This draft, December 2003, prepared by EH-22 has not been approved and is subject to modification. Project No. SAFT-0091

NOT MEASUREMENT SENSITIVE

DOE-STD-XXXX-YR
PROPOSED

DOE STANDARD

SPECIFIC ADMINISTRATIVE CONTROLS

U.S. Department of Energy
Washington, D.C. 20585

AREA SAFT

This document has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831; (423) 576-8401.

Available to the public from the U.S. Department of Commerce, Technology Administration, National Technical Information Service, Springfield, VA 22161; (703) 605-6000

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Scope

This Standard addresses guidance intended to apply to Administrative Controls that are selected to provide preventive and/or mitigative functions for specific potential accident scenarios, and which have safety importance equivalent to engineered controls that would be classified as Safety Class (SC) or Safety Significant (SS) if the engineered controls were available and selected. This class of Administrative Controls (ACs) is designated as Specific ACs. The Standard does not intend that Specific ACs be further classified as SC and SS ACs. There is no value in doing so, because there is no difference in the measures for assuring the dependability of Specific ACs that the Standard discusses that depend on whether protection of the public or workers or defense in depth is the function of the AC.

Similar to Safety SSCs, not all specific action ACs related to individual accident scenarios rise to the level of importance of Specific ACs, as discussed in the previous paragraph. Again, similar to SSCs of lower importance, which are sometimes referred to as "important to safety" or "defense in depth" SSCs, specific ACs of lesser importance can be addressed under the implementation of related Safety Management Programs.

The organization of this Standard is as follows: Section 1 relates this Standard to the DNFSB Recommendation to DOE concerning Specific ACs, and the existing requirements for derivation of safety bases, including hazard analyses, identification of hazard controls, derivation of TSRs, and the role of Administrative Controls in the TSR. It introduces the concept of Specific ACs.

Section 2 provides guidance for criteria by which to classify ACs as Specific ACs, how Specific ACs relate to the requirements and guidance for safety bases in 10 CFR 830 Subpart B, formats for TSR treatment of Specific ACs, and measures to ensure the dependability of Specific ACs.

Section 3 provides more guidance on the formats for treatment of Specific ACs in TSRs and provides some examples of those formats.

Sections 4 and 5 discuss training and causal and failure analyses as applied to Specific ACs.

1.2 Purpose

This Technical Standard clarifies and focuses existing requirements and guidance for the development and implementation of Administrative Controls (ACs) relied on to perform specific safety functions. To focus attention on the unique issues associated with of this type of AC, this Standard defines a new type of AC to be known as a Specific AC. A Specific AC exists when an AC:

a. is explicitly identified in the hazard analysis as a control needed to prevent or mitigate an accident scenario, and
b. has a safety function that would be safety significant or safety class if the function were provided by an SSC, or
c. is required to complete the safety function of a safety class or safety significant SSC.

This increased focus is intended to improve the dependability of these controls and to enhance their availability to perform specific safety functions when needed. This Standard should be used to comply with all DOE methods for DSAs and their associated TSRs for compliance with 10 CFR 830, when developing and implementing Specific ACs. It complements and expands on guidance contained in Nuclear Safety Technical Position 2003-1, *Use of Administrative Controls for Specific Safety Functions.*

1.3 Applicability

The information contained in this Standard is intended for use by all Department elements, including the National Nuclear Security Administration (NNSA), and all contractors for DOE-owned or DOE-leased, hazard category 1, 2, or 3, nuclear facilities or nuclear operations.

1.4 References

a. DOE-STD-3009-94*,CN2, Preparation Guide For U.S Department Of Energy Nonreactor Nuclear Facility Documented Safety Analyses*
b. DOE G 423.1-1*, Implementation Guide For Use In Developing Technical Safety Requirements*
c. DOE O 5480.19, *Conduct of Operations*, especially the Attachment to the Order, chapters X, Independent Verification, XI, Logkeeping, and XVI, Operations Procedures
d. DOE-STD-1092, Change Notice No. 1, *Writer's Guide for Technical Procedures*, December, 1998.
e. *Excellence in Human Performance,* INPO, September 1997

f. *"Environmental Management Guidelines and Lessons Learned for Nuclear Facility Safety Control Selection and Implementation,"* dated April, 2003.
g. *Guidelines for the Conduct of Operations at Nuclear Power Stations,* Institute of Nuclear Power Operations, INPO 01-002, May 2001
h. *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
i. Memorandum and its Attachment from the Assistant Secretary for Environmental Management, subject "*Environmental Management Guidelines and Lessons Learned for Nuclear Facility Safety Control Selection and Implementation*." May 20, 2003

1.5 Background

1.5.1 U.S. DOE's Implementation Plan for DNFSB Recommendation 2002-3, *Requirements for the Design, Implementation, and Maintenance of Administrative Controls*

The DNFSB issued Recommendation 2002-3 on December 11, 2002, noting that the development, selection, and implementation of an effective set of hazard controls are among the most important elements of nuclear safety. DOE has established a priority process that favors preventive over mitigative measures, passive design features over active controls and engineered controls over ACs. The approved process recognizes that, where necessary or practical, ACs may play an important role in hazard prevention and mitigation.

The Board has agreed with DOE's overall guidance for a hierarchy of controls and agrees that ACs are sometimes appropriate to prevent or mitigate accident consequences—even those that exceed evaluation guidelines for risk to the public.

The Board recommended that DOE promulgate requirements to establish expectations for the design, implementation, and maintenance of ACs when relied on to provide specific safety functions, and to ensure existing ACs of this nature are evaluated and upgraded as necessary.

DOE accepted the Board's recommendation and prepared DOE's Implementation Plan for DNFSB Recommendation 2002-3, DOE-STD-XXXX-YR addresses the plan's requirement for consolidating and clarifying existing DOE rule guidance and standards to ensure that contractors consistently develop, implement, and maintain ACs consistent with their importance to safety.

1.5.2 Relationship of DOE-STD-XXXX-YR to 10 CFR 830, DOE G 423.1-1, DOE G 421.1-2 and DOE-STD-3009

The Nuclear Safety Management Safety Basis requirements of 10 CFR 830 require contractors responsible for category 1, 2, and 3 nuclear facilities to develop safety bases for those facilities that consist of Documented Safety Analyses (DSAs) and hazard controls in Technical Safety Requirements (TSRs) that are derived from the DSA hazard analyses. Various guides and technical standards, such as this document, provide guidance to help interpret and implement requirements. Three such documents relating to 10 CFR 830.205 are as follows:

a. DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*
b. DOE G 421.1-2, *Implementation Guide For Use in Developing Documented Safety Analyses To Meet Subpart B Of 10 CFR 830*
c. DOE G 423.1-1, *Implementation Guide For Use In Developing Technical Safety Requirements*

DOE-STD-3009 represents a “Safe Harbor,” that is an acceptable method for preparation of a DSA under the requirements of 10 CFR 830, Appendix A, Subpart B. DOE-STD-3009 provides detailed guidance for preparation of SARs (DSAs), including the derivation of TSRs.

DOE-STD-3009-94 addresses derivation of ACs relative only to the anticipated application of ACs with major significance to defense in depth, or worker safety. These ACs are primarily related to safety management programs. Inclusion of these ACs in the TSRs formally acknowledges the importance of programmatic commitments (e.g., radiation protection, maintenance, quality assurance) to overall facility safety, but usually do not specify key aspects of each program as providing specific safety functions. The cumulative effect of these safety management programs is recognized as being important to overall facility safety, as opposed to specific accident risk reduction.

DOE Guide 423.1-1 provides detailed guidance for developing the TSR content, including ACs. The guide states that ACs should be a direct result of the DSA, but they may also result from institutional requirements that address many facilities. Section 4.10.7 of the guide goes further than DOE-STD-3009 in specifying the application of ACs, and recognizes that ACs may be applied for risk reduction of individual accident scenarios. Although recognized as being potentially applicable to specific accident scenarios, it states that ACs should be considered for defense in depth rather than as a primary control. The guide does, however, recognize the significance of “AC statements.” When ACs specifically state a limit or specific requirement rather than a generic programmatic reliance, failure to meet such statements results in a TSR violation. Both DOE G 423.1-1 and DOE-STD-3009, otherwise state that safety basis violation can only result from a gross safety management program failure, significant enough to render the DSA assumptions invalid.

DOE G 423.1-1 and DOE-STD-3009 continue to provide relevant guidance on the application of ACs as part of the DSA required controls. However, this document is intended to further amplify the appropriate development and implementation of ACs as required in the DOE Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-3.

1.5.3 Derivation of Hazard Controls in the DSA

Hazard controls in the DSA are selected to reduce the risks of authorized activities. Controls are classified by comparison to an Evaluation Guideline in the case of safety class SSCs for protection of the public, and by criteria described in DOE-STD-3009 for safety significant SSCs for worker protection and defense-in-depth. Safety class and safety significant SSCs are expected to be addressed in TSRs.

When selecting controls for inclusion as TSRs, it is preferable to choose engineering controls over ACs, due to the inherent uncertainty of human performance, and when choosing engineering controls, to choose passive SSCs over active SSCs. The actual design and selection process should consider the cost, availability, required reliability, and consequence of mechanical or human failure for each potential control.

1.5.4 The Role of ACs in TSRs

10 CFR 830 states that the safety basis means the DSA and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely in a manner that adequately protects workers, the public, and the environment.

Hazard controls means measures to eliminate, limit, or mitigate hazards to workers, the public, or the environment, including:

a. Physical, design, structural, and engineering features;
b. Safety SSCs;
c. Safety management programs;
d. Technical safety requirements (TSRs) ; and
e. Other controls necessary to provide adequate protection from hazards.

It is expected that the ACs will be tailored to the facility activities and the hazards identified in the DSA. This tailoring should be a direct result of the DSA, but it may also result from institutional requirements that address many facilities. As a general practice, safety controls for individual accident scenarios based on engineered SSCs are preferred to ACs because they are usually more reliable and more predictable. However, this should not be interpreted to mean that ACs do not have an important and useful role in the TSRs. Existing facilities sometimes use ACs as safety controls for individual accident scenarios because it is impractical to retrofit engineered SSCs.

There are instances where an AC may be the most important control. Such instances may include limiting the Material-at-Risk (MAR) for the facility. Accident analysis consequences could be unbounded if MAR is not established for the accident in question; therefore, MAR becomes the most important underlying assumption for all accident analyses as an AC.

Another instance where an AC may be one of the most important controls for a nuclear facility is in controlling transient combustible loading. Fire accident scenarios release large amounts of hazardous materials including radioactive and chemical materials. Therefore, controlling fire accidents in DOE facilities is of vital importance. Fire protection system design is based on the assumption that the combustible loading for a facility does not exceed a certain level, as an AC.

1.5.5 Application of ACs and Specific ACs

A distinction is made between general and Specific ACs. Most ACs are assumed to provide broad programmatic support for generic safety functions supporting defense in depth or worker safety. Failure to maintain all aspects of one of these programs will not result in a safety basis violation unless there is a gross failure, significant enough to render the DSA assumptions invalid. These ACs shall be classified as programmatic ACs.

Specific ACs are ACs that provide specific preventive or mitigative functions for accident scenarios identified in hazards analyses where the safety function has importance similar to, or the same as, the safety function of safety class or safety significant SSCs..

1.5.6 Specific ACs as an Alternative to Safety SSCs

In discussing safety SSCs, DOE-STD-3009 states, “that the decision as to whether an operating limit (such as an LCO) or a TSR administrative control is more appropriate for treatment of the SSC in a TSR is left to the judgment of the DSA preparer.”

DSA preparers should avoid using Specific ACs as an alternative to a Safety SSC whenever possible. Efforts shall be made to use engineered SSCs whenever possible for controlling the likelihood and consequences of accidents. While Specific ACs may be acceptable for ensuring safe operation, their generally lower reliability, compared with engineered controls, must be evaluated carefully when choosing safety measures for long-term hazardous activities.
Specific ACs shall be recognized for their elevated safety significance. Specific ACs which are credited in the analysis with providing specific safety function with safety importance equivalent to the importance of the safety function of safety SSCs must have stringent implementation and verification requirements to ensure their dependability and effectiveness.

2. Specific Administrative Control Attributes

The provisions in 10 CFR Part 830.204 require a DSA to include the derivation of hazard controls necessary to ensure adequate protection of the public, the 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 hazard 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 features and engineered safety features rather than procedural and ACs to address worker and public safety. Judgments must be made regarding what constitutes appropriate controls. These judgments 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.

A subset of all hazard controls will get safety class or safety significant designation, depending upon the consequences of the accident that they are intended to prevent or mitigate. Controls that are identified as part of a safety management program (e.g., fire, criticality, radiation protection, etc.) may or may not end up as controls that need to have enhanced reliability as is the case with Specific ACs based on the designations derived from the hazards and accident analyses in the DSA. Hazard controls should be identified on a case-by-case basis and should be graded according to the guidance in DOE-STD-3009 and this Standard, with regard to the classification of hazard controls.

For site-wide safety management programs (e.g., radiation protection), the DSA should explain the features of those programs that are important to the facility safety basis and can refer to the site-wide program documentation for the details. As appropriate to the hazard, the DSA may identify specific controls (e.g., hazardous material inventory limits) that are required for safety. When such controls are not associated with the operation of a safety SSC, it may be appropriate to identify a "Specific AC" as discussed below.

2.1 Identification of Specific ACs

The specificity of ACs within the DSA/TSR will vary depending on the severity of hazards, the complexity of the facility, and the administrative control's overall contribution to controlling potential accident consequences (i.e., primary or supplemental control). Specific ACs may also be needed to protect important initial conditions assumed in the hazard analysis (e.g., the assumption on combustible inventory limits).

Depending on the situation, some ACs that perform specific preventive or mitigative functions for accident scenarios may be identified in hazards analyses. These are more specific actions than implied by general commitments to safety management programs and they may need to be raised to a higher importance level. Some of these ACs may have critical importance similar to, or the same as, those that would be classified as Safety Class (SC) or Safety Significant (SS) Structures, Systems, or Components (SSCs) if their safety functions or objectives were performed by engineered safety systems. These types of ACs are referred to as "Specific ACs."

If an administrative control:

a. is explicitly identified in the hazard analysis as a control needed to prevent or mitigate an accident scenario, and
b. has a safety function that would be safety significant or safety class if the function were provided by an SSC, or
c. is required to complete the safety function of a safety class or safety significant SSC,

then the AC must be designated as a Specific AC. Identification as a control or a limiting factor in a hazard analysis is a necessary criterion for a Specific AC. Other factors that may be useful to designate an AC as a Specific AC include:

a. 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).
b. The safety function of the AC is explicitly identified in the DSA as needed to prevent or mitigate an accident scenario.
c. The AC has no defense-in-depth backup to prevent or mitigate an accident described in the DSA.
d. ACs provide the main mechanisms for hazard control (e.g., Safety SSCs are degraded, out of service, too costly to implement, or are impractical for a limited-life facility.)
e. Violation of the AC is important enough to result in an immediate TSR violation (i.e., the violation needs to be reported to DOE immediately).
f. The safety function of the AC could be considered for classification as safety significant or safety class if the function were provided by an SSC.

g. Safety SSCs are often used to provide a similar safety function.
h. The AC is used to replace a Safety SSC that has failed or been disabled.

No one of the eight factors in the second list need necessarily result in classifying an administrative control as a Specific AC, but they each are strong indicators that the AC should be considered for classification as a Specific AC.

2.2 Requirements Related to Specific ACs

DOE O 420.1A, Facility Safety, section 4.1.1.2, addresses the design requirements for nuclear safety. The Order states 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. Defense in depth shall include: …the provision of multiple means to ensure critical safety functions (those basic safety functions needed to control the processes, maintain them in a safe state, and to confine and mitigate radioactivity associated with the potential for accidents with significant public radiological impact…" These principles shall apply to the development and implementation of the ensemble of hazard controls, including Specific ACs. Redundant, independent, and diverse hazard controls, be they safety SSCs or Specific ACs performing functions similar to safety SSCs, are essential to ensuring that exposure to a high consequence hazard does not come about due to failure of a single barrier. Application of this concept to Specific ACs is particularly important, as ACs are generally regarded as less dependable due to the introduction of potential human error. The terms redundant, independent, and diverse, as applicable to Specific ACs, are discussed below:

Redundant: Important safety functions should not be protected by a single AC. The design process should strive to achieve an appropriate level of redundancy in the development of controls. In this context, redundancy refers to a second, similar control (as distinguished from diverse controls).

Independent: Controls should be independent of the process being controlled, and to the extent practicable from other controls that have been credited.

Diverse: To avoid the increased likelihood of failure due to common-cause effects, diverse controls should be employed to the extent practicable. In this context, diversity refers to separate controls of a dissimilar nature (as distinguished from redundant controls).

10 CFR 830, Subpart B, provides DOE's expectations for the safety basis requirements. DOE Guide 423.1-1 (TSR Implementation Guide) provides guidance on what technical safety requirements should contain and how they should be developed and maintained.

The DSA required by 10 CFR 830.204 furnishes the technical basis for TSRs. For some facilities, other documentation such as Criticality Safety Evaluations, Fire Hazards Analyses, or the Safety Evaluation Report may provide the bases for additional safety controls or operating restrictions that need to be reflected in the TSRs. DOE-STD-3009 provides guidance to be used in Chapter 4 of a DSA for identification of and documentation for Safety Class and Safety Significant SSCs. Where Specific ACs are used, similar identification and documentation shall be provided in the DSA. The DSA shall specifically describe the safety function, control description, functional requirements of the control, and the TSR controls for each Specific AC.

The DSA shall provide information (generally Chapter 5 of a DSA based on DOE STD-3009) to support the derivation of hazard controls described in the TSRs document. This includes the basis for Specific ACs or specific safety management programs necessary to perform institutional safety functions. Descriptions of Specific ACs in a DSA shall be sufficiently detailed so that a basic understanding is provided of what is controlled and why.

Specific ACs generally control a specific safety-related parameter or provide a specific safety function. These Specific ACs generally have two forms as identified below.

a. Limiting Conditions for Operation/ Surveillance Requirement

Specific ACs can often be written in the format of an LCO. Treatment of Specific ACs as LCOs in TSRs is contained Section 3 of this Standard.

b. Specific Directive Action AC

A Specific "Directive Action" AC is a statement of an AC requirement that prescribes a specific action to be performed in response to an observed facility condition. Treatment of Specific ACs as ACs in the TSRs is contained in Section 3 of this Standard.

2.2.1 Implementation and Maintenance of Specific ACs

The concepts of verification and validation are essential to ensuring that a Specific AC will effectively accomplish its required safety function and maintain its ability to perform its required function.

Verification: TSRs must be initially (prior to implementation) and periodically verified to perform their intended safety function. In the context of Specific ACs, this may involve "dry runs," procedure walk-downs, tabletop exercises, or actual hazard/casualty exercises. Additionally, the verification process should be performed by knowledgeable individuals who were not part of the development of the control to assure an unbiased assessment of the effectiveness of the control. Also, the control should be designed such that it is easily and readily verifiable through appropriate and ongoing testing, examination or surveillance activities. Periodic re-verification that a Specific ACs can perform their intended safety function shall be addressed through LCO Surveillance Requirements for Specific ACs written as LCOs, or through facility operations and maintenance procedures if the Specific AC is incorporated into the AC section of the TSRs. Consequences of incorrect implementation of the control shall be evaluated and measures to prevent control failure should be factored into the control formulation.

Validation: The validation process ensures that plant operators have sufficient time, indicators or alarms, tools, or other necessary resources to perform the task. For Specific ACs, a human factors analysis may be necessary to ensure that the operators have sufficient indicators or alarms, time, and equipment to perform their required tasks. Formal engineering calculations may be necessary to ensure that plant operators have the appropriate time and resources to carry out the required tasks. (For example, if it is assumed that operators will take actions to detect and isolate a leak, flowrate calculations will need to be performed to substantiate the available time interval necessary to accomplish the task.)

2.2.2 Measures Used to Ensure the Dependability of Specific ACs

Dependability of Specific ACs relies on human (operator) performance. Human performance is affected by a variety of factors (normally called Performance Shaping Factors) that affect people and systems in different ways when combined. The main factors that affect the dependability of an operator are:

- Specification of the task

- Level of difficulty of the task
- Design of the equipment and feedback, e.g. alarms.
- Time available to do a task or recover an error.
- Stress levels induced by the external environment, e.g. noise, heat, light and protective clothing worn.

Each of these factors shall be considered on a case-by-case basis when formulating and implementing Specific ACs. Most, if not all, of these factors will be evaluated and addressed when validating a Specific AC's effectiveness.

The dependability of Specific ACs is improved by implementing the Guidelines for Conduct of Operations provided in DOE O 5480.19. All DOE operations are subject to the requirements and guidance given in the Order. The guidelines form a compendium of good practices and describe key elements of programs that support operations at DOE facilities. Their implementation should result in a high level of performance and therefore contribute to safe and dependable operation.

Operators often must rely on effective instrumentation and controls and support equipment to implement Specific ACs. For this reason, design of instrumentation and controls and support equipment that support a Specific AC, to the extent possible, should employ redundancy, diversity, and independence of critical components similar to the design of these features for Safety SSCs. This equipment shall meet performance requirements similar to that required to Safety SSCs.

The dependability of a Specific AC is improved when written as an LCO in the TSRs. Treatment of Specific ACS in TSRs is addressed in Section 3 of this Standard. Guidance for developing and writing LCOs is provided in DOE G 423.1-1. Although this guidance is directed at LCOs used to support SSCs, a Specific AC has a safety function with importance similar to, or the same as, the safety function of safety class or safety significant SSCs. As such, the guidance given in this section can be directly applicable to Specific ACs written as LCOs. Specific ACs written as LCOs should generally comply with the guidance given in DOE G 423.1-1 for LCOs including, but not limited to, Specification for Limiting Conditions for Operation, Action Statements, Operability, Surveillance Requirements, Violation of Technical Safety Requirements, and TSR Bases.

For a Specific "Directive Action" AC listed in the ACs section of the TSRs, dependability is primarily a function of periodic verification of the capability of the safety function provided by the Specific AC. The periodicity and method of this verification of the safety function must be addressed in the Specific AC. This verification may be accomplished through “dry-runs,” procedure walk-downs, or actual hazard/casualty exercises.

Other specific measures that help to limit the likelihood of human error in performing the tasks required by a Specific AC, and that should be implemented as appropriate, include:

Independent Verification: Independent verification refers to the concept of having a second, qualified operator verify the actions of a primary operator. Independent verifications should be conducted in a manner such that each check constitutes an actual identification of the component or action and a determination of both its required and actual positions or condition. To be independent, the integrity of the checks must be maintained by minimizing interaction between the personnel operating components and those performing the independent verifications. For example, it is not always possible to determine if an operator has completely shut or opened a valve by merely observing the action; mistakes in component identification or requirement determination might not be caught without both individuals’ reading the labels and procedures. Additionally, consideration should be given to requiring managerial or supervisory signoff.

Task Feedback: To the extent practicable, measures should be implemented that provide appropriate feedback to the operators that a required action has been successful. This can be accomplished by the incorporation of appropriate monitoring equipment, valve position indication devices, etc.

Human Reliability Assessment: A formal Human Reliability Assessment (HRA) can serve to validate the dependability of a Specific AC. Alternatively, the HRA can identify weaknesses in the proposed procedures to implement a Specific AC and suggest additional measures to improve the overall dependability. However, an HRA can be a significant effort that should only be resorted to when there is an obvious benefit to justify that effort.

2.3 Lessons Learned on Human Actions Used for Safety Controls in Accident Scenarios

Human actions, either taken in response to an event or taken proactively to establish desired conditions, are subject to errors of omission or commission. Sets of ACs are prone to common cause failure. The following attributes, which can be tailored as appropriate, can improve worker performance in utilizing ACs:

- Use of reader/worker/checker systems;
- Independent verification;
- Positive feedback systems;
- Interlocks;
- Warning signs and barriers;
- Alarms and monitors;
- Human factor analysis;
- Operator training and certification;
- Continuing training and re-qualification;
- Abnormal event response drills;
- Ergonomic considerations in procedures;
- Dry runs for non-routine operations; and
- Use of double staffing or direct supervision for hazardous operations.
- Human Reliability Assessment

2.4 Establishing a Safety Culture

Both the Institute of Nuclear Power Operations (INPO) Excellence in Human Performance Initiative 2001 (Ref. e) provides insights on the importance of developing an appropriate safety culture to improving human performance. Excellence in human performance is more likely when both workers and managers embrace the following principles:

a. People are fallible, and even well trained and experienced staff can make mistakes.
b. Error-likely situations are predictable, manageable, and avoidable.
c. Individual behavior is influenced by organizational processes and values.
d. People achieve high levels of performance based largely on the encouragement and reinforcement received from their leaders, peers, and subordinates.

e. Most accidents can be avoided by understanding the reasons mistakes occur and applying the lessons learned from past events.

Some of the INPO recommendations that are most relevant to dependable implementation of Specific ACs include:

a. Communicate expectations and work plans accurately and frequently. When work processes are changing daily, job briefings and use of repeat backs are encouraged.
b. Inform coworkers, supervisors, and managers when there is a potential problem with performing a task. Perform post-job critiques to identify process improvements.
c. Anticipate error-likely situations. Most hazardous activities require both the worker and the backup/supervisor to understand the work process.
d. Verify instructions, equipment, location, and time constraints.
e. Focus attention on the task at hand. Think through the steps and key decision points of a task before acting.
f. Expect success, but anticipate failure. Routinely ask “what if.”
g. Take the time to do the job right.
h. Make sure schedules do not interfere with safety
i. Follow approved procedures with a sense of caution.
j. 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.

3. TREATMENT OF SPECIFIC ACs in TSRs

The TSR derivation section in the DSA is intended to provide a link between the safety analysis and the list of variables, safety SSCs, and ACs necessary to ensure safety.

3.1 TSR Treatment of Safety Controls Covered by Safety Management Programs

The traditional type of TSR ACs are the provisions relating to organization and management, procedures, record keeping, reviews, and audits governing safe operations and encompassed in safety management program commitments. Existing DOE directives *(References a. and b.)* specify that the ACs section of the TSR document will contain commitments to establish, maintain, and implement these programs at the facility and, as appropriate, facility organizational and administrative requirements. The brief mention of this type of control distinguishes them from Specific ACs.

Programmatic ACs are credited in safety basis documents with a significantly lower level of specificity than are Specific ACs. Absent in their selection are specific limits or discernible operator actions relating to specific hazard or accident analysis conditions. Rather, these ACs contain basic program elements or features that constitute the viability of the safety management program to support safe operations.

Typically, these ACs flow down as performance requirements contained in organizational or company-level procedures. Prior to implementation of DOE approved TSR ACs, contractors should first take appropriate actions to ensure a control's availability and readiness. These actions may include programmatic assessments, development, or modification of facility procedures, and training of facility personnel. Continuing verification of implementation of the programmatic control is typically verified through continuing assessment and performance monitoring (trend analysis).

3.2 Implementing Specific ACs in TSRs

When Specific ACs are identified, these shall be controlled through the TSR. Two methodologies are acceptable for the appropriate treatment of Specific ACs in TSRs. The first involves using the conventions for LCOs and associated SRs. Placement of the LCO and SR for a Specific AC shall be in the Operating Limits and Surveillance Requirements section of the TSR. This format shall be used when the Specific AC is well defined, clear corrective actions are available, and conditions supporting the Specific AC can be easily surveilled. An example of this type of format is shown in Figure 1.

Guidance for developing and writing LCOs is provided in DOE G 423.1-1. Although this guidance is directed at LCOs used to support SSCs, a Specific AC has a safety function with importance similar to, or the same as, the safety function of safety class or safety significant SSCs. As such, the guidance given in this section can be directly applicable to Specific ACs written as LCOs. Specific ACs written as LCOs should generally comply with the guidance given in DOE G 423.1-1 for LCOs including, but not limited to, Specification for Limiting Conditions for Operation, Action Statements, Operability, Surveillance Requirements, Violation of Technical Safety Requirements, and TSR Bases.

The second method available to incorporate Specific ACs in a TSR document is to identify the specific requirement/action in the Administrative Control 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, MAR limits, or expected responses during criticality safety infractions not covered by an LCO) or when definitive program requirements for specific activities can be stated. An example of this type of format is shown in Figure 2 of this section.

3.3 Considerations In Developing a MAR TSR Control:

MAR is the major analytic assumption that must be made before a hazard analysis can support any consequence binning beyond the purely subjective and before any non-qualitative accident analysis can be initiated. Further, MAR assumption violations place the facility in a formally unanalyzed space for which consequences would be unknown and potentially unbounded. It is essential that MAR assumptions are protected in a highly reliable and enforceable manner. However, it is not normally possible to control MAR with an active or passive Structure, System, or Component (SSC). Under normal circumstances MAR cannot be controlled through a Design Feature (DF) or SSC based LCO. This leaves only administrative type controls in the form of a TSR Section 3 / 4 (Operating Limits and Surveillance Requirements) LCO (in itself a type of Administrative Control) for MAR or a TSR Section 5 AC (Programmatic AC or Specific AC).

Use of an LCO is warranted when a defensible estimate can be made of how much of a MAR exceedance can occur. Provided this estimate can be made, it may be possible to make an estimate of the risk involved in exceeding the analyzed MAR for some time interval to support LCO action times as well as associated surveillance frequencies. The surveillance frequencies are established to ensure a reasonably confident expectation that MAR will not be exceeded. This must be documented in the supporting BASIS statements. When it can be defended, use of a MAR LCO has the advantage of allowing the facility an action completion time which, if met, would preclude a TSR violation. There are also feasibility limits associated with the LCO approach in addition to the need for estimating the potential size and duration of MAR exceedances. An example of this would be a facility, which needs to control MAR in a very large number of locations because of the way that the accident analysis was performed. If, for example, a facility analysis was performed on a glove box, room, wing, and facility wide basis and each of these yielded its own MAR limit. For consideration purposes assume that for a large facility, there may be 200 glove boxes, 100 rooms, 2 wings, etc. In this example, each location may require its own entry in the TSR LCO creating a very large number of entries (in this case potentially more than 300 entries). This could make the TSR LCO unduly complex and unwieldy from a human factors reliability perspective.

In the event that no reasonably confident estimate can be made of potential MAR exceedances to support action times and surveillance frequencies, or if the LCO is too complex and unwieldy, it may be hard to defend an LCO approach. In this case, it would be appropriate to use a TSR Section 5 AC (either programmatic or Specific AC). Because of the importance of controlling MAR to within the bounds of the analyzed consequence and hazard analyses, and the need for unequivocal MAR limits in a TSR, a Specific AC is preferred. However, Specific ACs do not support action times to allow the facility some time to correct the MAR exceedance. For the case involving the use of Specific ACs directive language should be used in the form of a SHALL statement which sets the maximum MAR limit. A violation of this Specific AC limit is an immediate TSR violation in this case. As in the case of an LCO, a Specific AC of this type also requires a specific MAR limit for each location. Use of a Specific AC may not be feasible for arguments similar to those used above for an overly complex and unwieldy LCO. In this case, use of a programmatic AC may be the only, though not preferred, path to controlling MAR.

When using a programmatic AC, there must still be clear delineation of what is controlled, why it is being controlled, and a clear linkage to the Hazard/Accident analyses. Detriments to the use of programmatic ACs for major assumptions like MAR are the control tends to become buried in sub-tier documents which may be harder to control from an interpretability, mutability, and enforceability perspective. If major safety controls like MAR are placed in programmatic ACs, sub-tier procedures now become TSR-level enforceable documents thus expanding the size of the nuclear safety basis.

3.4 TSR Use and Application Modifications for Specific ACs

In both cases, the Use and Application section of the TSR should define the ground rules for treating Specific ACs, including treatment of non-compliances as TSR violations and associated 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.

3.5 Revising TSR Definitions to reflect Specific ACs

The treatment of Specific ACs which are distinguished from programmatic ACs requires the addition of related terms to Section 1 of TSRs. Specifically, the following definitions would be needed.

> Specific AC – An AC that provides a specific preventive or mitigative function for accident scenarios identified in a hazards analysis where the safety function has importance similar to, or the same as, the safety function of a safety SSC. (e.g., discrete operator actions, combustible loading program limits, hazardous material limits protecting hazard analyses or facility categorization.)

4. Training and Qualification Requirements for Specific ACs

4.1 10 CFR 830, Subpart A, Quality Assurance Requirements

The requirements for training of personnel in DOE Nuclear Facilities are clearly addressed through Section 830.121, Quality Assurance Program, and Section 830.122, Quality Assurance Criteria.

Section 830.121 requires that "(a) Contractors conducting activities, including providing items or services, that affect, or may affect, the nuclear safety of DOE nuclear facilities must conduct work in accordance with the Quality Assurance criteria in § 830.122."

Section 830.122 establishes the following criteria for Management/Personnel Training and Qualification:

a. Train and qualify personnel to be capable of performing their assigned work.
b. Provide continuing training to personnel to maintain their job proficiency.

4.2 DOE O 5480.20A

Detailed guidance on operator training programs is provided in DOE Order 5480.20A, "Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities." The Order is implemented using a graded approach at DOE Nuclear Facilities based on the facility hazard categorization. Contractors at these facilities are required to prepare a Training Implementation Matrix, which defines and describes the application of the selection, qualification, and training requirements of the Order. This Matrix includes any exceptions taken for requirements that are not implemented.

The following points should be reemphasized with respect to the selection and training requirements for ACs employed in safety-significant and safety-class applications:

Personnel Selection: The minimum qualification and experience requirements of the personnel performing the task must be carefully considered when developing important ACs. Many important ACs may require operators with special knowledge, skills, or physical abilities. In the combustible loading example previously noted, such a control will require an individual with specialized knowledge and experience in assessing the fire hazards in an area. Some controls rely on the ability of the operator to distinguish color differences or to perform strenuous tasks or gain access to relatively inaccessible areas. These specific factors must be explicitly considered in the development and implementation of the controls.

Job Task Analysis: The development of Specific ACs should be preceded by a thorough job task analysis (JTA). A JTA will identify the required plant instrumentation, physical controls, operator skills and abilities, and other important variables necessary to successfully perform the task. The JTA must include or incorporate the appropriate human factors considerations in developing the controls.

Initial Qualification Requirements: Depending on the results of the JTA, the operator training and qualification requirements must then be developed. The training requirements must carefully account for and disposition each important variable in the JTA, hazard analysis, or other basis documents being used to develop the Specific AC. Many hazard and accident analyses contain assumptions (both implicit as well as explicit) regarding the ability of the operators to detect and respond to accident scenarios. It is important that these assumptions be clearly identified and that operators are specifically trained with respect to the Specific ACs that are credited in the analysis. The training program must explicitly identify the required training for Specific ACs. Additionally, consideration must be given to the development of formal written and practical examination requirements for these ACs.

Continuing training requirements: In addition to formal, initial training requirements, the knowledge and skills set for Specific ACs must be considered for inclusion in a continuing training program. This will ensure that the important training objectives for the controls are periodically reinforced to plant operators, supervisors, and managers. Additionally, such learning objectives must be considered in formal, periodic re-qualification programs.

5. SPECIFIC AC VIOLATION REPORTING AND FAILURE ANALYSIS

5.1 Notification Requirements for Violations of Specific ACs

Violations of Specific ACs must be reported to DOE in accordance with DOE Order 231.1A, *Environment, Safety, and Health Reporting,* and DOE Manual 232.1-2, *Occurrence Reporting and Processing of Operations Information*.

5.2 Causal and Failure Analysis for Violation of Specific ACs

Specific ACs provide assurance that the basic conditions assumed by the safety analysis are met. ACs are also assigned for the conditions, the safe boundaries, and the management controls necessary to ensure the safe operation of the facility and to reduce the potential risk to the public and facility workers from uncontrolled releases of hazardous materials or energy. Specific ACs are of vital importance for the overall safe operation of a nuclear facility. Violations of Specific ACs need to have causal or failure analysis performed and lessons learned developed from the violations in an effort to minimize future violations of the Specific ACs.

Identifying the causes for Specific AC violations is often difficult. The identification of human error as a root or contributing cause of violations provides little information about how to prevent similar problems from recurring. Recognizing human performance problems when they occur and accurately identifying their causes are necessary first steps to developing effective corrective actions. The following sections outline the DOE requirements for investigating and reporting Specific AC violations but the investigation of human performance failure is difficult. The investigator(s) must be both experts in human performance and the process or facility involved in the violation. See NUREG/CR-6751, *The Human Performance Evaluation Process: A Resource for Reviewing the Identification and Resolution of Human Performance Problems*.

5.3 Investigation of Specific AC Violations

DOE G 231.1-2, *Occurrence Reporting Causal Analysis Guide*, provides guidance on how to determine the Apparent Cause(s) of specific reportable occurrences including TSR violations and to explain the structure and nodes of the Causal Analysis Tree (CAT) for use in occurrence reporting and failure analysis.

The operator of a nuclear facility must: establish a process to investigate TSR violations including Specific AC violations that may occur during operation of the facility, determine their specific or generic cause(s) and generic implications, recommend corrective actions, and report those violations to the DOE as required by 10 CFR 830.205, DOE O 231.1A and DOE M 232.1-2. The following paragraphs outline DOE's expectations as they apply to Specific AC violations.

a. The investigator(s) should be independent from the line function(s) involved with the incident under investigation.
b. Investigations should begin within 48 hours of the TSR violation, or sooner, depending on the safety significance of the violation.
c. The violation failure log required for TSRs should be reviewed as part of the investigation.
d. The operator of a nuclear facility must monitor and document corrective actions, through completion; and
e. The operator of a nuclear facility must maintain documentation so that "lessons learned" may be applied to future operations of the facility.
f. The operator of a nuclear facility must have a formal policy or procedure in place for conducting TSR violations, and the policy or procedures needs to address the following elements:

    1. A documented procedure for investigating a TSR violation. This procedure is separate from any required Emergency Plan. The investigation of a TSR violation should begin as soon as possible, commensurate with the safety of the investigator(s), after the facility has been brought to a safe and stable state;
    2. A description of the functions, qualifications, and responsibilities of the investigator(s), the scope of the investigator(s) authority and responsibilities, and assurance of cooperation of management;
    3. Assurance of the investigator(s) authority to obtain all the information considered necessary, and independence from responsibility for or to the functional area involved in the violation under investigation;
    4. Procedures requiring maintenance of all documentation relating to TSR violations for 2 years or for the life of the operation, whichever is longer;
    5. Guidance for personnel conducting the investigation on how to apply a reasonable, systematic, structured approach to determine the cause(s) of the

problem consistent with the requirements of DOE O 231.1A and DOE M 232.1-2 and the guidance in DOE G 231-1. The level of investigation should be based on a graded approach relative to the severity of the violation and any resulting incident. Generally, any TSR violation is at least category SC2, although the Facility Manager may raise the designation (see Section 6 of DOE M 231.1-2). Violation of a Safety Limit is significance category SC1;

6. Requirements to make available, to the DOE, original investigation reports on request;
7. A system for monitoring to ensure completion of appropriate corrective actions;
8. Qualified internal or external investigators are trained to serve on investigating teams when required. The teams should include at least one process expert and at least one team member should be trained in root-cause analysis;
9. Auditable records and documentation related to TSR violations, investigations, and cause analyses are maintained. For each TSR violation, the incident report should include a description, contributing factors, causal analysis, and findings and recommendations. Relevant findings are reviewed with all affected personnel, and;
10. Two violations of the same Specific AC within a period of 12 months should be treated as a significance category SC1 and should be investigated by a trained team as if it were the violation of a Safety Limit. Note that this would then be the basis for a full investigation team rather than a single trained investigator as described in DOE G 231-1-2.

5.4 Specific AC Violation Reporting

The Final Report must be prepared and submitted as soon as practical but within 45 calendar days after initial categorization of the violation. The Final Report must be prepared using the writing instructions listed in Section 5.4.1 of DOE M 231.1-2 and must document the following:

a. The significance, nature, and extent of the violation;
b. The causes of the violation or condition (including the root cause, as required) using the codes provided in the CAT;
c. The immediate actions taken and the corrective action(s) to be taken; and
d. The lessons learned.

6. Figures

Figure 1 – Example LCO Format for Specific ACs

(TRU Waste Storage Facility)

<u>3/4 OPERATING LIMITS AND SURVEILLANCE REQUIREMENTS</u>

3.3 TRU Waste Storage Facility Material at Risk (MAR) Inventory Control

LCO: The quantity of nuclear material in containerized waste at TRU Waste Storage Facility **SHALL NOT** exceed the following MAR limits:

------------------------------------NOTE---

All MAR inventory limits are provided in curies equivalent of Pu239 unless otherwise stated. ---

1. The total quantity of nuclear material present at WASTE STORAGE FACILITY SHALL NOT exceed 2000 Curies.

<u>AND</u>

2. No single 55 gallon drum shall be ≥ 150 Curies

<u>OR</u>

3. No waste boxes or crates shall ≥ 300 Curies

MODE APPLICABILITY: At All Times [This should probably be "Modes," e.g., Static Storage, Movement of Material, etc.]

PROCESS AREA APPLICABILITY: Entire Facility

3.3 Limiting Condition for Operation: TRU Waste Storage Facility MAR Inventory Control ACTION(s)

CONDITION	REQUIRED ACTION COMPLETION	TIME
A. Total inventory of material within drums and waste boxes is exceeded	A.1 Suspend all waste container receipts at WASTE STORAGE FACILITY. **<u>AND</u>** A.2 Bring WASTE STORAGE FACILITY into compliance with quantity limits.	1 Hour 3 Weeks

B. Waste container Material at Risk limits are exceeded	B.1 Suspend all waste container movements within 10 feet of the non-compliant waste container. **AND** B.2.1 Remove the non-compliant waste container from WASTE STORAGE FACILITY **OR** B.2.2 Bring the non-compliant waste container into compliance with the material at risk limits.	1 Hour 3 Weeks 3 Weeks

SURVEILLANCE REQUIREMENTS	FREQUENCY
SR 3.3.1 Verify that quantities of waste in containers do not exceed the total limits for combined drums and waste boxes	Monthly
SR 3.3.2 Verify that the gram [Though this was supposed to be curies.] content of a containerized waste item that is to be received at Waste Storage Facility does not exceed the material at risk limits.	Before shipment OR At receipt

BASES:

BACKGROUND SUMMARY	Inventory Control and Material Management provides control for the location, storage configuration, and handling of nuclear material within WASTE STORAGE FACILITY based on the quantity, type, and form. This element protects the assumptions of the accident analysis that limit the amount of MAR available for potential release in the event of an accident.

APPLICATION TO SAFETY ANALYSIS	Accidents resulting from a breach of TRU waste containers can result in significant consequences to workers and potentially the public. Specific controls and restrictions are placed on radiological material inventory (containerized waste items and WASTE STORAGE FACILITY) to prevent the introduction of materials into WASTE STORAGE FACILITY that would invalidate the safety basis.
LCO 3.3	The total quantity of containerized waste that can be stored in WASTE STORAGE FACILITY is restricted to 2,000 plutonium-239 equivalent curies. Compliance shall be demonstrated by tracking the total quantity of nuclear material present within all waste boxes and other containers. The LCO set the initial MAR for accident scenarios that involve the entire WASTE STORAGE FACILITY waste inventory (*i.e.,* major fire, seismic). The initial MAR determination for these scenarios is based on projected waste container loading to the Site 95th UCL + 20% values. Using these values represents a very conservative MAR determination for the entire WASTE STORAGE FACILITY inventory. The MAR loadings for the highest estimated single TRU containers were used in the safety analysis for scenarios involving just a few waste containers and are carried forward as requirements. Compliance with these requirements can be demonstrated by utilizing the Waste and Environmental Management System (WEMS) database and process knowledge, scan data, radiological surveys, or other assessment methods indicating that the waste is TRU. Therefore, WEMS must contain a curie value or a waste type designation of TRU prior to acceptance of a container. High americium wastes do not fall in the category of TRU and are not evaluated in this safety analysis.
MODE APPLICABILITY	Waste storage is the only activity conducted in the WASTE STORAGE FACILITY.

ACTIONS A.1 and A.2	If WASTE STORAGE FACILITY exceeds the total quantity of material permitted, the building shall be brought into compliance to re-establish the assumptions of the WASTE STORAGE FACILITY specific safety analyses. Compliance may be re-established by removing container(s) from WASTE STORAGE FACILITY, re-assay to obtain a more accurate count, or expert review of an existing assay. Bringing WASTE STORAGE FACILITY into compliance within 3 weeks is required. Three weeks is considered adequate time for facility management to identify, communicate with, and coordinate a transfer to an appropriate on-site facility.
ACTIONS B.1 through B.2.2	If a waste container in WASTE STORAGE FACILITY contains more that the specified nuclear material at risk limits, all container movement in the vicinity of the non-compliant waste container must be suspended within 1 hour. Based upon the simplicity of the container movement activities in WASTE STORAGE FACILITY, one hour is judged to be adequate to notify all workers in the vicinity to suspend movement activities and to safely secure the handling equipment and waste containers involved. If a waste container in WASTE STORAGE FACILITY contains more than the specified nuclear material limits, the waste container is to be removed from the facility or brought into compliance to re-establish the assumptions of the WASTE STORAGE FACILITY specific safety analyses within 3 weeks. Compliance may be established by re-assay to obtain a more accurate count or expert review of an existing assay. Three weeks is considered adequate time for facility management to identify, communicate with, and coordinate a transfer to an appropriate on-site facility or to re-establish container compliance. An increase in a specific waste container MAR does not have any impact on contiguous waste containers, other than for issues dealing with criticality. Therefore, for all accidents not involving a criticality, high MAR containers do not require container segregation. The Criticality Safety Program is credited for handling any criticality issues related to high MAR containers and their movement. The likelihood of an occurrence of an accident involving identified high MAR waste container(s) is small during the maximum three-week interval for removal.

SR 3.3.1 and 3.3.2	Performance of SR 3.3.1 and 3.3.2 on a monthly basis assurances WASTE STORAGE FACILITY compliance with material at risk limits. Performance of SR 3.3.1 and 3.3.2 “before shipment” OR “at receipt” assures that WASTE STORAGE FACILITY is operated within the bounds of the safety analysis. A WEMS query may be used to perform SR 3.3.1, and SR 3.3.2.

Figure 2 – Example Directive Action Format for Specific ACs

Material-at-Risk Limit

Critical Safety Function

The material-at-risk (MAR) limit is the initial underlying assumption for the accident analysis performed in Chapter 3 of the DSA. The MAR limit protects this assumption and ensures that the consequences determined in the accident scenario are not invalidated placing the facility in formally unanalyzed space.

Control Description

The facility tritium limit SHALL be ≤ 50 grams.

Basis

The accident scenario in Chapter 3 of the DSA that produced the highest dose consequences (bounding scenario) to the public assumed a facility wide fire that consumed the entire facility inventory of 50 grams of tritium with 100% oxidation. Assuming a 100% oxidation of the tritium produces the highest dose conversion factor (DCF) for tritium uptake of 96 rem/Ci. Therefore, the MAR limit for the facility must be set to ≤ 50 grams of tritium to ensure that the bounding consequences are not exceeded as analyzed in the DSA.

7. CONCLUDING MATERIAL

Review Activity:
EM
NNSA
EH
NE
SC

Preparing Activity:
DOE-EH

Project Number:
SAFT-0091

Field and Operations Offices
CBFO
CH
ID
OH
OR
ORP
RFFO
RL
SR

Area and Site Offices
Argonne Area Office
Brookhaven Area Office
Livermore Site Office
Los Alamos Site Office
Nevada Site Office
Pantex Site Office
Savannah River Site Office
Sandia Site Office
Y-12 Site Office