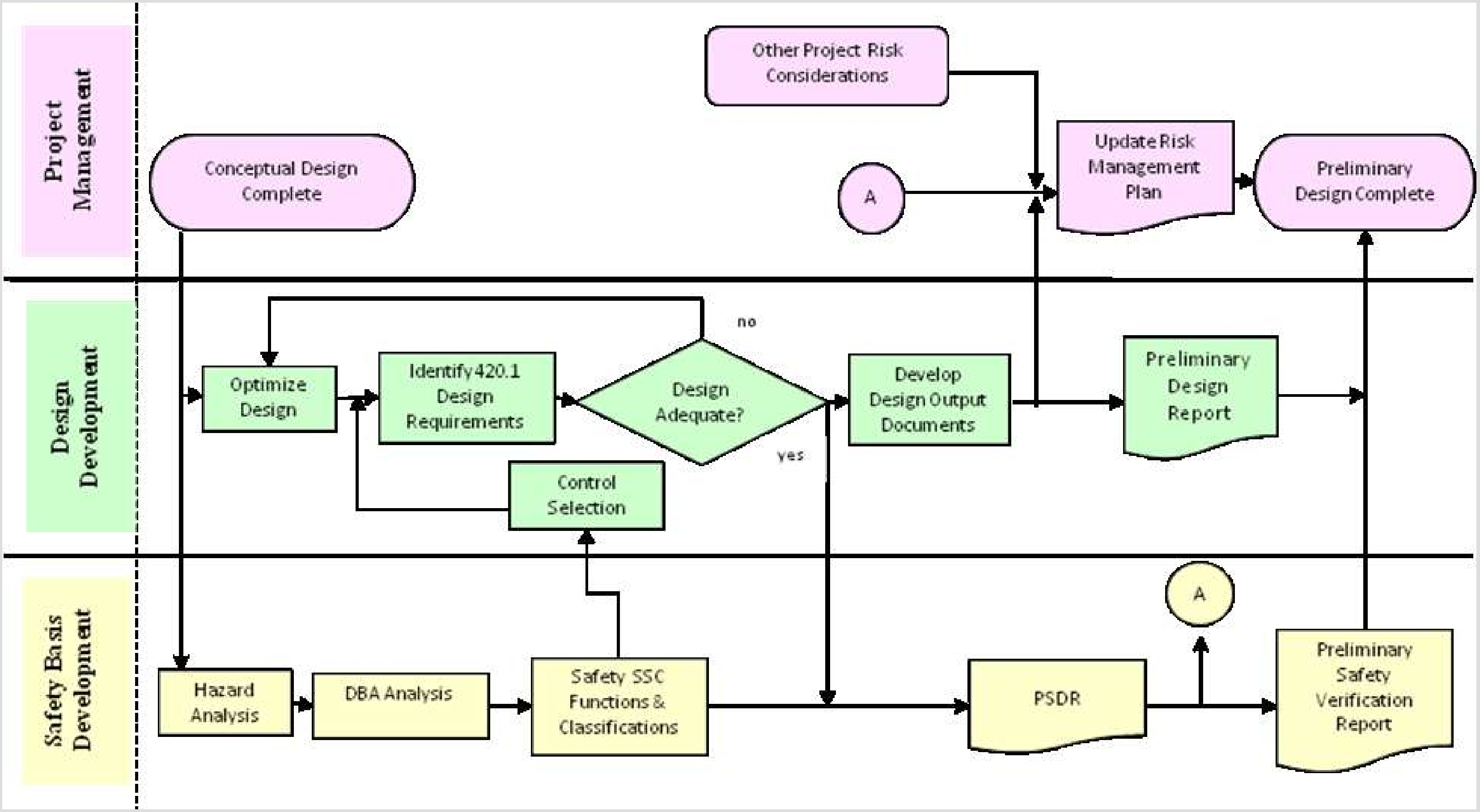
Conceptual Process Flow Recap



Preliminary Design Phase

- After CD-1 is granted by DOE, the design enters the preliminary design phase
- The preliminary design phase serves to advance the design toward the final product
- The end of the preliminary design phase typically represents about 30% of the final design

Preliminary Design Process Flow



Starting Preliminary Design

- Design basis from conceptual design
- Changes due to DOE reviews
- Changes due to DOE conditions of approval of CD-1 package
- May have new architect / engineer

Safety Activities in Preliminary Design

- Complete HA using design as a basis
- Optimize design choices
- Update SDS
- Evaluate and apply DOE O 420.1B and associated guide design requirements
- Develop DBAs based on actual design
- Develop the Preliminary Safety Design Report (PSDR)

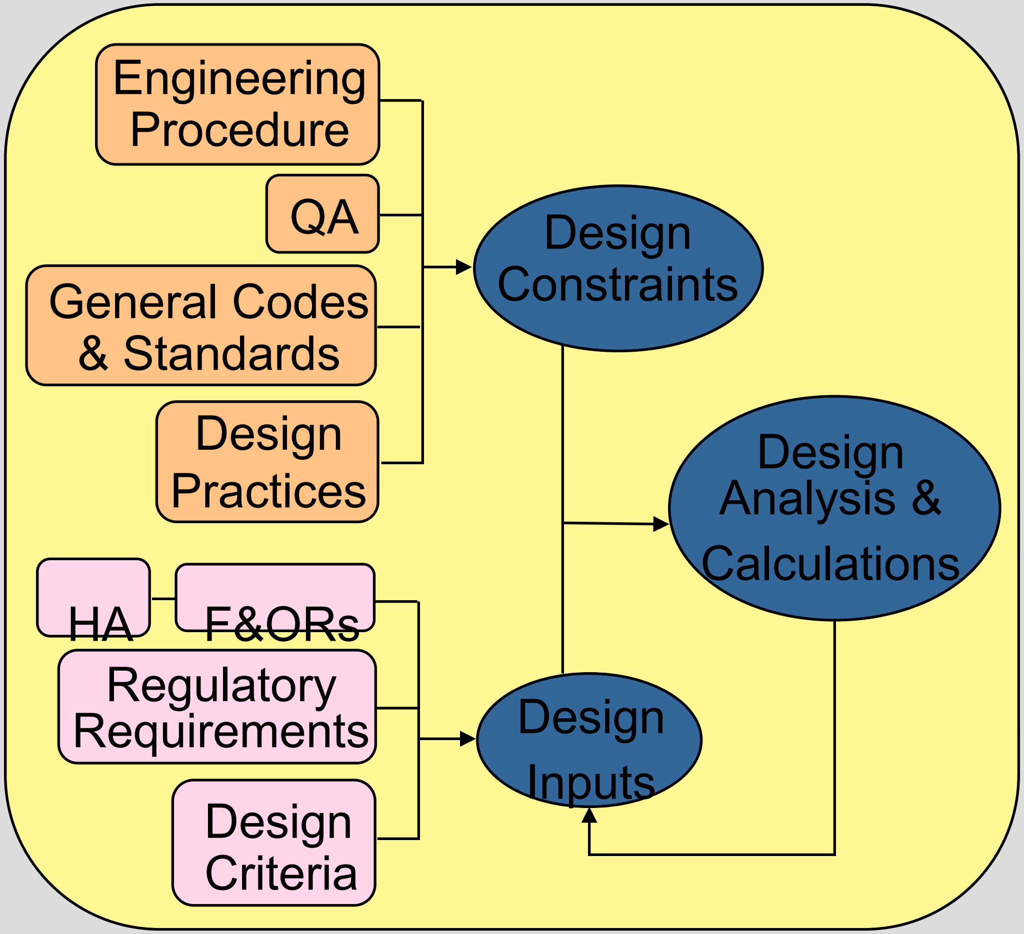
PrHA

- The PHA forms the basis for the PrHA
- The hazards analysis is updated to reflect the actual design
- SSCs that are chosen to provide safety functions are mapped into the PrHA
- SACs, if required, are identified and justified

DBAs in Preliminary Design

- DBAs are refined to address design requirements based on actual design
- Input to design requirements
- Provide the basis for final SSC functional classification
- DBAs, just as in conceptual design, do not have to have a public impact to be selected

Generalized Design Process



Interface with Design

- Assist designers in understanding
  - Safety requirements from Conceptual Design
  - Safety implications associated with design alternatives and trade studies
  - Safety interpretation of DOE O 420.1B and DOE G 420.1-1 requirements and recommendations
- Safety input into SDDs and SSC design
  - System boundaries
  - Derivative safety functions and requirements
  - Supporting analyses

Develop HA and PrHA

- Evolve from facility level analysis
- HA activities supports design selection
- Making design choices supports developing the HA and PrHA for the PSDR
- HA and PrHA activities support selection of DBAs and vice versa

PrHA and Design Evolution

- The outcome of the preliminary design phase is the design that is intended to be built, but without the details needed to actually purchase and construct
- Design maturity should allow selection of worker safety functions and associated design elements
- Final PrHA must be based on the selected design

Project Design Review Issues

- Design reviews within the project setting are not specifically addressed by 1189
- Frequently there are incremental design reviews associated with conceptual and preliminary design
- Safety basis input to these reviews helps ensure proper integration of safety
- How to accomplish this integration should be considered in the planning for the safety basis documentation
- One approach is to include the safety basis information as draft with additional support through addenda to design products like the SDDs

Preliminary Design Safety Report (PDSR)

- Developed to support safety adequacy of the preliminary design effort
- Based on the format and content of the PDSA
- Limited in that design information is also limited
- Discussed in 1189

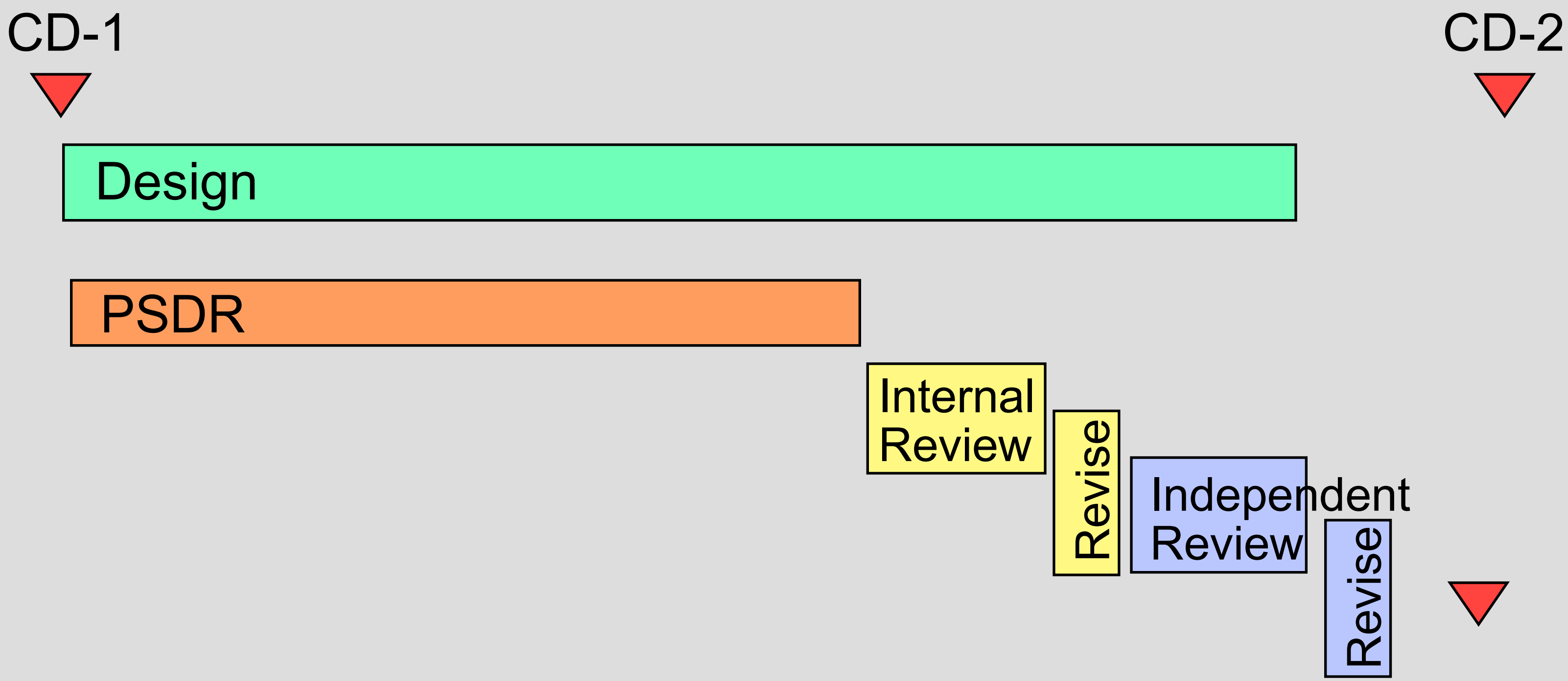
DOE Safety Validation Report

- SVR prepared by DOE to approve PSDR
- Similar to SER
- Guidance for SVR being integrated into revision to DOE-STD-1104
- SVR could contain required changes to design and/or additional analysis requirements

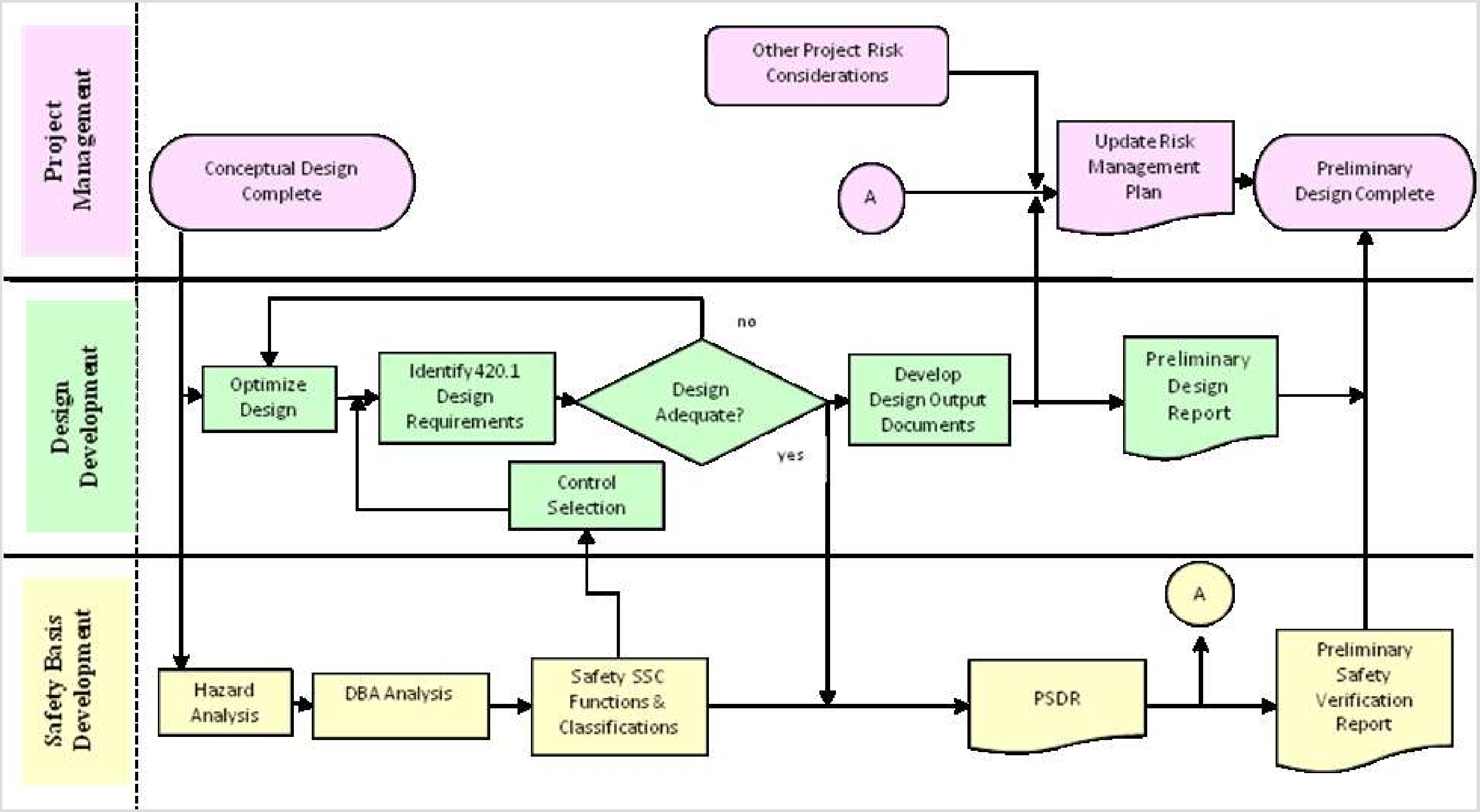
Schedule Concerns

- The PSDR is finalized at the end of the preliminary design
- Quality assurance dictates that reviews be conducted within the project team
- Scheduling to reduce impact of the PDSA on overall schedule may be desired

PSDR Schedule Issues



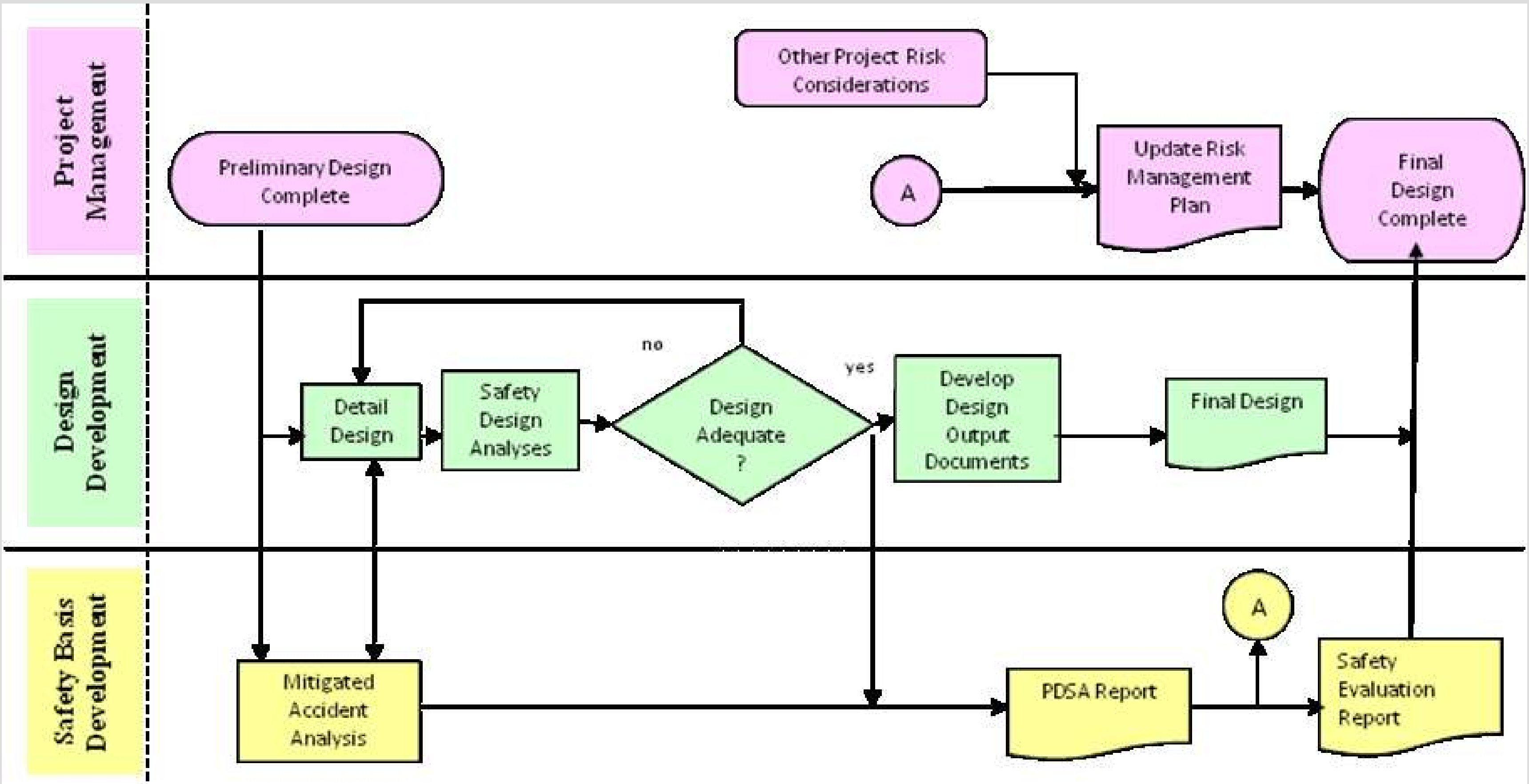
Preliminary Design Recap



Final Design

- The final design stage completes the design
- If preliminary design represents about 30% of the design, then 70% is performed in final
- Evolves the preliminary design to the point where
  - Specifications developed
  - Procurement can be accomplished
  - Test, inspection, and commissioning requirements detailed
  - SDDs and FDD completed

Final Design Process Flow



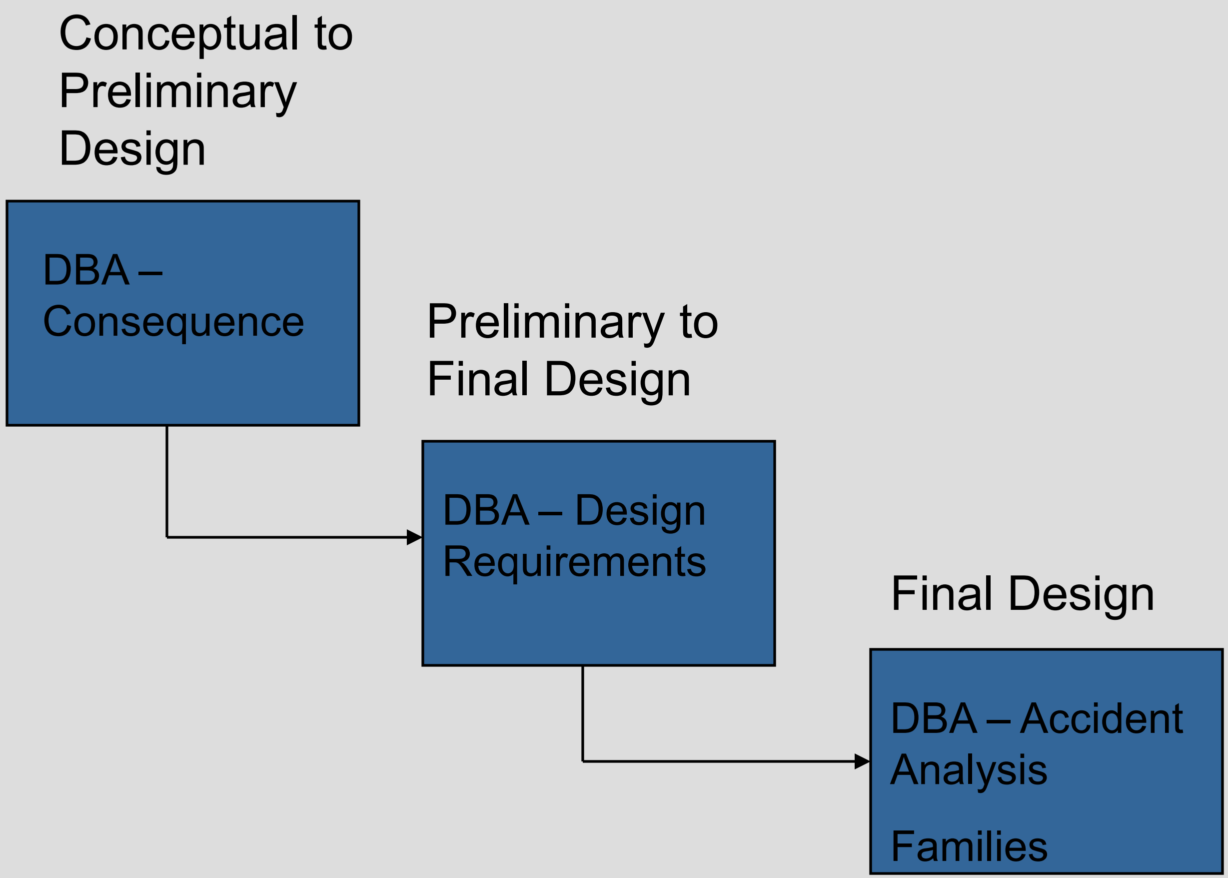
Safety Basis Activities

- Complete mitigated accident analysis
  - Evolves from DBAs
  - Shows adequacy of control suite
  - Credits the actual performance of the SSCs
  - Supports input into DSA
- Address SVR and other issues from preliminary design
- Develop the Design Safety Analysis arguments

Mitigated Accident Analysis

- What do we mean by this?
  - DBAs developed earlier define unmitigated consequences to assist in functional classification
  - DBAs also defined design requirements
  - 3009 uses DBA concept differently – as an Evaluation Basis Accident (EBA)
  - Mitigated accident analysis evolves DBAs and members of their family to 3009 like accident analysis

Accident Analysis Progression



PDSA

- Evolves from the PSDR
- Completes the analysis of the design
- Format and content covered in 1189
  - Based on DOE-STD-3009
  - Minimize need to rewrite for DSA
- Provides the argument for design adequacy with respect to nuclear safety

Design Safety Analysis

- Supports the argument that the design satisfies nuclear safety design criteria and derived safety requirements
- May reside outside the PDSA proper with results summarized and referenced
  - SDD (for active safety SSCs)
  - FDD (could be used for passive safety SSCs)

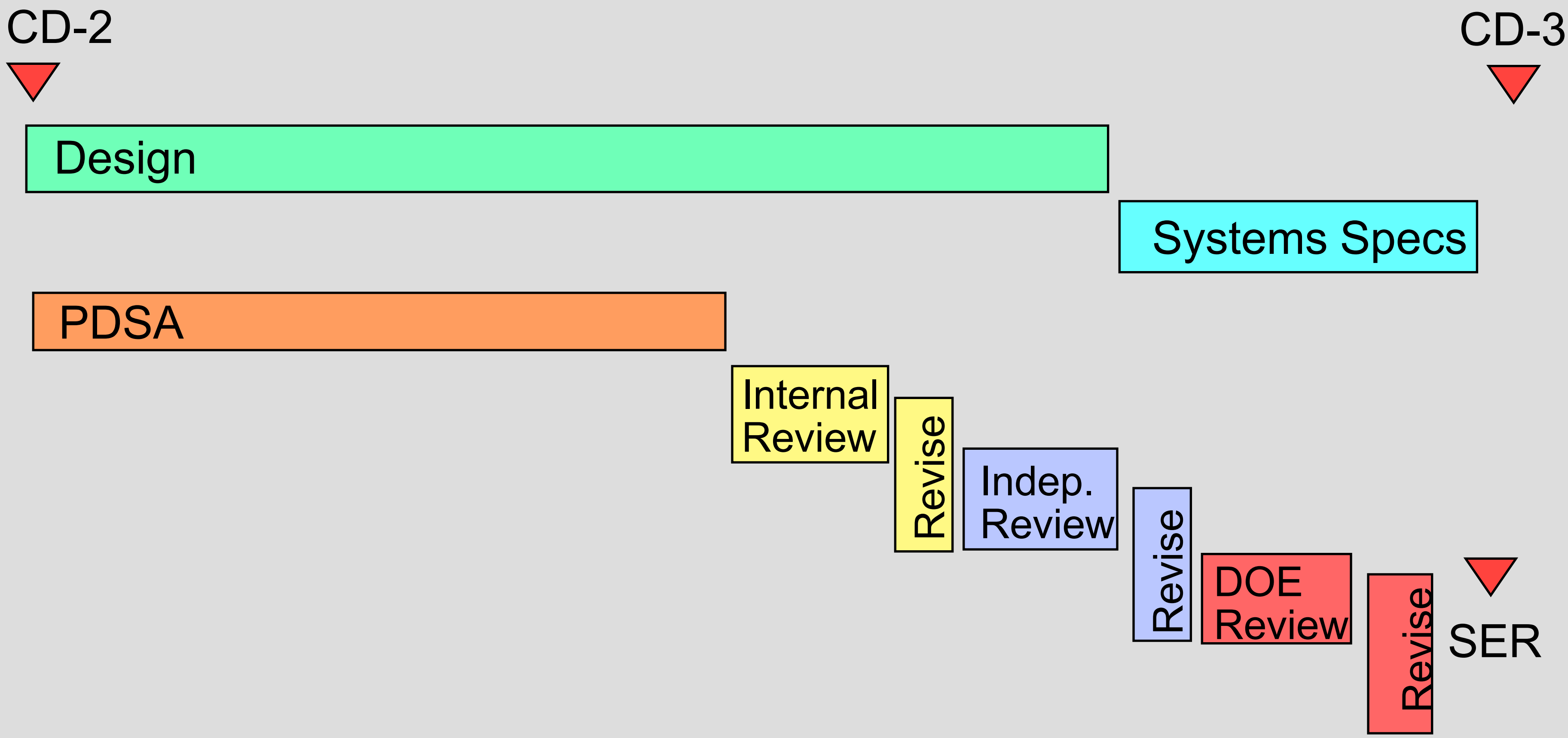
Example Design Safety Analyses (Criteria from DOE G 420.1-1)

- Defense-in-depth
- Safe failure modes
- NPH 2 over 1
- Conservative design margins
- Demonstration that concept is met- broader than 3009 approach
- Analysis of failure mechanisms and selection of preferable failures
- Identification of system interactions
- Defining safety margins

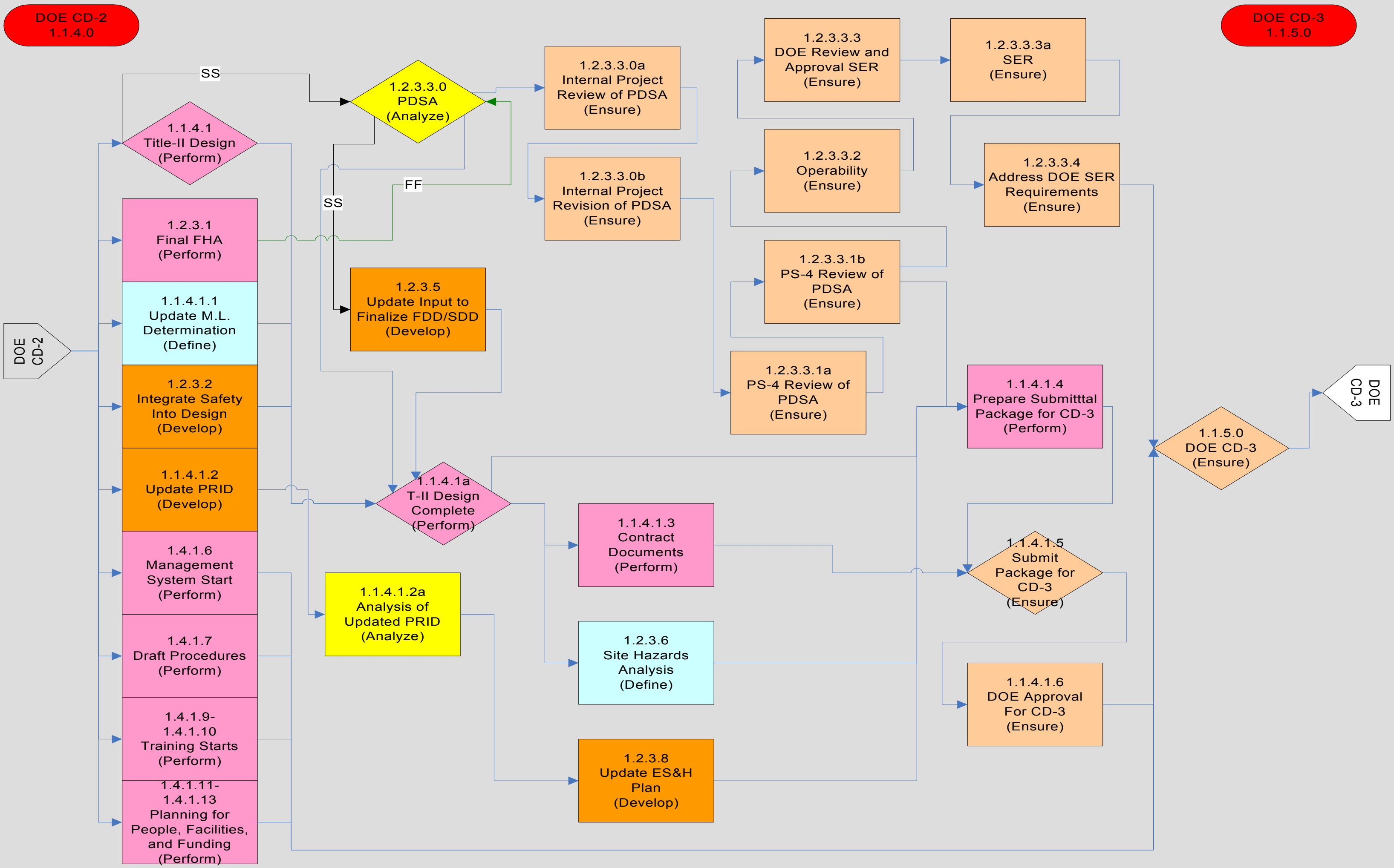
DOE SER

- Formal approval of the PDSA
- DOE-STD 1104 being updated to reflect requirements associated with the PDSA SER
- Approval via the SER is a prerequisite to beginning procurement and construction (some allowances for early procurement and construction allowed by DOE with justification)

PDSA Development Schedule Issues



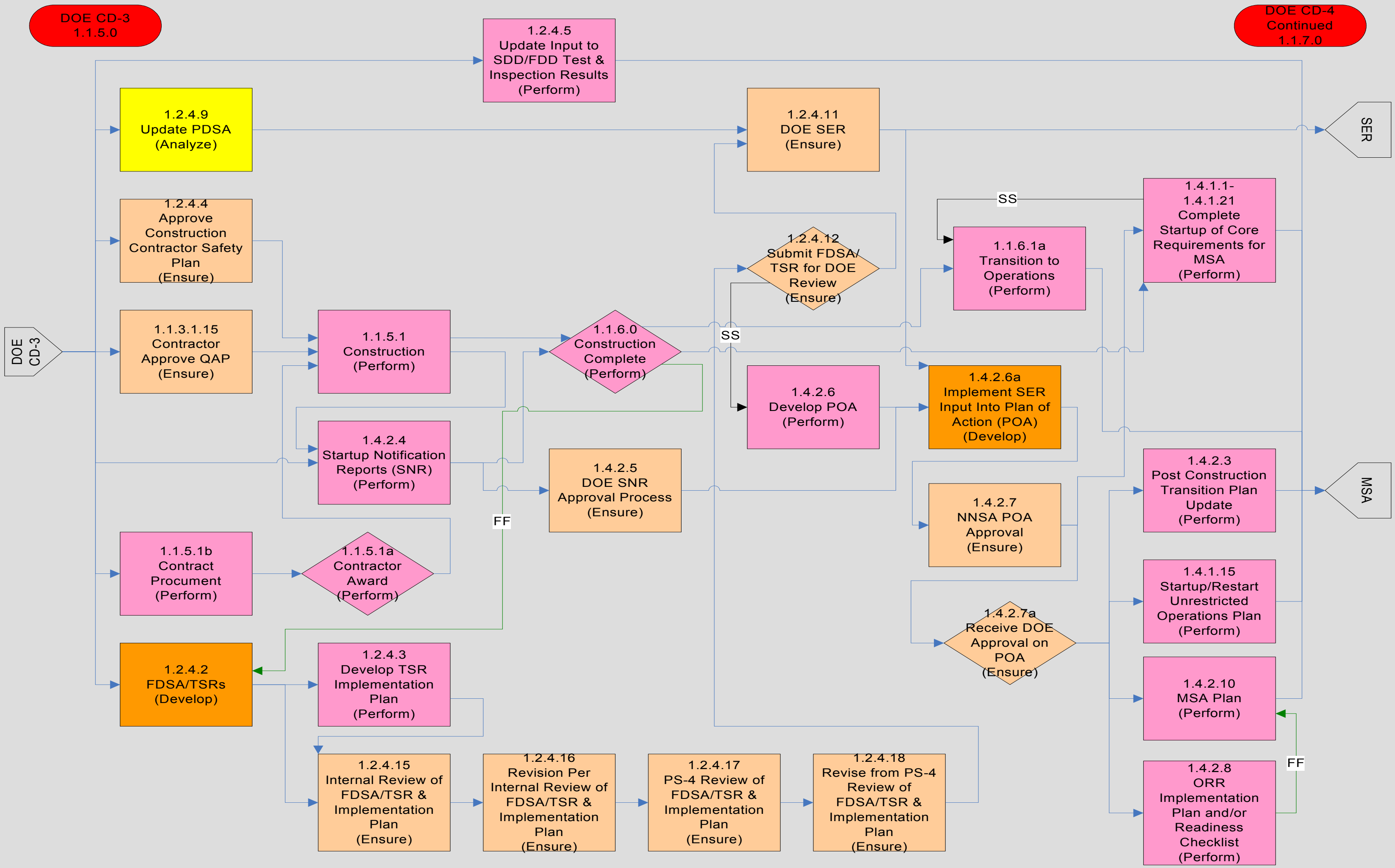
CD-3 (prior to 1189 for LANL)



Construction / Transition Phase
Design Related Issues

- Field Changes
- GFE and other equipment not part of primary design
- Revisions to PDSA (suggested by DOE for projects of long duration)
- Changes to comply with readiness review issues
- Input to DSA and TSR

Going from CD-3 to CD-4



Summary

- Safety in design is supported by specific actions in each project phase
- The safety in design process is supported by the preparation of safety analysis documents
  - CD-1, SDS and CSDR
  - CD-2, PSDR
  - CD-3, PDSA
- DOE-STD 1189 provides guidance for each of these products and discusses processes to help achieve design integration

Appendix A

Safety System Design Criteria

Purpose

- Provides guidance and objective criteria for specification of the seismic design basis and the safety classifications of SSCs based on radiological hazards
- Specifies the methodologies to be applied to the major preventative and mitigative SSCs that are selected from the analyses of the DBAs

Seismic Design Basis

- Applies recently published national standards for seismic design of DOE non-reactor nuclear facilities
  - ANSI/ANS 2.26-2004, *Categorization of Nuclear Facility Structures, Systems and Components for Seismic Design*; and
  - ASCE/SEI 43-05, *Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities*.

ANSI/ANS 2.26

- Establishes seismic design classifications. Combination of Seismic Design Category (SDC) and Limit States (LS) used with the radiological criteria of Appendix A provide the seismic design basis for SSC

ASCE/SEI 43-05

- Provides the design criteria to use for the defined seismic classification

Guidance for SDC Based on Unmitigated Consequences of SSC Failures in a Seismic Event

	Unmitigated Consequence of SSC Failure from a Seismic Event	
Category	Collocated Worker	Public
SDC-1	Dose < 5 rem	Not applicable - A hazard category 1, 2, or 3 nuclear facility with consequences to a collocated worker from failure of an SSC in a seismic event will require that SSC to be classified as SDC-1 at a minimum. Therefore, a public criterion for SDC-1 is not needed
SDC-2	5 rem < dose < 100 rem	5 rem < Dose < 25 rem
SDC-3	100 rem < dose	25 rem < dose

Default Seismic Criteria

- In conceptual design, if there are no bases for defining seismic related DBAs, hazard category 2 facility structural designs must default to ANSI/ANS 2.26 SDC-3, Limit State D.
- If the hazards analysis conducted during subsequent stages of design shows that unmitigated consequences are less than the threshold criteria for SDC-3 shown in Table A-1, then this may be reflected in the evolving design stages.

Safety Classification Methodology
Public Protection

- The guidance of DOE G 421.1-2 and DOE-STD-3009, Appendix A, should be used in classifying SSCs as Safety Class (SC) for radiological protection.
  - The words “challenging” or “in the rem range” in those documents should be interpreted as radiological doses equal to or greater than 5 rem, but less than 25 rem.
  - In this range, SC designation should be considered, and the rationale for the decision to classify an SSC as SC or not should be explained and justified.

Safety Classification Methodology Collocated Worker Protection

- Unmitigated accident analysis source term guidance of DOE-STD-3009, Appendix A, Section A.3.2 of and DOE G 420.1-1
- Dose of 100rem TEDE at 100m
- Use ICRP 68 dose conversion factors
- Apply χ/Q value at 100 m of 3.5E-3 sec/m3 for the dispersion calculation. This value is based upon NUREG 1140 (no buoyancy, F-stability, 1.0 m/sec wind speed at 100 m, small building size (10 m x 25 m), and 1 cm/sec deposition velocity).

Backfit Implications

- The seismic design classification and collocated worker Safety Significant criteria of this appendix shall not be applied in a backfit sense to existing facilities that are *not* undergoing modifications.

Backfit for Major Modifications

- For major modifications of existing facilities, criteria are applicable. Backfit analyses should examine:
  1. The need to upgrade interfacing structures, systems, and components in accordance with these criteria, and
  2. Whether there should be relief for the modification from the design requirements that application of these criteria in design would imply.

Appendix B

Chemical Hazard Evaluation

Purpose

- DOE is not invoking mandatory classification of safety SSCs or specifying nuclear design requirements based on chemical hazards alone

Content

- Guidance for consideration of Safety Significant designation of SSCs in terms of “advisory criteria” for chemical exposures based on a process of
  - Screening chemicals (hazardous materials) to determine those that may have the potential to immediately threaten or endanger onsite (collocated) workers or the public and
  - Evaluating the severity of potential exposures against advisory classification criteria for collocated workers and the public

Screening Criteria

- Chemicals that may be excluded from further analysis for functional classification and the identification of attendant design criteria include
  - Chemicals with no known or suspected toxic properties.
  - Materials used in the same form, quantity, and concentration as a product packaged for distribution and use by the general public.
  - Chemicals in a quantity that can be “easily and safely manipulated by one person.” – can be locally determined in accordance with the provisions of 29 CFR 1910.1450(b).

Screening Criteria (cont'd)

- Materials that have a health hazard rating of 0, 1, or 2, based on NFPA 704.
- Solid or liquid materials that, because of their physical form or other factors (e.g., plausible dispersal mechanisms), do not present an airborne exposure hazard.
- Chemicals that can be defined as a Standard Industrial Hazard for which national consensus codes and standards provide for safe design and operation. The Consensus Code or Standard needs to be identified and must be applicable to the use of the chemical in the facility that is to be screened from further evaluation.

Chemical Hazardous Materials Requiring Analysis

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

Methodology

- Methods for estimating exposures are detailed in Appendix B
  - Unmitigated chemical consequence analysis shall strive to use mean values for the parameters related to material release, dispersal in the environment and health consequences
  - It is desirable to reduce any tendency toward over-conservatism to achieve the risk-informed balance in the design of the SSCs

Advisory Criteria

- Public
  - Exposure > AEGL-2/ERPG-2/TEEL-2
- CW
  - Exposure > AEGL-3/ERPG-3/TEEL-3
- Heirarchy
  - Acute Exposure Guideline Levels (AEGL, EPA)
  - Emergency Response Planning Guidelines (ERPG, AIHA)
  - Temporary Emergency Exposure Limits (TEEL, DOE)

Appendix C

Facility Worker Hazard Evaluation

Hazard Analysis

- For each hazardous condition evaluated for the public and collocated worker in the hazards analysis, a qualitative evaluation of unmitigated consequence to the facility worker (FW) and identification of candidate preventive and mitigative controls should be included.

Consideration of Safety SSC

- Conditions that warrant consideration of Safety Significant SSC include:
  - energetic releases of high concentrations of radiological or toxic chemical materials where the FW would normally be immediately present and, therefore, unable to take self-protective actions;
  - deflagrations or explosions within process equipment or confinement and containment structures or vessels where serious injury or death to a FW may result from the fragmentation of the process equipment failing or the confinement (or containment) with the FW close by;

Consideration of Safety SSC (cont'd)

- chemical or thermal burns to a FW that could reasonably cover a significant portion of the FW body where self-protective actions are not reasonably available due to the speed of the event or where there may be no reasonable warning to the FW of the hazardous condition; and
- leaks from process systems where asphyxiation of a FW normally present may result.

Consideration of Safety SSC (cont'd)

- Also considered for cases involving significant exposure of the FW to radiological or other hazardous materials (after screening per Appendix B).
  - Qualitatively evaluating unmitigated consequences in terms of radiation dose, chemical exposure, or physical injury at specified receptor locations.
  - Consequence estimates can rely on experience or can be determined from (1) simple source term calculations, (2) existing safety documentation, and/or (3) qualitative assessment supported by "back-of-the-envelope" calculations.

Significant Exposure

- For radiological consequences, the suggested evaluation criterion is 100 rem TEDE.
- For chemical exposure, the evaluation criterion is AEGL-3 or equivalent (e.g., ERPG-3, TEEL-3).

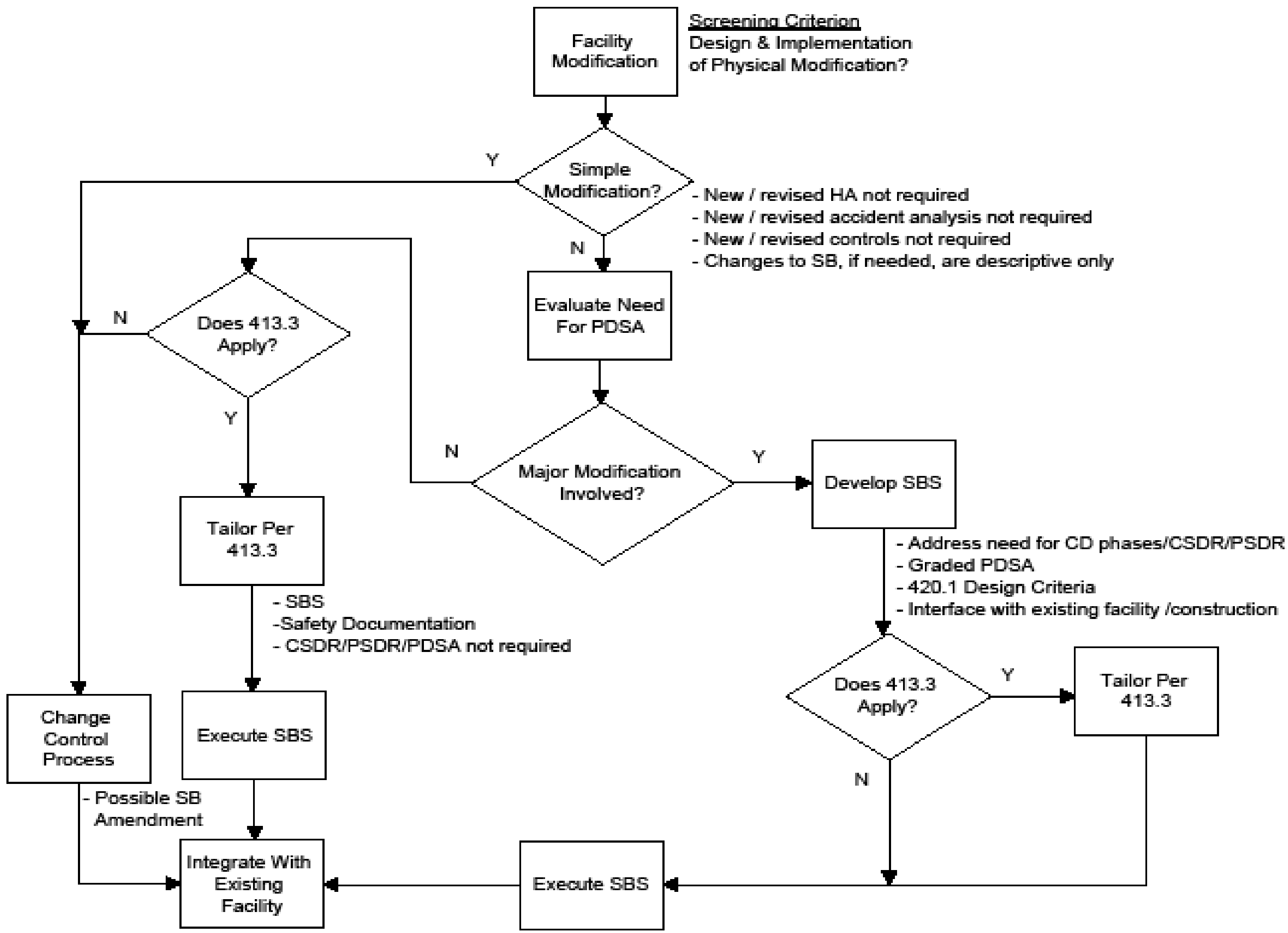
Qualitative Results

- By comparing the qualitatively derived FW radiological or chemical consequence to these evaluation criteria, an assessment can then be made about the need for SS preventive or mitigative controls.
- Where the qualitative consequence assessment yields a result that is not clearly above or below the evaluation criteria, then the need for SS FW controls shall be more closely considered by the project.

Facility Modifications

Introduction

- The process for integration of safety into the design of facility modifications is similar to that for new facilities, but it is tailored to the scope, magnitude, and complexity of the modification


Facility Modification
Screening Criterion
Design & Implementation of Physical Modification?
Simple Modification?
Y
N
- New / revised HA not required
- New / revised accident analysis not required
- New / revised controls not required
- Changes to SB, if needed, are descriptive only
Evaluate Need For PDSA
Does 413.3 Apply?
N
Y
Major Modification Involved?
N
Y
Develop SBS
- Address need for CD phases/CSDR/PSDR
- Graded PDSA
- 420.1 Design Criteria
- Interface with existing facility /construction
Tailor Per 413.3
- SBS
-Safety Documentation
- CSDR/PSDR/PDSA not required
Does 413.3 Apply?
Y
N
Tailor Per 413.3
Change Control Process
- Possible SB Amendment
Execute SBS
Integrate With Existing Facility
Execute SBS

Major Modification Definition and Implications

- As defined by 10 CFR 830.3, major modifications are those that “substantially change the existing safety basis for the facility.”
- A major modification requires the development of a Preliminary Documented Safety Analysis (PDSA) (830.206) and approval of the PDSA by DOE (830.207) prior to procurement or construction of the modification

Evaluating Modifications

- Simple modifications - review of the existing hazard analysis determines it is adequate for the modification, that the hazard controls adequately address the modification and associated activities, and that implementing the existing change control processes, such as the Unreviewed Safety Question (USQ) and configuration management processes, procedure changes, and training programs is adequate to support the proposed change.

Evaluating Modifications (cont'd)

- More than a simple modification - review indicates that a new or revised hazard analysis is required to support a proposed facility modification or associated activities.
  - Modifications to existing processes – the hazard analysis revision may involve identifying additional hazards and updating an existing hazards analysis
  - New discrete activities or processes – a new hazard analysis may be performed for activities not previously evaluated.

Determining a Major Modification

- It is important to determine the need for a PDSA as early as feasible in planning for a modification so that actions to revise the existing safety basis documentation or develop the PDSA document may begin early in the design process.
- In many situations, the need for a PDSA may be readily discernable with little or no detailed evaluation required.
- The Standard establishes criteria for evaluating the need for a PDSA, since this is the primary outcome of a Major Modification determination. If a PDSA is warranted, the facility mod is a Major Modification.

Major Modification Evaluation Criteria		
Evaluation Criterion No.	**Evaluation Criteria**	**Clarifying Detail / Examples**
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 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 impact any SC or SS 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 SC or SS safety functions or associated SSC (e.g., structural qualification, evacuation egress path, fire suppression spray pattern) or safety analysis assumptions. Changes that may involve adverse impacts require careful attention to maintaining adherence to applicable engineering standards and nuclear safety design criteria.
3	Change an existing process or add a new process resulting in the need for a safety basis change requiring DOE approval?	A change to an existing process may negatively affect the efficacy of an approved set of safety controls for a given event or accident. Likewise potential safety concerns associated with a new process may not be adequately addressed by the existing approved control sets. In this case, it is assumed that the existing analyses addressed the hazards associated with the new or revised process, but the specified control set(s) may no longer be valid. The evaluation of any new hazards introduced by the revised or new process should be addressed via Criterion 6
4	Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?	This assessment should include consideration of the impact that the use of new technology (including technology scale-up issues) or GFE may have on the ability to specify the applicable nuclear safety design criteria with a high degree of certainty in the early stages of the project. Additionally, refer to GFE discussion in Section 9**.3**. GFE may have a technical baseline that is not directly and fully supportive of the project functional and performance requirements. An example would be employing a new technology for removal of certain nuclides from a waste stream.
5	Create the need for new or revised Safety SSCs?	Consideration should be given to the relative complexity of the controls and the ease with which the controls can be implemented. The use of a complicated multi-channel Safety Class seismically qualified instrumented system to provide multiple interlock and alarm functions would typically pose a higher risk to the project than the use of a Safety Significant passive design feature. The degree of design and regulatory uncertainty should be addressed for this criterion for the development, review, and approval of new or revised safety analysis and attendant controls (e.g., presence of multiple regulatory/technical agencies on a single project).
6	Involve a hazard not previously evaluated in the 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.

SDS for Major Modification

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

Other Modifications

- A facility modification that does not qualify as a major modification may require a safety analysis and approval by DOE to implement the modification if it represents a positive USQD
- There is need to effectively interface with the existing facility for any modification activities

Interface with Existing Facilities

- Existing construction work control processes should fully implement the guiding principles and core functions of the Integrated Safety Management System to ensure:
  - The scope of work is clearly defined for the overall project and individual activity-level work documents.
  - Additional compensatory measures are implemented, as appropriate, to clearly identify system and work scope boundaries (e.g., signs, ribbons, physical barriers).

Interface with Existing Facilities (cont'd)

- Operations authorization is required for all construction work activities within the facility in accordance with plan-of-the-week and plan-of-the-day requirements, or equivalent.
- Work control processes fully identify and analyze hazards, particularly for those activities that can impact existing SSCs.
- Line management, both construction and facility, demonstrate ownership of safety.
- Roles and responsibilities for construction and facility personnel are defined and understood, particularly with respect to response of workers to alarms, facility training, oversight and supervision, and stop work authority.

Work Planning

- During the work planning process it is necessary to determine the methods and processes by which the modifications will be constructed or installed to evaluate:
  - effect of additional wall penetrations;
  - increased or decreased loading on existing SSCs;
  - capability of existing support systems to carry additional load demand (e.g., electrical, steam, air); and
  - effects of startup testing of new components in conjunction with existing facility systems.

Conclusion

- DOE-STD-1189 provides processes for achieving safety-in-design based on:
  - An SDS that communicates safety policies, philosophies, major safety requirements, and safety goals to guide the design process
  - Establishing an SDIT that is involved in early project decisions
  - Identification of potential design-affecting provisions and considerations during conceptual design
  - Developing early safety documentation that supports design decisions and demonstrates adequate integration of safety