

John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
Joseph J. DiNunno
Herbert John Cecil Kouts
John E. Mansfield

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004-2901
(202) 694-7000

99-0001917



July 8, 1999

The Honorable T. J. Glauthier
Deputy Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Mr. Glauthier:

There has been a long-standing safety practice in the design construction and operation of nuclear facilities to build-in and maintain structures, systems and components that contain or confine the radioactive materials to the work station. The establishment of requirements by the Department of Energy (DOE) to ensure such containment and confinement is authorized by statute.

Current requirements for nuclear safety design, criticality safety, fire protection and natural hazards mitigation are set forth in DOE Order 420.1, *Facility Safety*. This Order (Section 4.1.1.2), when contractually invoked, requires that:

Nuclear facilities shall be designed with the objective of providing multiple layers of protection to prevent or mitigate the unintended release of radioactive materials to the environment.

This "defense-in-depth" approach is the hallmark of nuclear facility and process designs.

For those structures, systems and components (SSCs) that will be relied upon to provide such defense-in-depth, that reliance is highly dependent upon the degree of certainty that they will function as intended, if and when, they are called upon to do so. Reliability in turn is highly dependent upon the quality built into the SSCs. While both reliability and maintainability are key considerations in all engineered structures and systems, it has been common practice in the nuclear industry to exercise special care for quality of structures, systems and components serving safety functions.

DOE has had an effort underway for some time to develop a more systematic and uniform approach to establishing such quality requirements. The effort is targeted at the specification of quality requirements commensurate with the consequences should failures occur.

The Defense Nuclear Facilities Safety Board (Board) and staff have reviewed draft guidance set forth in draft Guide 420.1-x, *Implementation Guide for Non-Reactor Safety Design Criteria*, and draft Appendix A to DOE-STD 3009-94. What this guidance advocates as a means of classifying safety structures, systems and components and specifying quality assurance measures are:

- The use of unmitigated, bounding-type, accident scenarios to calculate radiological exposures at the site boundary for purposes of safety system classification.
- Designation as “Safety Class” of any structure, system or component required to prevent exposures at the boundary from exceeding 25 rem Total Effective Dose Equivalent (TEDE).
- Designation as “Safety Significant” those safety structures, systems and components other than “Safety Class” provided for worker protection and for defense-in-depth to protect the public and the environment.
- Identification of quality ensuring Codes and Standards acceptable for the classification so identified.

The Board finds this general approach reasonable provided that it is made quite clear that the 25 rem evaluation guideline is not to be treated as a design acceptance criterion nor as justification for nullifying the general design criteria relative to defense-in-depth safety measures.

Enclosed are detailed comments prepared by the Board staff. These are offered for continued dialogue with the DOE staff who have been advancing this guidance effort.

It is important to note that protection against undesired consequences is assured through the defense-in-depth provided by engineering and administrative controls in the Technical Safety Requirements (TSRs), and additionally, through the use of manuals of practice, where protection of the public and workers is extended to prevention of accidents, and to further reduction of the consequences of accidents should they occur. The Board suggests that DOE-STD-3009-94 or its proposed Appendix A refer to the safety measures included in these manuals of practice. DOE should recognize its responsibility to ensure that designation of TSRs according to DOE-STD-3009-94 and the safety measures in the manuals of practice together form a unified safety structure.

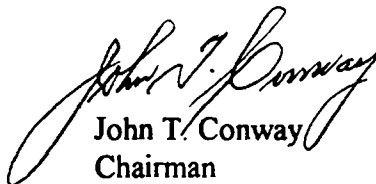
Additionally, the Board believes that the design of new hazard category 2 and 3 nonreactor nuclear facilities should be based on confining the hazardous radioactive materials during normal operation and potential accidents as required by DOE O 420.1, *Facility Safety*.

However, the Order should note that the confinement systems should be tailored according to the facilities' level of hazard and the principles of an Integrated Safety Management System and classified as safety-class or safety-significant SSCs. The design requirements for these classes of SSCs are given in DOE G 420.1.

The Board notes that the approach and guidance for selection of safety SSCs and defense-in-depth considerations described in these guidance documents are consistent with the approach used by the Savannah River Site (SRS) in establishing safety measures for the Consolidated Tritium Facilities. The Board acknowledged the SRS approach to identification of controls and use of the defense-in-depth concept in a letter to DOE dated March 18, 1999.

If you have any questions on this matter, please contact me.

Sincerely,



John T. Conway
Chairman

c: The Honorable Victor H. Reis
The Honorable David Michaels
Mark B. Whitaker, Jr.

Enclosures

Enclosure 1**DNFSB Comments on Chapter 2 of the Implementation Guide to DOE Order 420.1,
Facility Safety**

Draft forwarded by DOE letter dated January 29, 1999.

1. The following change to the second sentence of section 2.1, **Design Process and Safety Analysis Relationship**, is provided to emphasize the implementation of integrated safety management systems during the design phase:

In this section, the relationship between the facility design process and the parallel development of the facility safety analysis is discussed. Continuous coordination is necessary between these two activities throughout the project to ensure that the principles of integrated safety management systems as described in DOE P 450.4 and DOE G 450.4-1 are implemented and the final design meets the mission requirements and includes the required safety features. The safety analysis shall be performed in accordance with the guidance in DOE-STD-3009-94 and the requirements of DOE O 5480.23 to develop and validate the functional and performance requirements for the safety SSCs.

2. The following changes to section 2.1.3, **Safety-Significant SSCs**, are provided to better define the classification of SSCs to protect workers from significant radiological or chemical exposures.

2.1.3 Safety-Significant SSCs

The following paragraphs constitute the current definition of Safety-Significant SSCs as presented in DOE-STD-3009-94. Together with the discussions of defense-in-depth of Section 2.3 of this Guide, they provide guidance for the identification of Safety-Significant SSCs.

Safety-Significant structures, systems, and components (Safety-Significant SSCs) are structures, systems, and components not designated as Safety-Class SSCs, but whose preventive or mitigative function is a major contributor to defense-in-depth (i.e., prevention of uncontrolled material releases) and/or worker safety as determined from hazard analysis.

As a rule of thumb, Safety-Significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in irreversible consequences to workers. Irreversible consequences are defined to be prompt fatality, serious injuries, or significant radiological or chemical exposures. Serious injuries, as used in this definition, refer to immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb). Significant potential effects of exposure or uptake of radiologically or chemically hazardous materials should be considered for identification of Safety-Significant SSCs using qualitative estimates of the consequences.

The general rule of thumb cited above is not an evaluation guideline. It is a lower threshold of concern for which Safety-Significant SSC designation may be warranted, not a quantitative criteria. Estimates of worker consequences for the purpose of a Safety-Significant SSC designation are not intended to require detailed analytical modeling due to the uncertainties in the analysis, especially for the facility workers. Considerations should be based on engineering judgment and expert elicitation of possible effects and the potential added value of Safety-Significant SSC designation. Experience has shown that Safety-Significant SSCs identified through defense-in-depth considerations also provide safety for workers.

3. The other sections of the Implementation Guide should be revised to be consistent with the change to section 2.1.3. The definition for Evaluation Guideline should be revised to eliminate reference to a specific numerical value because the value is now provided in section 2.1.2 in context for selection of Safety-Class SSCs.

Enclosure 2**DNFSB Comments on DOE-STD-3009-94 and its Appendix A**

Draft forwarded by DOE letter dated January 29, 1999.

I. Comments on Appendix A:

1. The draft Section 2.1.2 of the Implementation Guide to DOE O 420.1 contains statements such as: "If the resulting site boundary dose approaches the Evaluation Guideline, then the candidate SSC need to be evaluated to see if ...being designed as Safety-Class." And "If unmitigated dose results are in the rem range, then serious consideration should be given to identifying related safety SSCs as Safety-Class. In most cases it will be found that mitigating Safety-Class SSCs effectively reduce offsite doses far below 25 rem. Especially considering this, it should emphatically be understood that 25 rem is not an acceptance criterion for safety design." These statements are more conservative and favorable to the Board than statements in the draft Appendix A such as "If EG values are exceeded by the unmitigated consequences or a release scenario, a need for Safety-Class SSC designation is indicated." Draft Appendix A should be made consistent with the approach presented in the Implementation Guide.
2. The revisions to section 2.1.3, Safety-Significant SSCs, provided in Enclosure 1 should also be included in Appendix A and the body of DOE-STD-3009, as appropriate.

II. Comments on the Standard, DOE-STD-3009-94:

1. The first paragraph under *Guiding Principles* in the Foreword should be revised to include application of Integrated Safety Management System as follows:

This standard should be applied consistent with the policy and guidance provided in DOE P 450.4, Safety Management Systems Policy, and DOE G 450.4-1, Safety Management Systems Guide, to ensure that safety is integrated in all aspects of defense nuclear facilities' activities. This Standard incorporates and integrates many different approaches regarding safety analysis report format and content. To ensure a consistent application of this Standard among users, the following guiding principles are provided.

2. The first paragraph under *Purpose of DOE-STD-3009-94* in the Introduction should be revised as follows:

This Standard describes a SAR preparation method that is acceptable to the DOE. It was developed to assist Hazard Category 2 and 3 facilities in preparing SARs that will satisfy the requirements of DOE O 5480.23, "Nuclear Safety Analysis Reports" and are consistent with the requirements of DOE P 450.4, Safety Management Systems Policy. Hazard Category 1 facilities are typically expected to be Category A reactors for which extensive precedents for SARs already exist.

3. The section on Worker Safety under *SAR Preparation Conceptual Basis and Process* in the Introduction should be revised to emphasize worker protection through proper training and use of procedures and manuals of practice as follows:

Worker Safety

Workers, typically those in proximity to operations, are the population principally at risk from potential consequences associated with Hazard Category 2 and 3 facilities. DOE recognizes, via DOE O 5480.23, the importance of including worker safety in safety analyses by specifically noting the worker as a population of concern. This represents a new emphasis for SARs, which have traditionally focused on potential consequences to the public. Accordingly, developing a conceptual basis for the methodology used in this Standard requires answering the fundamental question of how worker safety is most appropriately addressed in the SAR.

An important element of worker protection is provided by the contractor or the operating organization in training the operators and preparing an adequate set of procedures and manuals of practice. The workers, especially the facility workers, are protected through implementation of the manuals and codes of practice that are derived from DOE rules and Orders such as 10 CFR 835 and DOE O 440.1, or application of standard industry practices.

The Occupational Health and Safety Administration (OSHA) has recently published 10 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals." The purpose of this regulation is defined by OSHA in summary fashion as, "Employees have been and continue to be exposed to the hazards of toxicity, fires, and explosions from catastrophic releases of highly hazardous chemicals in their workplaces. The requirements in this standard are intended to eliminate or mitigate the consequences of such releases." Many of the topics requiring coverage in this federal regulation, such as design codes and standards, process hazard analysis, human factors, training, etc., are directly parallel to the topics addressed by DOE O 5480.23. The regulation also provides overall integration of these topics.

DOE O 440.1 and the OSHA standard address the issue of worker safety from process accidents by requiring the performance of hazards analyses for processes (exclusive of standard industrial hazards) in conjunction with implementation of basic safety programs that discipline operations and ensure judgments made in hazard analyses are supported by actual operating conditions. These requirements effectively integrate programs and analyses into an overall safety management structure without requiring quantitative risk assessment. This integration and the basic concepts of Process Safety Management (PSM) described above are philosophically accepted as appropriate for SARs. This Standard effectively merges PSM principles with traditional nuclear SAR precepts.

4. The following statement in the Safety-Class SSC Subsection to the Section on TSR and SSC commitment should be deleted: "Safety-Class SSC's normally will not be associated with Hazard Category 2 and 3 Facilities due to their limited potential for offsite impact."