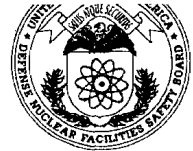


John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
John W. Crawford, Jr.
Joseph J. DiNunno
Herbert John Cecil Kouts

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004
(202) 208-6400

96-0003947



October 2, 1996

The Honorable Thomas P. Grumbly
Under Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

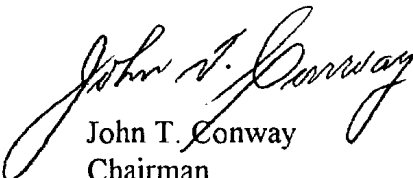
Dear Mr. Grumbly:

Consistent with the Implementation Plan for Defense Nuclear Facilities Safety Board (Board) Recommendation 95-2, the Department of Energy (DOE) and some of its contractors made presentations to the Board on the contractors' approaches to implementing Integrated Safety Management Systems (ISMS) at ten priority facilities. While some projects are progressing more rapidly than others, an encouraging start is evident overall. The enclosure provides comments on what appear to be particularly effective and useful practices discussed by the contractors and others. These comments are presented for consideration in developing guidance for the Recommendation 95-2 implementation efforts.

The objective of ISMS is to protect the public, workers, the environment, and essential facilities while executing the missions of DOE. The scope of work involved in such missions can include research, development, demonstration, production (including dismantlement of weapons), and maintenance, as well as deactivation and decommissioning of facilities no longer needed. Because of the broad spectrum of activities and facilities, ISMS need to be appropriately tailored to be practical and effective. Thus, the comments in the enclosure do not necessarily apply to all situations.

Please contact me if you have any questions.

Sincerely,


John T. Conway
Chairman

Enclosure

OBSERVATIONS ON BEST PRACTICES IN IMPLEMENTING INTEGRATED SAFETY MANAGEMENT SYSTEMS

The following comments focus primarily on Integrated Safety Management Systems (ISMS) being developed by various Department of Energy (DOE) contractors, rather than the DOE review and approval of the ISMS. Many of the observations are based on presentations by personnel from the Los Alamos National Laboratory (LANL) at the institution level and TA-55, the Pantex Plant, and the Savannah River Site (SRS) during the months of June and July 1996.

General Comments

- The greatest progress seems to have been made by organizations that take positive, constructive approaches and where ISMS development is directed most forcefully by line management.
- The most successful approaches recognize that successful development of ISMS includes:
 - (1) The early identification of appropriate standards and requirements at the institution, facility, and activity levels through safety and hazards assessments and by other means.
 - (2) Assurance that standards and requirements, along with any additional necessary controls, are implemented and adhered to at the activity/worker level.
- Employee safety awareness and empowerment were correctly noted by some as essential to safe operations.

Safety Management Functions

The Implementation Plan for Recommendation 95-2 identifies the following safety management functions: (1) define scope of work, (2) analyze hazards, (3) develop/implement controls, (4) perform the work, and (5) provide feedback/improvement.

- Following the hazards identification and assessment of the “analyze hazards” phase, actions focused on risk reduction (not risk rationalization) are very important to ensuring safety. Several presenters noted that risk reduction often requires iteration among the “define scope of work,” “analyze hazards,” and “develop/implement controls” functions.
- LANL, Pantex, and others emphasized that an ISMS must be “layered” to assure proper integration of controls at a facility where there is a diversity of work. At LANL this is reflected by the “nested and converging” 95-2 ring model. At Pantex this is reflected by

the pyramid of the Essential Standards Program, with the three layers of interchangeable segments (Activity, Process/Facility, Site-Level).

- Both LANL and Pantex seem to have placed appropriate emphasis on the need for “activity-specific” safety management, including specific “process hazard analysis” [e.g., Hazard Analysis Reports (HARs) for assembly/disassembly work at Pantex].
- The Process Hazards Analyses methodologies listed by OSHA in 29 CFR 1910.119, *Occupational Safety and Health Standard* [namely What-if, Checklist, What-If/Checklist, Hazard and Operability Study (HAZOP), Failure Mode and Effects Analysis (FMEA), or Fault Tree Analysis] are sometimes appropriate for activities at defense nuclear facilities. Typically, however, DOE contractors apply these methods to quantities of hazardous materials far below the threshold levels of 29 CFR 1910.119.
- Pantex (in briefing the Board on site, after the formal 95-2 meeting) found it necessary to modify the 95-2 ring model to demonstrate that certain aspects of its safety management program needed special emphasis. They separated “Identify and Implement Controls” into two separate steps (“Identify” and “Implement”), since these are two very distinct efforts. They also added a separate “Confirm Readiness” element, as this has become a major, independent, and important precursor to the initiation of nuclear explosive operations. This approach appeared to add clarity.
- LANL, subsequent to its initial briefing to the Board, suggested a change of “Feedback and Improvement” to “Performance Assurance and Improvement.” This reflects an emphasis by LANL’s staff on the proper use of “Feedback” information, and appears to be related to their desire to be able to realistically judge how they are doing, rather than just collect data.
- The safety management system developed for the SRS Canyons successfully integrates the site’s standards program into facility-specific implementation, including an assessment and feedback function.

Standards/Controls

- LANL, Pantex, and SRS reported vigorous local standards development programs (at varying states of progress) to tailor broad standards to their specific sites, facilities, and activities.
- The Pantex program reflects a commitment to the identification of operational/facility controls, which are derived from a variety of sources [Safety Analysis Report (SAR),

HAR, Nuclear Explosive Hazards Analysis (NEHA), etc.]. Right now their control of this “Acronym Alphabet Soup” is embryonic, but they clearly have recognized the need to both “Identify” and “Implement” a formal system of controls.

- To implement authorization basis requirements, the SRS is developing a database that links these requirements and controls with procedures and technical work documents. This noteworthy innovation is particularly important for facilities with many implementing controls and various authorization basis source documents.

Relationship of Safety Management Functions to Functional Areas and Safety Analysis Reports

Fundamentals for Understanding Standards-Based Safety Management of Department of Energy Defense Nuclear Facilities, (DNFSB/TECH-5) provides examples of “functional areas” to be considered in the development of safety management systems. They include: conduct of operations, training and qualification, maintenance, configuration management, emergency management, fire protection, nuclear explosive and explosive safety, nuclear criticality safety, environmental protection, waste management and minimization, occupational safety and industrial hygiene, radiological protection, and others.

- For two key safety management functions, namely “analyze hazards” and “develop/implement controls,” the better presentations included the concepts discussed in Table 1.
- SARs written in accordance with DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, do not necessarily result in adequate worker protection. Thus, the “analyze hazards” step executed at the activity level is critical to identifying controls needed for worker protection. In addition, controls can derive from regulations and permits intended to protect the environment. Thus, controls identified in ISMS typically include Technical Safety Requirements (TSR)—namely Safety Limits, Limiting Control Settings, Limiting Conditions for Operation, Surveillance Requirements, and Administrative Controls resulting from SARs. In addition, engineered and administrative controls are derived from hazards analyses, which lead to protection of the public, workers, and environment and from regulations, permits, etc., to protect the environment.

Table 1. Relationship of Safety Management Functions to Functional Areas

	Analyze Hazards	Develop/Implement Controls
Institution	Identify hazards to be handled site wide and their related functional areas; such as fire protection and aspects of radiation protection, occupational safety and industrial hygiene, and emergency response.	Develop site-wide policies and site-wide standards and requirements covering hazards to be handled on a site-wide basis. Provide implementation requirements and guidance.
Facility	Perform safety analyses including SARs or BIOs <u>as well as other safety analyses more focused on worker safety.</u> Identify TSRs, Operating Limits, and functional areas required.	Develop facility-specific standards and requirements. Implement site-wide and facility standards/requirements, as well as TSRs. Develop a safety management system for functional areas identified as needed.
Activity	Perform appropriate safety and process hazards assessments. Identify potential actions to reduce risk.	Develop safety management strategies consistent with institutional and facility standards/requirements and hazards assessments of activity.

Work Control

- Control must be maintained over who can perform work activities, and when and under what conditions work can be performed. Typically, specific individuals are given responsibility for work control. These individuals, as well as the people performing the work, may be operating to internal authorization bases approved by the contractor, depending on the level of hazards.
- Information on standards, requirements, controls, and protective features identified in hazards assessments, etc., needs to be understood by workers before they are permitted to begin work.