DOE-STD-1189-2008, *INTEGRATION OF SAFETY INTO THE DESIGN PROCESS*

An overview of the March 2008 Issued Standard and Lessons Learned

*Brad Evans*, Pacific Northwest National Laboratory

*Bob Lowrie*, Washington Safety Management Solutions

*Richard Englehart*, Longenecker and Associates

INFORMATION RELEASE PNNL-SA-55345
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 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.

– Deputy Secretary of Energy, December 5, 2005
PURPOSE

- DOE Standard 1189 has been developed to show how project management, engineering design, and safety analyses can interact to successfully implement the Deputy Secretary’s expectations.
- This class provides the central ideas and themes of 1189 and conveys lessons learned from project implementation of the Standard.
OVERVIEW OF CLASS

- Safety-in-Design Concepts
- Applicability
- Project Integration and Planning
- Design Process
- Appendices A – C
- Facility Modifications
- Lessons Learned
- Q & A
SAFETY-IN-DESIGN CONCEPTS

Basic Precepts

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

Summary of Key Concepts and Guiding Principles

- Establishment and early involvement of integrated project teams and their coordination
- Defining the overall strategy for the project, including how safety integration is to be accomplished, and obtaining DOE approval of the strategy
- Identifying CD-1 as the key point in a project by when major safety systems and design parameters should be defined

- Establishing objective criteria for the designation and design of safety structures, systems, and components
- A conservative front-end approach to safety-in-design that is reflected by a “risk and opportunities” assessment
- Identifying key project interfaces (physical and programmatic) that affect design decisions
- Ongoing involvement of regulator(s) in safety-in-design decisions
APPLICABILITY

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

- New DOE hazard category (HC) 1, 2, and 3 nuclear facilities
- Major modifications to DOE HC 1, 2, and 3 nuclear facilities (as defined by 10 CFR 830)
- Other modifications to DOE HC 1, 2, and 3 nuclear facilities managed under the requirements of DOE O 413.3A
CONTINGENCIES THROUGHOUT PROJECT

Legend
- Project Performance Uncertainties
- Safety Uncertainties

Risk and Opportunity Options

Project Contingency ($)

Project Phases

CD-0  CD-1  CD-2  CD-3
SAFETY AND DESIGN INTEGRATION

Project Integration and Planning
KEY COMPONENTS OF PROJECT INTEGRATION AND PLANNING

- Federal Integrated Project Team
- Contractor Integrated Project Team
- Safety Design Integration Team
- Safety Design Strategy
- DOE and Contractor Roles and Responsibilities
- Tailoring
Federal Project Director leads an Integrated Project Team (IPT) whose membership should represent the business and technical disciplines necessary for successful execution of the project.

Subgroups to the Federal IPT may be chartered, and should include a Contractor IPT led by the contractor Project Manager (frequently, the contractor develops a project team with similar membership to the Federal IPT).

Roles, responsibilities, and functions of the Federal IPT are provided in the Office of Engineering and Construction Management (OECM) Project Management Practices, *Integrated Project Teams*. 
WHAT IS THE CONTRACTOR INTEGRATED PROJECT TEAM?

- Standard encourages the formation of the Contractor IPT; similar makeup to Federal IPT
- Contractor IPT is comprised of personnel 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 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 SAFETY DESIGN INTEGRATION TEAM?

- Formed to support the IPT (Federal and Contractor)
- Working-level integration of safety into design for the project
- Usually composed of subset of Contractor IPT plus other specialties as needed
- Core team
  - Safety
  - Design
  - Operations
- Additional composition depends on the hazards, safety, and security issues
SDIT OBJECTIVES

- Identify and analyze hazards in the facility
- Draft the project Safety Design Strategy
- 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
- May be fulfilled by the CIPT or Project Safety Lead for small or simple projects
An Example Contractor Integrated Project Team Organization

Vice President - Operational Unit of a Contractor Organization

Federal Integrated Project Team

Project Director

Quality Assurance

Safety & Health¹

Radiation Protection¹

Nuclear Safety¹,²

Fire Protection¹

Chief Engineer¹ (Design Authority)

Equipment/Process¹ Engineering

Facility Engineering¹

Start-up Manager (future)

Transportation Safety

Architect/Eng.¹ (Design Agent) (future)

Project Controls

Project¹ Management

Planning & Projects

Operations¹ Manager

Analytical Services

Safeguards and Security

TRU Program

Environmental/Permitting

Procurement/Material Management

¹ Member of Safety Design Integration Team
² Integrated Project Team Safety Lead
DOE O 413.3A, Chg 1, allows tailoring of the Critical Decision 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.

“As established in the tailoring strategy for the project, the information and approvals for documentation, as required by this Standard, can be sequenced, organized, and bundled as the project team desires to meet the safety performance measures in this Standard”
“Tailoring of the safety design basis development steps and documents for a project is also permitted based on the level of risk posed by the facility chemical and radiological hazards, the complexity of the processing operations, and the scope of the hazards analysis required for the project”
“A Safety Design Strategy (SDS) must be developed for all projects subject to this Standard.”

This includes:

- new DOE HC 1, 2, and 3 nuclear facilities,
- major modifications to DOE HC 1, 2, 3 nuclear facilities as defined by 10 CFR 830, and
- other modifications to DOE HC 1, 2, and 3 nuclear facilities managed under the requirements of DOE O 413.3A
SDS BASIS AND PURPOSE

The SDS is based on the DOE expectations for execution of safety activities developed to support the statement of mission need during mission need.

The SDS provides preliminary information to gauge the scope of significant hazards and the general strategy for addressing those hazards.

The SDS guides design, documents the safety analysis approach, and establishes concurrence on major safety decisions related to project cost and schedule.

The SDS provides a single source for project safety policies, philosophies, major safety requirements, and safety goals to maintain alignment of safety with the design basis during project evolution.
The SDS should address at minimum the following main attributes of safety integration as the project progresses through project planning and execution:

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

- DOE communicates its expectations for safety-in-design in the context of the mission need.
- The SDIT develops the SDS as early in the conceptual design phase as is practical to address DOE expectations.
- The SDS addresses the safety integration attributes in the context of the project’s tailoring strategy - 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.
- The DOE Safety Basis Approval Authority and the Federal Project Director formally approve the SDS (with advice of the Chief of Nuclear Safety or the Chief of Defense Nuclear Safety).
SDS UPDATES

► Updates to the SDS should focus on those major safety decisions that influence project cost (e.g., seismic design criteria, confinement ventilation, safety functional classification, and strategy)

► Interim SDS updates can provide a means by which all parties are kept informed of important changes due to safety in design evolution between Critical Decision points
SDS FORMAT AND CONTENT

- Described in Appendix E
- 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 and Design Integration
DOE-STD-1189-2008

Design Process by Project Phase
PRE-CONCEPTUAL PHASE

CD-0, Establish Mission Need

Program and Project Management

- Mission Requirements
- Program Requirements Document (NNSA only)
- Initial Alternatives Analysis

Mission Needs Statement → CD-0 Approval

Project Engineering

Safety Design Basis

- Identify Safety Hazards 3.1
- Pre-conceptual Hazards Analysis and Categorization 3.1
- Safety in Design Tailoring Strategy 3.1

DOE Expectations for Safety in Design 3.1 → A
Objective is to identify and assess a program gap, compare that gap to the strategic plan, and then to propose a project to close the mission related performance gap.

Analysis focus:
- Special Safety Requirements
- New facility or modification
- Available technology
- Process material inputs and outputs
- Upper level facility functions.

Results in development of Mission Need which becomes a baseline document in project if CD-0 is granted.
SAFETY-RELATED ACTIVITIES IN PRECONCEPTUAL PHASE

- Assign project safety lead (establishes continuity)
- Establish Mission Requirements (upper-level functions and performance requirements)
- Identify top level hazards (including process inputs and outputs)
- Develop high-level hazard analysis (may be associated with particular approaches or alternatives)
- Determine preliminary hazard categorization
- Develop Tailoring Strategy
- DOE formally establishes Expectations (pre-cursor to Safety Design Strategy)
- Identify project interfaces that are critical for the project and which may drive cost/schedule/solution (e.g., security)
CONCEPTUAL DESIGN PHASE

- Goal for safety-in-design in this phase is to evaluate alternative design concepts, prepare the SDS, and provide a conservative design basis for the preferred concept.
- Perform sufficient analysis to make informed safety decisions for this phase.
- Document risks and opportunities for selections including cost and schedule range impacts.
- Begin considerations of quality requirements (QAP established).
- This is the best opportunity for safety analysis to cost effectively influence the design.
KEY SAFETY-RELATED ACTIVITIES

- Form Integrated Project Teams (both DOE and Contractor) and Safety Design Integration Team
- Assess security vulnerability
- Develop Safety Design Strategy (include considerations from other stakeholders such as security)
- Establish configuration management to maintain consistency among the various concepts and their supporting documentation
- Evaluate alternatives and provide recommendation
- Assess risks and opportunities as safety-related input to the Risk Management Plan
KEY SAFETY-RELATED ACTIVITIES (CONT’D.)

- Develop preliminary hazard analysis (PHA) for recommended alternative
  - Define safety functions
  - Identify high-cost safety systems
  - Initiate hazard analysis data capture (Appendix G)
- Identify facility-level design basis accidents (DBAs)
  - Bounding consequences
  - Safety and seismic classification
- Commit to nuclear safety design requirements (DOE O 420.1B)
- Develop Conceptual Safety Design Report (CSDR)
- Maintain project interfaces focus
DESIGN BASIS ACCIDENTS (DBAs)

- Simple DBAs 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)

- Establishes the facility preliminary hazard category
- Preliminary identification of hazards (PHA) and facility-level DBAs
- Assess the need for safety-related facility-level controls (based on the PHA / DBAs)
- Preliminary assessment of appropriate seismic design criteria
- Commitment to nuclear safety design criteria
- Format and content of CSDR in Appendix H
Preliminary Hazard Categorization per DOE-STD-1027

DBAs – Summary Table
- DBAs are a key part of integrating safety and design
- Addresses major systems with significant cost/schedule implications (facility structure, confinement, fire protection, emergency power, etc.).

Security Implications

Nuclear Safety Design Criteria

Plan for moving forward
- Considerations include planned studies or analyses, risks and opportunities, and lessons to be learned.
CONCEPTUAL SAFETY VALIDATION REPORT (CSVR)

DOE prepares the CSVR to confirm the preliminary safety positions constitute an appropriately conservative basis to proceed to preliminary design, based on:

- preliminary hazard categorization of the facility;
- preliminary identification of facility DBA;
- assessment of the need for SC and SS facility-level hazard controls;
- preliminary assessment of the appropriate seismic design basis for the facility structure and major hazard controls; and
- position(s) taken with respect to compliance with the safety design criteria of DOE O 420.1B.
PRELIMINARY DESIGN PHASE

Pre-CD-2, Preliminary Design

Program and Project Management
- CD-1 Approval
- Update Security Vulnerability Assessment
- Update Project Risk Considerations
- Update Risk Management Plan
- Establish Technical, Cost, & Schedule Baseline
- CD-2 Preliminary Design Package
- Baseline Validation Independent Review
- DOE Approves Technical, Cost, & Schedule Baseline

Project Engineering
- Initiate Preliminary Design
- Identify Detailed Nuclear Safety Design Criteria
  DOE O 420.1
- Validate Design vs. Desired Control Functions & Criteria
- Update Safety in Design Risk & Opportunities Assessment
- Develop Design Output Documents
- Design Reviews (Fed and/or Contractor, as appropriate)

Safety Design Basis
- Hazards Analysis
- System Level DBA Unmitigated Analysis
- Update Safety SSC Functions and Classification
- Preliminary Safety Validation Report
- PSDR
- Updated SDS, as needed
- Preliminary Safety Validation Report

38
PRELIMINARY DESIGN PHASE

- Advance conceptual design toward final design
- Evolve the HA to include facility worker protection
- Design specific solutions are developed based on safety design requirements
- Prepare for final design
- NEPA documentation is complete
SAFETY ACTIVITIES IN PRELIMINARY DESIGN

- Update Security Vulnerability Assessment
- Update hazard analysis (HA) to address process level hazards based on the selected design
- Evaluate and apply DOE O 420.1B and associated Guide design requirements
- Evolve system-level DBAs with appropriate added specificity based on selected design
- Update Risk and Opportunity Assessment
- Update SDS reflecting design and safety evolution
- Develop the Preliminary Safety Design Report (PSDR)
HAZARD ANALYSIS AT THE PROCESS LEVEL

- The HA evolves from facility level PHA
- The HA reflects the actual design
- Hazard analysis & design iteration
  - HA activities support identification of safety functions and selection of DBAs
  - DBAs and safety function support design selection and associated design criteria
  - Design selection / criteria support development of a refined HA for the PSDR
  - Several iterations may be necessary occur as preliminary design progresses
  - Hazard Analysis table updated as necessary
DBAS IN PRELIMINARY DESIGN

The DBAs:

- Refined from Conceptual Design based on system design
- Provides input for new or revised design criteria
- Establishes system-level safety classification

DBAs are selected based on safety function and magnitude of hazard but, as in conceptual design, are not limited based on consequence (do not have to have a public impact to be selected)
SAFETY INTERFACE WITH DESIGN

► Assist designers in understanding and addressing
  ■ 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 System Design Descriptions (SDDs) and SSC design
  ■ System boundaries
  ■ Safety functions and requirements
  ■ Supporting analyses

► Project design reviews
  ■ Include safety design basis information, including information included in design products (e.g., SDDs)
PRELIMINARY SAFETY DESIGN REPORT (PSDR)

- Developed to support safety adequacy of the preliminary design effort
- Limited to the extent that design information is also limited
- Format and content guide in Appendix I
- Preliminary SVR prepared by DOE to approve PSDR
- Similar to CSVR in purpose and scope
FINAL DESIGN PHASE

Pre-CD-3, Final Design

Program and Project Management
- CD-2 Approval
- Update Project Risk Considerations
- Update Risk Management Plan
- Baseline Management
- CD-3 Final Design Package
- Execution Readiness Independent Review
- DOE Authorizes Procurement, Construction, & Final Implementation
- CD-3 Approval

Project Engineering
- Initiate Final Design
- Validate Design vs. Desired Control Functions & Criteria 3.4
- Update Safety in Design Risk & Opportunities Assessment 3.4
- Develop Design Output Documents
- Design Reviews (Fed/or Contractor, as appropriate)
- Construction, Transition, & Closeout 7.0

Safety Design Basis
- Update Hazards Analysis 4.4
- Mitigated Accident Analysis 4.4
- Update Safety SSC Functions and Classification 4.4
- PDSA 4.4
- Updated SDS, as needed 2.3
- Safety Evaluation Report

DOE Authorizes Procurement, Construction, & Final Implementation
FINAL DESIGN

- The final design stage completes the design
- Finalize HA and DBAs (mitigated analysis)
- Evolves the preliminary design to the point where
  - Specifications are developed
  - Security Vulnerability Assessment is finalized
  - Procurement and construction can be accomplished
  - Test, inspection, and commissioning requirements are developed and detailed
  - SDDs and FDD (or appropriate design basis documentation) are completed
MITIGATED ACCIDENT ANALYSIS

What do we mean by this?
- DBAs developed earlier define unmitigated consequences to assist in safety classification
- DBAs also defined design requirements
- Together, these provide the “design basis” for the facility

Mitigated accident analysis maintains the design basis of facility SSC while meeting need for final accident analysis supporting facility operation
PRELIMINARY DOCUMENTED SAFETY ANALYSIS (PDSA)

- Evolves from the PSDR
- Completes the analysis of the design
- Format and content covered in Appendix I
  - Based on DOE-STD-3009
  - Minimizes need to rewrite for DSA
- Provides the basis for design adequacy with respect to nuclear safety
- Change control established
“DESIGN SAFETY ANALYSIS”

- Based on DOE G 420.1-1
- Supports the position that the design satisfies nuclear safety design criteria and derived safety requirements
- May reside outside the PDSA proper with results summarized and referenced; examples:
  - SDD (for active safety SSCs)
  - FDD (could be used for passive safety SSCs or to consolidate systems that provide a single safety function)
CONSTRUCTION / TRANSITION / CLOSEOUT PHASE
DESIGN RELATED ISSUES

- Field Changes
- GFE and other equipment not part of primary design
- Revisions to PDSA
- Changes to comply with readiness review issues
- Input to DSA and TSR
CRITERIA FOR DETERMINING PDSA REVISION

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

- Safety in design is supported by specific actions in each project phase, which evolve the safety basis and design.
- The safety in design process is guided by the development and use of the SDS.
- Documentation at each design phase is through preparation of safety design documents (CSDR, PSDR, and PDSA).
- DOE-STD-1189 provides guidance for each of these products and discusses processes to help achieve design integration.
- The Key Concepts and Guiding Principles provide the overarching guidance throughout this process.
SAFETY AND DESIGN INTEGRATION
DOE-STD-1189-2008

Appendix A – Safety System Design Criteria
PURPOSE

Provides objective criteria requirements for specification of the seismic design basis and for safety classifications of SSCs

- Seismic design basis includes specification of seismic design classification (SDC) and limit state (LS) for an SSC based on radiological hazards
- Adds collocated worker Safety Significant radiological classification criterion along with Safety Class criterion for the public
SEISMIC DESIGN BASIS

Applies recently published national standards for seismic design of non-reactor nuclear facilities

- ANSI/ANS 2.26-2004, *Categorization of Nuclear Facility Structures, Systems and Components for Seismic Design*; and

SEISMIC DESIGN STANDARDS

- ANSI/ANS 2.26 provides seismic design bases (SDC and LS) for SSCs based on unmitigated radiological dose (as modified by DOE) to collocated workers and to the public and on the safety function of the SSC.

- ASCE/SEI 43-05 provides the design criteria to use with the seismic design basis.
**GUIDANCE FOR SEISMIC DESIGN CRITERIA**

<table>
<thead>
<tr>
<th>Category</th>
<th>Collocated Worker*</th>
<th>Public*</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDC-1</td>
<td>Dose &lt; 5 rem</td>
<td>Not applicable – Defaults to SDC-1</td>
</tr>
<tr>
<td>SDC-2</td>
<td>5 rem &lt; dose &lt; 100 rem</td>
<td>5 rem &lt; Dose &lt; 25 rem</td>
</tr>
<tr>
<td>SDC-3</td>
<td>100 rem &lt; dose</td>
<td>25 rem &lt; dose</td>
</tr>
</tbody>
</table>

* Using the safety classification methodology for public and collocated workers

If the quantitative public criterion for SDC-3 of Table A-1 is exceeded significantly for any project (between one and two orders of magnitude), then the possibility that SDC-4 should be invoked must be considered on a case-by-case basis.
## LIMIT STATES (EXAMPLES)

<table>
<thead>
<tr>
<th>SSC Type</th>
<th>Limit State A</th>
<th>Limit State B</th>
<th>Limit State C</th>
<th>Limit State D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building structural components</td>
<td>Substantial loss of SSC stiffness; some margin against collapse</td>
<td>Some loss of SSC stiffness; substantial margin against collapse</td>
<td>SSC retains nearly full stiffness and strength; passive components will perform normal and safety functions</td>
<td>SSC damage is negligible</td>
</tr>
<tr>
<td>Structures or vessels for containing hazardous material</td>
<td>Low hazardous material; vessel not likely to be repairable</td>
<td>Moderate hazardous liquids; cleanup and repair expeditious</td>
<td>Low pressure vessels with worker hazard if contents released; damage minor</td>
<td>Leak tightness must be assured; moderate to high hazard gases/liquids</td>
</tr>
</tbody>
</table>

Other SSCs covered include: confinement barriers (glove boxes, ducts), equipment support structures, filter assemblies and housings, etc.
COMPARISON TO PERFORMANCE CATEGORY
SUPPLEMENTAL GUIDANCE FOR ANS 2.26 WHEN SELECTING SDCS AND LIMIT STATES (SDB)

- Safety analyst, seismic design engineer and the equipment design engineer should work together and evaluate the functional requirements for the SSC and its subcomponents to determine the appropriate SDB.

- If the safety functions of an SSC include confinement and leak tightness, irrespective of the Seismic Design Category (SDC) of the SSC, following the intent of Section 5 of ANS 2.26, a Limit State C or D must be selected.

- Guidance for an SDC-1 or SDC-2 SSC having safety functions requiring Limit States A, B, C or D.
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 (5 to 25 rem), 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 100 rem TEDE at 100 m
- Use ICRP 68 dose conversion factors
- Apply $\chi/Q$ value at 100 m of $3.5E-3$ sec/m$^3$ 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 FOR MAJOR MODIFICATIONS

- For major modifications of existing facilities, Appendix A criteria are applicable.
- Backfit analyses should examine:
  - The need to upgrade interfacing structures, systems, and components in accordance with these criteria, and
  - Whether there should be relief for the modification from the design requirements that application of these criteria in design would imply.
ANS 2.27 Criteria for Investigations of Nuclear Facility Sites for Seismic Hazard Assessments and ANS 2.29 Probabilistic Seismic Hazards Analysis have been completed and approved.

DOE plans to adopt them and to update DOE G 420.1-2 (NPH guide) apparently are in flux.

EM and NNSA working on NPH chemical hazard criteria
SAFETY AND DESIGN INTEGRATION
DOE-STD-1189-2008

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, but the Standard does provide *advisory* chemical safety criteria.

- The guidance provides a sense of scale as to what is meant by a “significant exposure” in the criterion for classifying SSCs as safety significant.

Note: DNFBS has advised DOE to consider the need to effectively implement controls for chemical hazards, including guidance on the design of hazard controls (ref. letter dated 2/22/08, Eggenberger to Sell).
Guidance for consideration of Safety Significant designation of SSCs for significant chemical exposures is 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

Note: Chemical exposure for facility workers is addressed in Appendix C.
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 FOR SAFETY SIGNIFICANT CLASSIFICATION

► Public
  ■ Exposure > AEGL-2/ERPG-2/TEEL-2
    ● Potential for irreversible or serious long-lasting health effects

► Collocated Worker
  ■ Exposure > AEGL-3/ERPG-3/TEEL-3
    ● Potential for life threatening health effects or death

► Hierarchy
  ■ Acute Exposure Guideline Levels (AEGL, EPA)
  ■ Emergency Response Planning Guidelines (ERPG, AIHA)
  ■ Temporary Emergency Exposure Limits (TEEL, DOE)
DNFSB issue on design guidance for SS SSCs is being addressed

- in a new draft DOE standard implementing ANSI/ASI-84 (ISA-84), Functional Safety: Safety Instrumented Systems for the Process Industry Sector, and by a revision to DOE G 420.1-1, and

- by a revision to DOE G 420.1-1.

NNSA and EM guidance under development for NPH classification based on chemical hazard levels to the public and to workers.
SAFETY AND DESIGN INTEGRATION
DOE-STD-1189-2008

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:

- **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;
- **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.
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.

Note: SDC-3 or PC-3 classification consideration for in-facility worker protection when the worker must remain in the building for safe shutdown or other safety purpose.
SAFETY AND DESIGN INTEGRATION
DOE-STD-1189-2008

Facility Modifications
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 PROCESS

Screening Criterion
Design & Implementation of Physical Modification?

Facility Modification

Simple Modification?

N

Y

Evaluate Need For PDSA

Major Modification Involved?

Does 413.3 Apply?

Y

N

Develop SDS

- Address need for CD phases/CSDR/PSDR
- Graded PDSA
- 420.1 Design Criteria
- Interface with existing facility/construction

Tailor Per 413.3

Does 413.3 Apply?

Y

N

Execute SDS

- New / revised HA not required
- New / revised accident analysis not required
- New / revised controls not required
- Changes to SB, if needed, are descriptive only

Tailor Per 413.3

Change Control Process

Execute SDS

- SDS
- Safety Documentation
- CSDR/PSDR/PDSA not required

Integrate With Existing Facility

Execute SDS

- Possible SB Amendment

Does 413.3 Apply?

Y

N
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.
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.
<table>
<thead>
<tr>
<th>Evaluation Criterion</th>
<th>Evaluation Criteria</th>
<th>Clarifying Detail / Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add a new building or facility with a material inventory ≥ HC 3 limits or increase the HC of an existing facility?</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>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?</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>Change an existing process or add a new process resulting in the need for a safety basis change requiring DOE approval?</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Utilize new technology or GFE not currently in use or not previously formally reviewed / approved by DOE for the affected facility?</td>
<td>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.</td>
</tr>
<tr>
<td>5</td>
<td>Create the need for new or revised Safety SSCs?</td>
<td>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).</td>
</tr>
<tr>
<td>6</td>
<td>Involve a hazard not previously evaluated in the DSA?</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
For major modifications or other projects that are being incorporated into or added onto existing nuclear facilities, it is necessary to ensure that the requirements of the approved and implemented safety basis for the facility being modified are observed and protected throughout the construction and testing processes.
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.
UNREVIEWED SAFETY QUESTION (USQ) REVIEW

▶ It is necessary to ensure that all proposed project activities are reviewed against the existing safety basis using the USQ process.

▶ If the result of the USQ determination is that DOE approval is necessary, the contractor may need to establish alternate or supplemental safety basis documentation activities, such as a specific amendment to existing and implemented safety basis or a standalone interim safety basis covering construction activities, to support construction and installation.
CONCLUSION

DOE-STD-1189 provides processes for achieving safety-in-design based on:

- Establishing:
  - The Federal and Contractor IPTs and involving them in early project decisions
  - An SDIT that brings focus to safety-in-design strategy and issues
- An SDS that communicates safety policies, philosophies, major safety requirements, and safety goals to guide the design process
- Establishing objective criteria for selection of safety SSC
- Identification of potential design-affecting provisions and considerations during conceptual design (risks and opportunities)
- Developing early safety design basis documentation that supports design decisions and demonstrates adequate integration of safety
- Establishing criteria for determining the existence of a “major modification” to an existing facility
SAFETY AND DESIGN INTEGRATION
DOE-STD-1189-2008

Lessons Learned
SOURCES OF LESSONS LEARNED

- DOE Project Reviews
- DNFSB Project Reviews
- Project Implementation Experience
- Implementation Questions from Field
- Questions During 1189 Training Sessions
LESSONS LEARNED

“IF YOU TRY TO MIMIC THE LAST SUCCESSFUL PROJECT, YOU ARE DESTINED TO BE A CHAPTER IN A LESSONS LEARNED BOOK.”*

 ► Need for detailed training on STD-1189 for FPDs, safety leads, engineering leads
   - Surface level review of the Standard; focus on products (SDS, CSDR, PSDR, etc. instead of understanding the integrating process approach)
   - Project management, safety, and engineering design personnel should have a level of familiarity with the requirements and guidance relevant to the other disciplines

 ► Nuances missed in application:
   - level of HA as function of design stage;
   - nuclear criticality safety not included in HA/control identification;
   - Risk and Opportunity Assessments not carried into Project Risk Management Plan;
   - security not included in SDIT
LESSONS LEARNED

🔹 Need for formality in establishment and activities of SDIT

  Project management commitment; designation of an SDIT lead (forcing function for effective communication safety/design).

  Especially important when different contractors are doing safety work and design work.

  Communication!
LESSONS LEARNED
“BE CAREFUL ABOUT TREATING ALL PROJECTS THE SAME OR YOU MIGHT END UP AS THE POINT OF A DILBERT COMIC STRIP.”*

► Importance of a requirements management system (e.g., Dynamic Object Oriented Requirements System)
  ➢ Flowdown of functional requirements to design documentation (SDDs)
  ➢ Management of change
  ➢ Don’t’ let development of SDDs get out of sync with safety input and documentation in CSDR, PSDR, PDSA

► Need to assess/verify ability of safety SSCs to provide the safety function indicated by hazards analysis
  ➢ Compliance with safety design guidance of DOE G 420.1-1
LESSONS LEARNED

Role of the Safety Design Strategy (SDS) document

- Tailoring of CD stages and safety documentation

- Revising conservative safety assumptions with better information as design proceeds

- Real time mechanism to achieve consensus on safety in design approaches (living document)
LESSONS LEARNED

► Need for an authoritative source for “interpretations” or implementation advice for STD-1189 (HS-21)

► Need for coordinated “supplemental guidance”

- Variations in implementation guidance between NNSA and EM

- Potential for misleading or incorrect information from individuals
MISTAKES WILL HAPPEN!

“Rule: Never make the same mistake in succession. Always make at least one intervening mistake.”

Corollary: “When your goal is to keep from making a mistake, you are sure to make a doozy.”*

Every project is unique!
QUESTIONS

► What parts of the Standard are mandatory?
► Preconceptual safety planning and SDS; what can be done preconceptually?
► Facility level; process level; and component level DBAs – purpose and objectives. HA methodologies.
► Means for choosing/justifying alternative safety design criteria. Does commitment to O 420.1B criteria mean commitment to the associated guides as well?
► Level of detail of DOE review of safety design documents (CSDR/PSDR/PDSA) in meeting O 420.1B safety design requirements.
► How to modify early conservative safety design assumptions/approaches. Considerations.
WHAT PARTS OF THE STANDARD ARE MANDATORY?

► Originating with STD-1189
  - Safety Design Strategy
  - CSDR and PSDR (and DOE reviews)
  - Appendix A seismic design basis and collocated worker safety significant SSC criteria
  - Key Concepts and Guiding Principles (for full implementation of STD-1189)

► Derivative
  - 10 CFR 830
  - DOE O 413.3A Cng. 1
  - DOE O 420.1B
PRECONCEPTUAL SAFETY PLANNING AND SDS; WHAT CAN BE DONE PRECONCEPTUALLY?

▶ Guiding philosophies or assumptions to be used to develop the design
  - Commitments to STD-1189 and O 420.1B and related guidance documents
  - Confinement strategy

▶ Safety in design and safety goal considerations for the project
  - Anticipated hazard categorization
  - Major hazards involved
  - Safety in design risk identification and management
PRECONCEPTUAL SAFETY PLANNING AND SDS; WHAT CAN BE DONE PRECONCEPTUALLY?

► Approach to developing the safety design basis
  ▪ Tailoring of CD stages and associated safety documentation
  ▪ Coordination with DOE SBRT

► Significant discipline interfaces impacting safety
  ▪ Security
  ▪ Criticality
MEANS FOR CHOOSING/JUSTIFYING ALTERNATIVE SAFETY DESIGN CRITERIA

Considerations?
- Cost
- Schedule implications
- Equivalent or better outcomes/demonstration thereof

Does commitment to O 420.1B criteria mean commitment to the associated guides as well?
- Guides are not requirements (unless committed to by contract)
- DOE expectation is that guides will be followed unless a different approach is proposed and defended as appropriate (e.g., NRC Regulatory Guide expectations)
LEVEL OF DETAIL OF DOE REVIEW OF SAFETY DESIGN DOCUMENTS (CSDR/PSDR/PDSA) IN MEETING O 420.1B SAFETY DESIGN REQUIREMENTS

- A function of the stage of design

- Sufficient to identify issues that need to be addressed in the next stage (because they were overlooked or incompletely addressed)

- Acceptability of safety in design approaches so that if carried through could result in a facility design for which operations could be approved (safety basis)
HOW TO MODIFY EARLY CONSERVATIVE SAFETY DESIGN ASSUMPTIONS/APPROACHES

► Potentials for this should be identified in SDS and in the Risk and Opportunity Assessment and Project Risk Management Plan

► Modify the SDS and get approval of the update

► Considerations
  ■ Refined design inputs (process design, MAR, new information…)
  ■ Cost and schedule impacts of redesign
    • e.g., redesign of building structure for lower SDC/LS