Department of Energy
Office of Nuclear and Facility Safety Policy
Nuclear Safety Management Technical Position
NSTP 2003-1

Use of Administrative Controls for Specific Safety Functions

Issue:

When administrative controls that provide safety functions similar in importance to safety class or safety significant engineered controls are selected for accident prevention or mitigation, they must be formulated and implemented in such a way that their safety functions are effective and dependable.

Background:

On December 11, 2002, the Defense Nuclear Facilities Safety Board issued Recommendation 2002-3. Recommendation 2002-3 noted concerns about the lack of rigor and quality assurance accorded some discrete operator actions or administrative controls that are required to control or mitigate the consequences of accidents at DOE nuclear facilities. The Board noted that the DOE does not have an adequate set of requirements for the design, implementation, and maintenance of important safety-related administrative controls to ensure that they will be effective and reliable. The Board recommended that DOE promulgate a set of requirements to establish appropriate expectations for the design, implementation, and maintenance of these important safety controls and that DOE ensure that all existing administrative controls of this nature be evaluated against these requirements and upgraded as necessary to meet expectations.

In response to this recommendation, DOE assessed the existing requirements and guidance. The assessment found that DOE requirements and guidance provide relevant statements of expectations that administrative controls that perform specific safety functions must be included within hazard controls and described in Documented Safety Analyses (DSA), and must be justified and maintained. These expectations are distributed throughout the requirements and guidance documents but are not as focused and specific as the guidance for safety structures, systems, and components (SSCs).

In the case of safety class and safety significant SSCs, DOE guidance for new facilities and major modifications to existing facilities provides design guidance and reference to national consensus standards, with the aim that these SSCs must be capable of performing their safety functions when called upon (See DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1, Facility Safety*). When administrative controls provide safety functions of similar importance to Safety SSCs, they are likely to be less dependable than Safety SSCs even with measures to compensate for the inherent lesser dependability of human vs. engineered safety measures. DOE is developing a technical standard to provide guidance

on measures to improve the dependability of these administrative controls. This technical standard will be issued after DOE-wide review and comment.

It is the purpose of this Technical Position to bring together the existing requirements and guidance for administrative controls that perform a specific safety function in a more focused fashion. This technical position also makes clear DOE's policy expectations for the proper understanding and implementation of these administrative controls as interim guidance pending the issuance of the technical standard.

Technical Position:

The provisions in Title 10 CFR Part 830.204 require that a DSA include the derivation of hazard controls necessary to ensure adequate protection for the public, workers, and the environment; demonstrate the adequacy of these controls; and define the process for maintaining the hazard controls current at all times and controlling their use

All safety-related controls are identified and characterized during the course of the hazards and accident analyses performed in support of the DSA. DOE encourages the use of design and safety features rather than procedural and administrative controls to address worker and public safety. Judgments of what constitutes appropriate controls should consider the level of the hazard and potential consequences, the practicality and effectiveness of possible control options, the importance of the mission of the facility, and other relevant factors, if any. These are all elements of the graded approach to implementing DOE's nuclear safety management requirements.

Administrative controls are always important contributors to safe operation of a facility. Safety management programs such as Conduct of Operations, Radiation Protection, Maintenance Management, Personnel Training, and Criticality Protection work primarily to assure that normal operations are maintained within intended bounds. In analyses of facility hazards the effective implementation of these safety management programs is implicitly assumed, and it is essential that this assumption be protected. That is, safety management programs must be in place and implemented through commitments in Technical Safety Requirements (TSRs). The discipline imposed by safety management programs goes beyond merely supporting the assumptions identified in hazard analyses and is an integral part of defense in depth. Poor implementation of otherwise adequate administrative controls can lead to safety failures that could be misinterpreted as poor administrative controls, when the real issue is less than adequate implementation.

Depending on the situation, some administrative controls that perform preventive or mitigative functions for accident scenarios may be identified in hazards analyses. As with engineered controls, these administrative controls must be justified, effectively and reliably maintained, and verified. Many such administrative controls may be implemented directly under the provisions of a safety management program. However, some of these administrative controls may have critical importance similar to, or the same as, those that would be classified as safety class or safety significant SSCs if their safety functions or objectives could be performed by engineered safety systems. For convenience, these types of administrative controls (ACs) will be referred to as Specific ACs.

Factors that may be used to identify an administrative control as a potential Specific AC include the following:

- The AC is explicitly identified in hazards analysis as needed to prevent or mitigate an accident scenario.
- The AC is the basis for validity of the hazard or accident analyses (e.g., a hazardous material inventory such as combustible materials or material at risk (MAR) limit).
- The AC has no defense-in-depth backup to prevent an accident event.
- The AC is a necessary element of a set of controls for an accident scenario.
- The AC is more effective and dependable than an available SSC.
- Only ACs (no SSCs) are available for hazard control.
- Violation of the AC is important enough to result in a TSR violation.
- The safety function of the AC would be considered for classification as safety significant or safety class if the safety function were provided by an SSC.

No one of these factors, if applicable, need necessarily result in classifying an administrative control as a Specific AC, but they are indicators that the AC should be considered for classification as a Specific AC.

When administrative controls are used for purposes other than generic coverage of safety management programs, as would be the case for Specific ACs, descriptions of them in a DSA should be sufficiently detailed so that a basic understanding is provided of what is controlled and why, and should include bases information sufficient to derive TSR administrative controls for specific control features. The TSR derivation section in the DSA is intended to provide a link between the safety analysis and the list of variables, systems, components, equipment, and administrative procedures that must be controlled or limited in some way to ensure safety.

The development, implementation, and ongoing verification and validation of Specific ACs must be conducted with a special degree of rigor and quality assurance, similar to that afforded engineered controls or design features with similar safety importance. In developing and implementing Specific ACs, the following factors must be considered:

A. Specific design attributes to assure effectiveness and dependability;

B. Specific treatment in TSRs;

C. Specific training and qualifications to ensure that the appropriate facility operators, maintenance and engineering personnel, plant management, and other staff properly implement each control;

D. Periodic reverification that each control remains effective; and

E. Root cause and failure analysis, similar to those required upon a failure of an engineered system.

The following paragraphs discuss guidance for applying each of these factors to Specific ACs. Note: some items (requirements and guidance) listed in the following paragraphs are paraphrased, and some are directly quoted.

A. Specific design attributes to assure effectiveness and dependability

The expectations for the process of developing Specific ACs to assure effectiveness and dependability are clear. QA requirements of 10 CFR 830.122, specifically criteria 6 and 4, are applicable.

10 CFR 830.122, criterion 6:

1. "Design items and processes using sound engineering/scientific principles and appropriate standards."
2. "Incorporate applicable requirements and design bases in design work and design changes."
3. "Identify and control design interfaces."

10 CFR 830.122 criterion 4:

1. "Prepare, review, approve, issue, use, and revise documents to prescribe processes, specific requirements, or establish design."
2. "Specify, prepare, review, approve, and maintain records."

These requirements are not limited to the design of hardware, but include all items that bear on nuclear safety, including the formulation of Specific ACs. However, these requirements do not provide guidance on how to accomplish the desired end. The primary DOE references for this topic are: DOE O 5480.19, Conduct of Operations, especially the Attachment to the Order, chapters X, Independent Verification, XI, Logkeeping, and XVI, Operations Procedures; and DOE-STD-1092, Change Notice No. 1, Writer's Guide for Technical Procedures, December, 1998.

The Institute of Nuclear Power Operations (INPO) Excellence in Human Performance Initiative 2001 and related INPO publications (see References 1 and 2 at the end of this document) provide guidance on developing effective and reliable administrative controls, including the following:

- "Develop procedures with a clear, logical sequence of tasks that make them understandable to the user. Procedures provide all the information individuals need to perform assigned tasks. In addition to operating experience, procedure development takes into account training, experience, human limitations, and level of supervision of the intended users. Plant conditions for use are specified, complexity is minimized, and segments critical to plant safety and reliability are appropriately highlighted."

- "Communicate policies for procedure use and adherence. Guidance for use of specific procedures should identify those tasks or evolutions for which continuous in-hand use or strict adherence is required. This guidance takes into account other factors such as the consequences of improper performance, the complexity of the task, the capabilities of the individual, human limitations, and the frequency of performance."

- "Verify the integrity of defenses, especially for tasks important for nuclear safety. The number and strength of defenses, such as multiple safeguards, equipment

trains, interlocks, physical barriers, supervision, and procedures, are related to the potential safety-related consequences of errors."

- "Alert workers and supervisors to key task decision points. Managers elevate the attention of individuals by incorporating appropriate cues, such as cautions and notes, at specific junctions of a procedure important for nuclear safety, especially for tasks containing irreversible actions."

- "Incorporate appropriate information into procedures from applicable source documents, such as the plant design documents (and) plant-specific (safety) analyses."

- "Detail prerequisites and initial conditions. Carefully consider the location of this information in the procedures so that the intent of each procedure is understood."

- "Define nomenclature used in the procedure"

- "Describe only one action in each procedure step."

- "Provide individual signoffs for selected critical steps. One signoff applies to only one action."

- "Separate signoffs are provided for independent verifications."

Other methods to design processes in a manner to eliminate defects, including human errors, may be available. This Technical Position does not endorse any one method over others that may be equally valid.

B. Specific treatment in TSRs

There are at least two ways of treating Specific ACs in TSRs. One is via a Limiting Condition for Operation (LCO) and associated Surveillance Requirement (SR). The LCO and SR could be in the Operating Limits and Surveillance Requirements section of the TSR. This format may be appropriate when the AC can be well defined, clear corrective actions are available, and conditions can be easily surveilled. This method is covered in more detail in a May 20, 2003 memorandum from the Assistant Secretary for Environmental Management, subject "Environmental Management Guidelines and Lessons Learned for Nuclear Facility Safety Control Selection and Implementation." See Section 3 of the report attached to the memo, and the examples in Attachments 2 and 3 to the report. This resource can be found at:
http://apps.em.doe.gov/safetybases/safetybases.asp

A second way to incorporate Specific ACs in a TSR document is to list the specific requirement/action in the Administrative Control (AC) section of the TSR in a special section. This format may be appropriate when it is essential that the Specific AC be performed when called upon every time and without any delay (e.g., hoisting limits for nuclear explosives).

In both cases the Use and Application section of the TSR should define the ground rules for treating Specific ACs, including treatment of violations as TSR violations and reporting requirements. In addition, it has been found to be helpful to include a statement of the basis of the Specific AC where it is invoked.

C. Specific training and qualifications to ensure proper implementation

The applicable requirements for training for proper implementation of Specific ACs can be found in:

> 10 CFR 830.122 criterion 2, sub item (1):
> (1) "Train and qualify personnel to be capable of performing their assigned work."
>
> DOE O 5480.20A: Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities:
> Train facility staff, as appropriate according to the facility's Training Implementation Matrix, on TSRs and operating procedures.

D. Periodic reverification that each control remains effective

Under the TSR provisions for a Specific AC, either as an LCO with Surveillance Requirements or as a Specific AC in the Administrative Controls section, dependability is enhanced because of its TSR status. If an LCO is used, the associated Surveillance Requirement (SR) would be the periodic reverification. Specific ACs in a TSR Administrative Controls section should be incorporated into facility procedures and reverified in accordance with Chapter XVI of DOE Order 5480.19, Conduct of Operations.

As a Specific AC in the Administrative Controls section, violation of the AC would be an immediate TSR violation, requiring notification of DOE. The violation should be reported through the Occurrence Reporting System (ORPS) and the Noncompliance Tracking System (NTS). These required actions for violations of Specific ACs ensure that they will be periodically reviewed and verified.

In addition, the following QA provisions apply:

> 10 CFR 830.122 criterion 3, sub items (1), (2), and (4):
> (1) "Establish and implement processes to detect and prevent quality problems."
> (2) "Identify, control, and correct items, services, and processes that do not meet established requirements."
> (4) "Review item characteristics, processes implementation, and other quality-related information to identify items, services, and processes that need improvement."
>
> 10 CFR 830.122 criterion 5, sub items (2) and (3):
> (2) "Identify and control items to ensure their proper use."
> (3) "Maintain items to prevent their damage, loss, or deterioration."

E. Root cause and failure analysis

The following DOE requirements apply to failures of Specific ACs:

> DOE O 231.1A, Environment, Safety, and Health Reporting; and DOE M 231.1-2, Occurrence Reporting and Processing of Operations Information
> The Occurrence Reporting Program includes guidance for root cause analysis, corrective action, trending, and escalation of repeat events.. Events that might qualify related to Specific ACs might fall under Group 3, Nuclear Safety Basis; Group 4, Facility Status; Group 7, Nuclear Explosive Safety; or Group 8, Transportation.
>
> 10 CFR 830.122 criterion 3, sub item 3
> (3) "Identify the causes of problems and work to prevent recurrence as a part of correcting the problem."
>
> 10 CFR 830.122 criterion 9:
> "Ensure managers assess their management processes and identify and correct problems that hinder the organization from achieving its objectives."
>
> 10 CFR 830.122 criterion 10, sub item 1:
> (1) "Plan and conduct independent assessments to measure item and service quality, to measure the adequacy of work performance, and to promote improvement."

Additional Considerations:

Administrative controls depend on human performance. Excellence in human performance is as vital to the success of administrative controls as the institutional factors in the previous discussion. Three reference documents listed at the end of this Technical Position provide insights on the importance of the facility and organizational safety culture to operational safety. They also include concepts and methods for enhancing safety culture. Excerpted from Reference 2, INPO's *Excellence in Human Performance*, here are some principles of human performance improvement:

- "People are fallible, and even the best make mistakes."
- "Error-likely situations are predictable, manageable, and preventable."
- "Individual behavior is influenced by organizational processes and values."
- "People achieve high levels of performance based largely on the encouragement and reinforcement received from leaders, peers, and subordinates."
- "Events can be avoided by understanding the reasons mistakes occur and applying the lessons learned from past events."

The report goes on to describe how the individual, the leaders, and the organization can promote excellence in human performance. Some of those very relevant to implementing Specific ACs include the following:

- Communicate accurately and frequently. Regularly use repeat backs.

- Inform coworkers, supervisors, or managers when there is a potential problem with performing a task. Perform post job critiques to identify improvements.
- Anticipate error-likely situations. Verify instructions, equipment, location, and time constraints.
- Check others. Actively monitor and challenge each other's actions and thought processes.
- Focus attention on the task at hand. Approach each job with a questioning attitude, thinking through the steps and key decision points of a task before acting.
- Expect success, but anticipate failure. Routinely ask "what if."
- Take the time to do the job right.
- Follow approved procedures with a sense of caution.
- Stop the task and collaborate with others when unfamiliar or unanticipated conditions arise.

Leaders and managers should foster a work environment that encourages these behaviors on the part of the operations staff.

References:

1. *Guidelines for the Conduct of Operations at Nuclear Power Stations,* Institute of Nuclear Power Operations, INPO 01-002, May 2001

2. *Excellence in Human Performance,* INPO, September 1997

3. *Putting the Human into Hazard Assessment,* Helen Rycraft, BNFL, a paper presented at the 2003 annual meeting of the Energy Facility Contractors Group (EFCOG) Safety Analysis Working Group (SAWG), Salt Lake City, June 2003

Approved: Bevery A Cook Date: 10/29/03