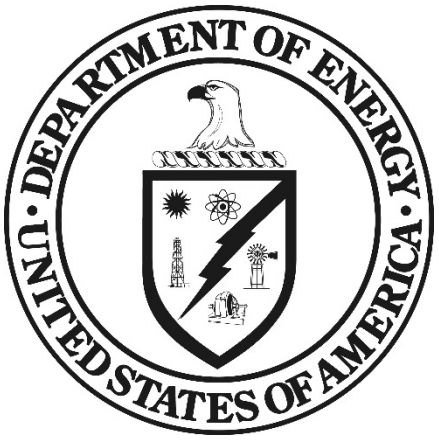
NOT MEASUREMENT SENSITIVE

DOE-STD-1186-2016
December 2016

DOE STANDARD

SPECIFIC ADMINISTRATIVE CONTROLS



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

FOREWORD

1. This Department of Energy (DOE) Standard (STD) has been approved for use by DOE, including the National Nuclear Security Administration, and their contractors.

2. Beneficial comments (recommendations, additions, and deletions), as well as any pertinent data that may be of use in improving this document should be e-mailed to nuclearsafety@hq.doe.gov or addressed to:

   Office of Nuclear Safety (AU-30)
   Office of Environment, Health, Safety and Security
   U.S. Department of Energy
   19901 Germantown Road
   Germantown, MD 20874

3. This Standard provides acceptable methods for developing and implementing Specific Administrative Controls (SACs) at DOE's Hazard Category 1, 2, and 3 nuclear facilities. A SAC is an administrative control that is identified to prevent or mitigate a hazard or accident scenario and has a safety function that would be safety significant or safety class if the function were provided by a structure, system, or component.

4. Throughout this Standard, the word "shall" denotes actions that are required to satisfy this Standard. The word "should" is used to indicate recommended practices. The use of "may" with reference to application of a procedure or method indicates that the use of the procedure or method is optional. To use this Standard, in support of an acceptable methodology for meeting the requirements of 10 CFR Part 830, *Nuclear Safety Management*, for preparing DSAs, all applicable "shall" statements need to be met.

DEDICATION

This Standard is dedicated to Jeff Shackelford; a strong advocate for nuclear safety, including clear and effective Specific Administrative Controls.

TABLE OF CONTENTS

DEFINITIONS

Note: The origins of the definitions below are indicated by references shown in square brackets [ ]. If no reference is listed, the definition originates in this Standard and is unique to its application.

Accident. A specific event or progression of a sequence of events resulting from an initiating event that is followed by any number of subsequent events that may lead to a release of radioactive or other hazardous material and/or exposure to a predefined receptor. [DOE-STD-3009-2014]

Accident analysis. The process of deriving a set of formalized design/evaluation basis accidents from the hazard evaluation and determining their consequences. Accident analysis results are used to identify the need to designate safety class and safety significant controls. [DOE-STD-3009-2014]

Administrative controls. Provisions relating to organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility. [10 CFR § 830.3]

Decommissioning. Those actions taking place after deactivation of a nuclear facility to retire it from service, and includes surveillance and maintenance, decontamination, and/or dismantlement. [10 CFR Part 830, Appendix A, Table 3]

Decontamination. The removal or reduction of residual radioactive and hazardous materials by mechanical, chemical, or other techniques to achieve a stated objective or end condition. [10 CFR Part 830, Appendix A, Table 3]

Design basis. The set of requirements that bound the design of structures, systems, and components within the facility. Some, but not necessarily all, aspects of the design basis are important to safety. [DOE-STD-3009-2014]

Documented safety analysis (DSA). A documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety. [10 CFR § 830.3]

Facility. A defined assembly of equipment, structures, systems, processes, excavations, or activities that fulfills a specific purpose. Examples include accelerators, storage areas, fusion research devices, nuclear reactors, production or processing plants, radioactive waste disposal systems and burial grounds, environmental restoration activities, testing laboratories, research

laboratories, transportation activities and accommodations for analytical examinations of irradiated and non-irradiated components. [DOE-STD-3009-2014]

Graded approach. The process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement in this Standard is commensurate with:

- The relative importance to safety, safeguards, and security;
- The magnitude of any hazards involved;
- The life cycle stage of a facility;
- The programmatic mission of a facility;
- The particular characteristics of a facility;
- The relative importance of radiological and non-radiological hazards; and
- Any other relevant factor.

[10 CFR § 830.3]

Hazard. A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to a person or damage to a facility or to the environment (without regard to the likelihood or credibility of accident scenarios or consequence mitigation). [10 CFR § 830.3]

Hazard analysis. The identification of materials, systems, processes, and plant characteristics that can produce undesirable consequences (hazard identification), followed by the assessment of hazardous situations associated with a process or activity (hazard evaluation). Qualitative techniques are usually employed to pinpoint weaknesses in design or operation of the facility that could lead to accidents. The hazard evaluation includes an examination of the complete spectrum of potential accidents that could expose members of the public, onsite workers, facility workers, and the environment to radioactive and other hazardous materials. [DOE-STD-3009-2014]

Hazard categorization. Evaluation of the consequences of unmitigated radiological releases to categorize facilities in accordance with the requirements of 10 CFR Part 830. Note: 10 CFR Part 830 requires categorization consistent with DOE-STD-1027, Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports. [DOE-STD-3009-2014]

Hazard controls. Measures to eliminate, limit, or mitigate hazards to workers, the public, or environment, including: (1) physical design, structural, and engineering features; (2) safety structures, systems, and components; (3) safety management programs; (4) technical safety

requirements; and (5) other controls necessary to provide adequate protection from hazards. [10 CFR § 830.3] Note: "hazard controls" include "specific administrative controls."

Hazard scenario. An event or sequence of events associated with a specific hazard, having the potential to result in undesired consequences identified in the hazard evaluation. [DOE-STD-3009-2014]

Hazardous material. Any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise could adversely affect the health and safety of the public or the workers or harm the environment. [DOE-STD-3009-2014]

Limiting conditions for operation (LCOs). The limits that represent the lowest functional capability or performance level of safety structures, systems, and components required for safe operations. [10 CFR § 830.3]

Mitigative control. Any structure, system, component or administrative control that serves to mitigate the consequences of a release of radioactive or other hazardous materials in a hazard or accident scenario. [DOE-STD-3009-2014]

Nonreactor nuclear facility. Those facilities, activities, or operations that involve, or will involve, radioactive and/or fissionable materials in such form and quantity that a nuclear or a nuclear explosive hazard potentially exists to workers, the public, or the environment, but does not include accelerators and their operations and does not include activities involving only incidental use and generation of radioactive materials or radiation such as check and calibration sources, use of radioactive sources in research and experimental and analytical laboratory activities, electron microscopes, and X-ray machines. [10 CFR § 830.3]

Nuclear facility. A reactor or a nonreactor nuclear facility where an activity is conducted for or on behalf of DOE and includes any related area, structure, facility, or activity to the extent necessary to ensure proper implementation of the requirements established by 10 CFR Part 830. [10 CFR § 830.3]

Preventive control. Any structure, system, component or administrative control that eliminates the hazard; terminates the hazard scenario or accident; or reduces the likelihood of a release of radioactive and/or hazardous materials. [DOE-STD-3009-2014]

Public. All individuals outside the DOE site boundary. [DOE-STD-3009-2014]

Safety analysis. A documented process to: (1) provide a systematic identification of both natural and man-made hazards associated with a facility; (2) evaluate normal, abnormal, and accident conditions; (3) derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, and demonstrate their adequacy; and (4) define the characteristics of the safety management programs necessary to ensure the safe operation of the facility. [DOE-STD-3009-2014]

Safety basis. The documented safety analysis 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. [10 CFR § 830.3]

Safety class (SC). Classification of a hazard control that indicates the control provides a preventive or mitigative function that is necessary to limit radioactive hazardous material exposure to the public, as determined from safety analyses.

Safety class structures, systems, and components (SC SSCs). Structures, systems, or components, including portions of process systems, whose preventive or mitigative function is necessary to limit radioactive hazardous material exposure to the public, as determined from safety analyses. [10 CFR § 830.3]

Safety limits (SLs). Limits on process variables associated with those safety class physical barriers, generally passive, that are necessary for the intended facility function and that are required to guard against the uncontrolled release of radioactive materials. [10 CFR § 830.3]

Safety management program (SMP). A program designed to ensure that a facility is operated in a safe manner that adequately protects workers, the public, and the environment by covering a topic such as quality assurance; maintenance of safety systems; personnel training; conduct of operations; inadvertent criticality protection; emergency preparedness; fire protection; waste management; or radiological protection of workers, the public, and the environment. [10 CFR § 830.3]

Safety significant (SS). Classification of a hazard control that indicates the control provides a preventive or mitigative function that is a major contributor to defense-in-depth and/or worker safety, as determined from safety analyses.

Safety significant structures, systems, and components (SS SSCs). Structures, systems, and components which are not designated as safety class SSCs, but whose preventive or mitigative function is a major contributor to defense-in-depth and/or worker safety, as determined from safety analyses. [10 CFR § 830.3]

Safety structures, systems, and components (Safety SSCs). Both safety class structures, systems, and components, and safety significant structures, systems, and components. [10 CFR § 830.3]

Specific administrative control (SAC). An administrative control that is identified to prevent or mitigate a hazard or accident scenario and has a safety function that would be safety significant or safety class if the function were provided by a structure, system, or component. [DOE-STD-3009-2014]

Technical safety requirements (TSRs). The limits, controls, and related actions that establish the specific parameters and requisite actions for the safe operation of a nuclear facility and include, as appropriate for the work and the hazards identified in the DSA for the facility: safety limits, operating limits, surveillance requirements, administrative and management controls, use and application provisions, and design features, as well as a bases appendix. [10 CFR § 830.3]

ABBREVIATIONS AND ACRONYMS

CFR	Code of Federal Regulations
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
G	Guide
JTA	Job Task Analysis
LCO	Limiting Conditions for Operation
MAR	Material-at-Risk
NNSA	National Nuclear Security Administration
O	Order
SAC	Specific Administrative Control
SC	Safety Class
SMP	Safety Management Program
SR	Surveillance Requirement
SS	Safety Significant
SSC	Structure, System, and Component
STD	Standard
TSR	Technical Safety Requirement
USQ	Unreviewed Safety Question
WEMS	Waste and Environmental Management System

1 INTRODUCTION

1.1 SCOPE AND PURPOSE

This Standard provides requirements and guidance on acceptable methods for developing and implementing Specific Administrative Controls (SACs) at nuclear facilities operated by the Department of Energy (DOE). A SAC is an administrative control that is identified to prevent or mitigate a hazard or accident scenario and provides a safety function that would be safety significant or safety class if the function were provided by a structure, system, or component. Appropriate use of SACs at DOE's nuclear facilities can significantly enhance the safety of DOE's nuclear facilities.

The organization of this Standard is as follows: Section 1 defines SACs and describes the existing requirements for derivation of safety bases, including hazard analyses, identification of hazard controls, derivation of Technical Safety Requirements (TSRs), and the role of SAC in the TSRs. Section 2 describes methods for identifying, formulating, implementing, and maintaining SACs. Section 3 provides methods to improve the dependability of SACs. Section 4 provides acceptable methods for use of SACs in TSRs. Section 5 describes reporting and investigation of violations of SACs. Section 6 presents TSR examples.

1.2 APPLICABILITY

This Standard applies to all DOE elements, including the National Nuclear Security Administration (NNSA), and all DOE and NNSA contractors for design and operation of DOE's nuclear facilities. This Standard is intended to support preparation of Documented Safety Analyses (DSAs) complying with the identified "safe harbor methods" of Title 10 Code of Federal Regulation (CFR) Part 830, and the associated TSRs. For example, this Standard may be used with DOE Standard (STD) 3009-94, CN3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*, or other safe harbor standards or alternate methods approved for use in preparing the associated DSA.

1.3 USE OF THIS REVISION WITH EXISTING, APPROVED SACS

This section addresses use of this revision of this Standard with SACs that were approved and implemented prior to the issuance of this Revision. This Standard was revised to be consistent with current, approved directives and standards, including DOE-STD-3009-2014 and DOE Order (O) 420.1C, *Facility Safety*. In some cases, these more recent directives and standards have clarified key concepts such as hierarchy of safety controls and importance of support systems.

This Standard provides an acceptable method for development and implementation of SACs. Other methods may be used when their use is justified and appropriate. Compensatory measures

may be necessary when the methods in this Standard are not fully applied.

A review of each existing, approved SAC against the contents of this Revision is neither required nor intended. When existing SACs are revised, the application of this Standard should be considered. If this Standard is applied, existing SACs should be evaluated against the contents of this Revision to identify any gaps, assess potential vulnerabilities, and determine the need to update the SACs. Such evaluations may be performed as part of the DSA annual update process.

1.4 BACKGROUND

Section 830.3 of 10 CFR Part 830 defines administrative controls as the provisions relating to organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility. Administrative controls are identified in DSAs or TSRs for DOE nuclear facilities. Administrative controls include (1) administrative provisions, such as reporting requirements, (2) staffing requirements, and (3) commitments to Safety Management Programs (SMPs).

In 2002, the Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2002-3, *Requirements for the Design, Implementation, and Maintenance of Administrative Controls*, which recommended increased attention to administrative controls used for safety class and safety significant functions. In 2003, DOE issued Nuclear Safety Management Technical Position 2003-1, *Use of Administrative Controls for Specific Safety Functions*, which introduced the concept of "Specific Administrative Controls." This document evolved into DOE-STD-1186-2004, *Specific Administrative Controls*, the predecessor of this revision.

Subsequent to issuance of DOE-STD-1186-2004, DOE assessed the existing set of SACs against the new standard and upgraded them where necessary. This revision of the Standard reflects the lessons learned and good practices derived from the SAC assessment and upgrade effort. In addition, this revision also reflects updates to various DOE directives and technical standards governing safety analysis and facility design.

1.5 SAFETY BASES AND HAZARDS CONTROLS

Subpart B of 10 CFR Part 830, "Safety Basis Requirements" requires contractors responsible for hazard category 1, 2, and 3 nuclear facilities to develop safety bases for those facilities. The safety bases comprise DSAs and associated hazard controls, including those in TSRs derived from the DSA's hazard analyses. The provisions in 10 CFR §830.204(b)(4) require that a DSA "derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use."

Various guides and technical standards, such as this Standard and the DSA safe harbor methodologies listed in 10 CFR Part 830, Appendix A, Table 2, provide guidance and acceptable methods to interpret and implement safety basis requirements. DOE O 420.1C [Attachment 2, Chapter I, Section 3.a (2).(c)] requires that safety analyses be used to identify SACs needed to fulfill safety functions.

Safety analyses identify SACs, their functions, and their safety significance. Safety analyses are then compiled in the DSA, which identifies safety functions of SACs and documents the adequacy of each SAC to its assigned safety functions in the DSA. SACs provide a safety function that would be Safety Significant or Safety Class if the function were provided by a Structure, System, and Component (SSC).

DOE-STD-3009-2014 provides an acceptable method for preparing a DSA for nonreactor nuclear facilities. It also provides detailed guidance for preparation of DSAs, including the derivation of TSRs.

1.6 SELECTION AND HIERARCHY OF CONTROLS

Preventive or mitigative controls are selected using a judgment-based process that applies hierarchy of control preferences. DOE has established a control selection strategy based on a hierarchy of controls. DOE O 420.1C, Attachment 2, Chapter I, Section 3(b)(4)(d) requires that new nuclear facilities and major modifications to existing nuclear facilities be designed to "*provide controls consistent with the hierarchy described in DOE-STD-1189-2008.*" The second principle of DOE-STD-1189-2008 "Safety Design Guiding Principles" presents this hierarchy, which was subsequently clarified in DOE-STD-3009-2014.

Following efforts to minimize hazardous materials, this control selection strategy translates into the following hierarchy of controls, listed from most preferred to least preferred.

(1) SSCs that are preventive and passive

(2) SSCs that are preventive and active[1]

(3) SSCs that are mitigative and passive

(4) SSCs that are mitigative and active

(5) Administrative controls that are preventive

(6) Administrative controls that are mitigative

[1] An exception to this hierarchy is that active confinement ventilation is preferred over passive confinement systems.

Based on this hierarchy, administrative controls, including SACs, represent the least preferred means of implementing safety controls. While SACs can provide acceptable and effective controls, they should only be used if adequate engineered controls are not readily available. In general, SSCs are preferable to SACs due to the uncertainty of human performance inherent in implementation of SACs. However, it is not always possible to follow the hierarchy of controls stated above, particularly for existing nuclear facilities.

In cases where SSCs are not plausible or practical for accomplishing a required safety function, the safety basis is expected to provide a discussion to support use of SACs in lieu of SSCs. (Note: Section 3.3 of DOE-STD-3009-2014 includes a requirement that a technical basis be provided to support the controls selected; Section 4.5.X.2 of DOE-STD-3009-94, CN3, provides a similar expectation, "*If a SAC is utilized in lieu of the identification of safety SSCs, clearly identify and discuss the rationale for this decision.*"; and DOE-STD-1189-2016, *Integration of Safety into the Design Process*, also provides similar requirements for new DOE nuclear facilities and major modifications to existing DOE nuclear facilities). This discussion should address the various engineered options available and why they were not selected; this is necessary so that the approving official can clearly gauge the appropriateness of selecting administrative controls in lieu of engineered features. In cases where no SSCs are part of the credited control strategy and it is plausible that an SSC could provide the required safety function, the technical basis should address consideration of potential upgrades or modification of engineered features such that the final suite of controls does not rely entirely on administrative controls. For existing DOE nuclear facilities with approved DSAs, the costs and benefits of facility hardware changes may be considered when making decisions between SSCs and SACs for necessary hazard controls.

Where failure of a supporting SSC (such as an indication) would result in losing the ability to initiate or perform the action required by the SAC, such SSCs are required by DOE O 420.1C (Attachment 3, Section 3.a.(5)) to be designated as safety class or safety significant for new nuclear facilities and major modifications. DOE-STD-3009-2014, Section 3.3 provides the following additional direction for existing facilities:

> *"For existing facilities, support SSCs shall be designated at the same classification (SC or SS) as the safety controls they support, or else compensatory measures shall be established to assure that the supported safety [control] can perform its safety function when called upon.*
>
> *SSCs whose failure would result in losing the ability to complete an action required by a SAC shall be identified. These SSCs shall be designated as SC or SS based on the SAC safety function, or justification provided if not so designated."*

This requirement is consistent with the expectation in DOE-STD-3009-94, Chg. 3, Section 4.5.X.2:

> *"Identify SSCs whose failure would result in losing the ability to complete the action required by the SAC. These SSCs would also be considered safety-class or safety-significant based on the significance of the SAC safety function."*

Where there are multiple SSCs that can provide necessary support for a SAC, losing one method may not prevent the ability to complete the action required by the SAC. Where multiple SSCs are available, at least one SSC would typically be classified as a safety SSC unless adequate technical justification can be provided. Such a justification should consider a number of factors such as the reliability and diversity of the SSCs when they are required to function, and the time needed to perform the SAC using alternate support SSCs if failure is detected.

While SACs may be acceptable for ensuring safe operation, they generally provide lower reliability compared with engineered controls. The actual design and selection process should consider the ensemble of controls used to address a hazard, balancing factors such as cost, implementation effort, risk reduction, availability, required reliability, and consequence of mechanical or human failure for each potential control. In comparison to other administrative controls, SACs have elevated safety significance, and more stringent implementation and verification requirements to ensure their effectiveness and dependability, as described in this Standard.

1.7 SACS FOR HAZARDOUS MATERIAL INVENTORY LIMITS

Where necessary and feasible, SACs should be used to control or limit material-at-risk (MAR) and other important physical attributes, such as waste acceptance criteria on radiological or fissile concentrations, by establishing material inventory limits for a given facility. In cases where fire is a concern, for example, a SAC might be used to control the facility's inventory of combustible materials. If the facility contains a dangerous substance such as plutonium that could be released in certain types of accidents, a SAC might be used to control how much plutonium is permitted in the facility at any given time (a MAR limit). With the one exception of hazardous material inventory limits (and any associated waste acceptance criteria or material concentration limits), SACs should not be used to protect assumptions in the unmitigated accident analysis.

1.8 SACS FOR SPECIFIC ASPECTS OF SAFETY MANAGEMENT PROGRAMS

Controls related to a SMP may or may not be SACs, based on the designations derived from the hazards and accident analyses in the DSA. In general, programmatic administrative controls recognized as part of SMP descriptions are not intended to be used to provide specific limits or

define mitigative actions for accident scenarios identified in DSAs where the safety function has importance similar to, or the same as, the safety function of SC or SS SSCs. Designating the entire SMP as a SAC is also not appropriate because a SMP description does not provide a specific credited safety function. However, SACs are appropriate when a specific aspect of a SMP is credited in the safety analysis and provides a specific safety function, which may include major contributions to defense-in-depth. SACs should not be confused with the key elements of SMPs, identified in Chapter 7 of a DSA. DOE-STD-3009-2014 briefly explains the distinction as follows:

> "*Key elements are those that: (1) are specifically assumed to function for mitigated scenarios in the hazard evaluation, but not designated an SAC; or, (2) are not specifically assumed to function for mitigated scenarios, but are recognized by facility management as an important capability warranting special emphasis. It is not appropriate for a key element to be identified in lieu of a SAC. The basis for selection as a key element, as specified in the safety analysis, includes detail on how the program element: (1) manages or controls a hazard or hazardous condition evaluated in the hazard evaluation; (2) affects or interrupts accident progression as analyzed in the accident analysis; and (3) provides a broad-based capability affecting multiple scenarios.*"

2 IDENTIFICATION, FORMULATION, IMPLEMENTATION, AND MAINTENANCE OF SACS

2.1 IDENTIFICATION OF SACS

SACs shall be designated where an administrative control performs an SC or SS safety function to prevent or mitigate a postulated hazard or accident scenario. SACs should also be designated in the following conditions:

a. The administrative control is the basis for validity of the hazard or accident analyses (e.g., a hazardous material inventory, such as an assumed MAR); or

b. An administrative control provides the main mechanisms for hazard control (e.g., safety SSCs are degraded, out of service, too costly to implement, or impractical for a limited-life facility)

As described in Section 1.6, SACs should only be specified if adequate engineered controls are not readily available.

The DSA is required to describe the SAC safety function and bases for each SAC. The safety function and bases should clearly tie to the hazard evaluation or accident analysis. The specific accident(s) or general rationale (e.g., to protect initial conditions of the analysis) associated with the safety function are identified. There may, or may not be, a single accident that, by itself, completely defines the safety function.

The DSA also provides a description of the SAC and the basic principles by which it performs its safety function. The discussion should be clear as to the actions necessary to satisfy the safety function (e.g., how much time is necessary, how the actions are verified, the periodicity of verification, availability of indications, etc.). Also described are boundaries and interface points with any SSCs relevant to the safety function, such as manual actions interfacing with sensors, instrumentation and other equipment. If a SAC is used in lieu of safety SSCs, the DSA describes the rationale for this decision. When describing the SAC, provide a basic summary of the physical information known about the SAC, including: tables or drawings showing relevant information (such as instrumentation); any relevant SSCs; physical boundaries; approved storage areas; and, operator routes or locations.

The DSA also specifies the functional requirements for both the SAC and any needed supporting SSCs. Functional requirements are to be described for the specific accident(s) where the SAC may be relied on. Functional requirements for SACs may involve ensuring unimpeded access to specific rooms or areas, use of certain instrumentation, written procedures or checklists, and special tooling. Functional requirements specifically address the pertinent response parameters or non-ambient environmental stresses related to an accident for which the safety function is relied on. Functional requirements are derived from the hazard and/or accident analysis as necessary to provide the SAC safety function. Such requirements are specified for both the SAC and any needed supporting SSCs.

2.2 FORMULATION OF SACS

The general approach to formulating SACs, as described in this Standard, parallels existing guidance for designing safety SSCs. Attachment 2, Chapter I, and Attachment 3 of DOE O 420.1C provides design requirements for nuclear safety controls.

SACs are required to perform their identified safety functions when called upon. The degree of rigor in formulation of the SAC should be commensurate with the importance of the safety function. The SAC, in concert with other hazard controls, should provide multiple levels of protection against normal, anticipated, and accident conditions. The practicality of a SAC is ensured by engineering evaluations and experience.

If a SAC relies on operator actions to perform its safety function, a human factors analysis should be performed as part of the SAC formulation to: (1) validate the dependability of a SAC, (2) identify any weaknesses in the proposed approach for implementing the SAC, and (3) suggest additional measures to improve the overall dependability. Formal engineering calculations may be necessary to ensure that plant operators have adequate time and resources to carry out required tasks. (Note: ANSI/ANS-58.8-1994, *Time Response Design Criteria for Safety-Related Operator Actions*, may be helpful in ensuring minimum response times are appropriate). For example, if a SAC requires that operators take action to locate and isolate a leak, flow rate

calculations would be needed to justify the time interval needed to accomplish the task. Consequences of incorrect implementation of the control should be evaluated, and measures to prevent control failure should be factored into the control formulation.

Redundancy, independence, and diversity of hazard controls are also important principles for ensuring that a high consequence accident does not occur due to the failure of a single barrier. When SACs are part of the hazard control ensemble, these principles are applied to the ensemble. If a SAC is the primary line of defense for protection of the public (i.e., provides a safety function that would be classified as safety class), these principles should be applied to the SAC to the extent possible. The terms redundant, independent, and diverse are discussed below.

Redundant: Redundancy refers to using at least two independent, identical controls to carry out a required safety function. An SSC-related example might be providing two diesel generators for backup power when only one is necessary in a loss of offsite power event. A SAC-related example might be taking and analyzing two samples of waste for characterization before a transfer is made, or taking and analyzing two samples for fissile material concentration before a solution is transferred from a pencil tank to a geometrically unsafe condition.

Independent: Independence refers to preventing, to the extent possible, a common mode failure, such as a fire or earthquake from affecting redundant safety systems. In the diesel generator example above, measures to ensure independence might include separating the redundant generators by a fire barrier and seismically qualifying at least one of the units and its fuel supply. For a waste characterization SAC, an example would be taking two samples of waste from different locations and sending them to different laboratories for analysis; and for fissile concentration SAC, an example might be sending a sample to the lab for analysis and doing an in-situ Non-Destructive Analysis of the tank solution.

Diverse: Diversity refers to averting a common mode failure by using two or more different methods of achieving a specified safety function. An SSC example might be providing both an automatic and a manual control for actuating a fire protection system. A waste characterization SAC example of diverse controls could involve taking samples for lab analysis and ensuring that the ventilation system is operable and reliable (e.g., if the concern is hydrogen generation); and for fissile materials transfer, it could involve lab analysis of the samples and radiation monitoring of the transfer line to indicate solution concentration as it passes through.

When SACs are part of the hazard control strategy, these principles should be applied to the entire set or ensemble of hazard controls to ensure that safety-class functions for protection of the public can be achieved.

The DSA required by 10 CFR § 830.204 furnishes the technical basis for hazard controls. 10 CFR 830 requires the DSA to demonstrate the adequacy of hazard controls to eliminate, limit, or mitigate identified hazards. DOE-STD-3009-2014 provides guidance to identify and document SACs as required in Chapter 4 of a DSA. Technical justification for selection of a SAC over an engineered control (i.e., why SSCs are not plausible or practical for accomplishing the safety function) is also expected to be included in the DSA. The DSA also provides the basis for classification of the SAC and describe its preventative or mitigative safety function. A description of how the SAC is to be implemented (e.g., important procedural features, including interfaces with sensors, etc.) should be presented in the DSA. Pertinent aspects of the SAC that relate directly to the safety function, such as qualifications of personnel required and time available to perform associated tasks, as well as the basis for selecting the SAC assessment frequency, should be described. SACs that provide a SC safety function will need a more comprehensive discussion in the DSA compared to SACs that provide a SS safety function because of their importance to public safety.

The DSA should also provide information (generally Chapter 5 of a DSA based on DOE-STD-3009) to support the derivation of hazard controls described in the TSR document. This Chapter content is the linking document between the DSA hazard analysis that results in the designation of SACs and their required safety functions and attributes, and the TSR document. TSR and SAC procedure writers refer to the DSA to identify the accident scenarios that generated the need for the SAC (in Chapter 3), and information on its safety function and required attributes. The TSR basis portion of the DSA (typically Chapter 5) should provide a summary description of this information and references to the supporting information in hazards and control selection portions of the DSA (typically Chapters 3 and 4).

To help ensure SAC reliability, lessons learned from historical incidents involving SAC failures and violations should be incorporated into SAC formulation. For example, DOE's Occurrence Reporting and Processing System database will contain recent information relating to SAC failures and violations that could help with SAC formulation and anticipate potential problems with implementation.

Validation. The formulation of SACs should include a process to ensure that required tasks in a SAC can be performed by facility operators within the timeframes assumed in the safety basis. If a SAC requires operator action, an evaluation that addresses the following human factors shall be completed, on a graded approach:

- Adequacy and clarity of the description of required SAC actions;
- Level of difficulty of the SAC actions;
- Ergonomic design of equipment needed by the operators, such as indicators and alarms;
- Time available to do the task and to recover from errors;

- Stress caused by noise, heat, light, protective clothing, and time constraints; and
- Potentially hazardous conditions that could exist in an area requiring action under a SAC.

The SAC should be formulated so that it is verifiable through appropriate and ongoing testing, examination, and assessment activities. In the context of SACs, this verification 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 formulation of the control to assure an unbiased assessment of the effectiveness of the control. Periodic re-verification that SACs are performing, or capable of performing, their intended safety function should be addressed through Limiting Conditions for Operation (LCO) Surveillance Requirements (SR) for SACs written as LCOs, or through facility operations and maintenance procedures if the SAC is incorporated into the administrative control section of the TSRs.

2.3 IMPLEMENTATION AND MAINTENANCE OF SACS

Line Management Implementation: SACs are implemented to control facility operations using formally controlled procedures. Line management should ensure the procedures: (1) appropriately implement the SAC consistent with facility conditions, (2) are understandable (contain clear and concise work instructions with necessary detail), (3) are practical and usable, (4) are adequate for meeting the functional requirements and expectations of the SAC TSR, (5) highlight in a meaningful way those procedural steps applicable to implementing the SAC, and (6) include a mechanism to ensure reliable procedural compliance such as reader-worker method, hold points, or use-each-time. In addition, the effective implementation of SACs should also ensure that support SSCs relied upon for the SAC to perform its safety function are available, reliable, and maintained consistent with their safety classification.

Implementation Verification Reviews: SACs identified in TSRs shall be initially (prior to operation) and periodically verified to be capable of performing their intended safety function. Appendix C, *Performance of Implementation Verification Reviews (IVRs) of Safety Basis Controls,* of DOE Guide (G) 423.1-1B, *Implementation Guide for Use in Developing Technical Safety Requirements,* provides guidance on conduct of IVRs, including Form 5, *SAC Implementation Review Criteria*. The purpose of an IVR is to provide independent confirmation of the proper implementation of new or revised safety basis controls. IVRs should be conducted for the implementation of SACs identified in new or revised TSRs prior to initial use and on a periodic basis thereafter using the methods described in DOE G 423.1-1B.

Unreviewed Safety Question (USQ) Determination: Title 10 CFR Part 830 allows DOE contractors to make changes to DOE nuclear facilities without DOE approval if those changes are within the existing approved safety basis. DOE G 424.1-1B, *Implementation Guide for Use*

in Addressing Unreviewed Safety Question Requirements, provides acceptable methods for USQ programs and procedures. Changes to SAC-related TSRs require DOE approval in accordance with 10 CFR Part 830, and do not need to be evaluated by the USQ process. Changes to SAC descriptions in DSAs and implementing procedures for SACs are evaluated in accordance with the approved USQ process.

Configuration Management: DOE O 420.1C, *Facility Safety*, Attachment 2, Chapter V, states:

> *"A documented configuration management program must be established and implemented that ensures consistency among system requirements and performance criteria, system documentation, and physical configuration of the systems within the scope of the program."*

These requirements are applicable to SACs to assure the continuing ability of SACs to perform their safety function when called upon.

3 MEASURES USED TO ENSURE THE DEPENDABILITY OF SACs

3.1 HUMAN ACTIONS AS SAFETY CONTROLS

SACs, by their very nature, require human actions, and human actions tend to be less reliable than automatic systems, especially under stressful conditions. To ensure that SACs are reliable, it is important to reduce the human error rate as much as possible. The following measures, taken singly or in combination, can be used to minimize the effect of human error on SACs.

- Reader/worker/checker systems;
- Independent verification;
- Positive feedback systems;
- Interlocks;
- Warning signs and barriers;
- Alarms and monitors;
- Human factors analysis;
- Operator training and certification;
- Continuing training and re-qualification;
- Abnormal event response drills;
- Ergonomic considerations in procedures;
- Dry runs for non-routine operations;
- Double staffing;

- Direct supervision of hazardous operations; and
- Human Reliability Assessment.

3.2 CONDUCT OF OPERATIONS

The dependability of all hazard controls, including SACs, is enhanced by the conduct of operations program as set forth in DOE O 422.1, *Conduct of Operations*. Proper conduct of operations is a key SMP and is typically described in the facility DSA as such. The detailed attributes in DOE O 422.1 form a compendium of good practices and describe key elements of programs that support effective operations of DOE facilities.

Of the program elements that are listed in the Order, two of them, Independent Verification and Lockouts/Tagouts, are especially relevant to the dependability of SACs.

3.2.1 Independent Verification

SACs should be included in the facility's independent verification program. Verification methods should be identified explicitly in facility procedures or other controlled documents. DOE O 422.1 (Section 2.j of Attachment 2) provides the following specific requirements on Independent Verification Programs:

> *"The operator must establish and implement operations practices to verify that critical equipment configuration is in accordance with controlling documents, addressing the following elements:*
>
> *(1) structures, systems, components, operations, and programs requiring independent verification;*
> *(2) situations requiring independent verification;*
> *(3) methods for performing and documenting independent verification;*
> *(4) situations, if any, allowing concurrent dual verification; and*
> *(5) methods for performing concurrent dual verification, if used."*

Independent verifications in support of SACs should be conducted in a manner so that the relevant components are identified and verified and the relevant actions or conditions are verified to conform with the established SAC. Verification should be performed by a different qualified person than the one performing the SAC.

3.2.2 Lockouts and Tagouts

A Lockout/Tagout program as described in DOE O 422.1 (Section 2.i of Attachment 2) should be used to support implementation of SACs where the SACs that depend in part on the position

or condition of equipment, components, or controls be placed in during normal operations.

A lockout/tagout program meeting these requirements can provide additional assurance that the requirements of the SAC are properly implemented. A tagout program meeting the requirements and attributes in DOE O 422.1 includes the placement of a tagout device on an energy-isolating device, in accordance with an established procedure, to indicate that the energy-operating device and the equipment being controlled may not be operated until the tagout device is removed. Similarly, a lockout program that is consistent with DOE O 422.1 includes the placement of a lockout device (e.g., a lock, or hasp with a lock in place) on an energy isolating device in accordance with an established procedure ensuring that the energy-isolating device and the equipment being controlled cannot be operated until the lockout device is removed. An effective lockout/tagout program should be developed by each facility and should include detailed administrative procedures, training of personnel, and uniquely identifiable tags. The program should also exercise appropriate control over lockout/tagout preparation, approval, placement, and removal; and provide for adequate documentation.

Note: Where the implementation of SACs is dependent on a specific position or condition of equipment, components, or controls to be placed in during normal operations, then formulation of that SAC should strongly consider use of the LCO format so that the lockout tags may be serviced and removed as necessary to support maintenance and scheduled outages where hazards are minimized through other means. In such cases, directive action SACs may not provide the same flexibility for out of service equipment.

3.3 TRAINING AND QUALIFICATION FOR SACS

Effective implementation of SACs includes training and periodic re-training of operators on SACs and associated implementing procedures. Training requirements for DOE contractor personnel are provided in both 10 CFR Part 830, Subpart A, *Quality Assurance*, and in DOE O 426.2, *Personnel Selection, Training, Qualification, and Certification Requirements for DOE Nuclear Facilities*.

As a minimum, hazard analysts, personnel assigned to formulate SACs, and TSR writers should receive training on the requirements and guidance in this Standard. Training on TSRs for operations personnel should include specific training on attributes of the SACs as identified in the safety basis. Training should also cover the implementing procedures for SACs.

3.3.1 DOE O 426.2

Detailed guidance on operator training programs is provided in DOE O 426.2. 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 to requirements, which are not implemented.

The following training issues should be evaluated carefully for applicability to new SACs, and existing SACs, as defined in this Standard:

Personnel Selection: The minimum qualification and experience requirements of the personnel performing the task should be considered carefully when formulating, implementing, and maintaining SACs. Some SACs may require operators with special knowledge, skills, or physical abilities. For example, a combustible loading control may 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, to perform strenuous tasks, or gain access to relatively inaccessible areas. These specific factors shall be addressed explicitly in the formulation, implementation, and maintenance of SACs.

Job Task Analysis: The formulation of SACs should include 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 should 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 for tasks related to SACs should then be developed. The training requirements should account for and disposition each important variable in the JTA, hazard analysis, or other basis documents being used to develop the SAC. 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 to identify clearly these assumptions so that operators are specifically trained with respect to the SACs that are credited in the analysis. The training program should identify explicitly the required training for SACs. Additionally, formal written and practical examination requirements for these administrative controls should be developed and implemented.

Continuing training requirements: In addition to formal, initial training requirements, the knowledge and skills set for SACs should 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 should be considered in formal, periodic re-qualification programs.

3.4 QUALITY ASSURANCE REQUIREMENTS

Title 10 CFR 830, Subpart A, *Quality Assurance Requirements,* establishes quality assurance requirements for DOE nuclear facilities. Section 830.121(a) requires that:

> *"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."*

4 TREATMENT OF SACs IN TSRs

The TSR derivation section in the DSA provides a link between the identified hazards, safety SSCs, and SACs necessary to ensure safety.

4.1 TSR TREATMENT OF SAFETY MANAGEMENT PROGRAMS

A traditional type of TSR administrative controls relate to organization and management, procedures, record keeping, reviews, audits governing safe operations, and SMP commitments. Existing DOE directives and standards specify that the administrative control 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.

Such programmatic administrative controls are generally described in safety basis documents with a significantly lower level of specificity than that provided for SACs. Unlike SACs, these controls lack specific limits or operator actions intended to prevent or mitigate specific hazard or accident scenarios. Rather, these administrative controls contain basic program elements or features that constitute the viability of the SMP to support safe operations. As described in Section 1.8, key elements should not be confused with SACs.

Specific care needs to be taken in the application of SACs related to Nuclear Criticality Safety Programs so that the analysis is integrated between discussions in the DSA and the Nuclear Criticality Safety Evaluations.

4.2 IMPLEMENTING SACS IN TSRS

When SACs are identified, they shall be controlled through the TSR. Two formats may be used to meet this requirement: (1) LCO format, or (2) Directive Action format.

The LCO format should be used when specific corrective actions can be taken to maintain the facility within its safety basis. In such cases, the LCO and associated SRs for the SAC should be placed in the Operating Limits and SR section of the TSR, respectively.

The Directive Action format should be used when it is essential that the SAC 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 requirements for specific activities can be stated. In such cases, the Directive Action SAC should be placed in the administrative controls section of the TSRs and describe the SAC actions and any periodic review requirements.

The distinguishing feature of a Directive Action SAC is that it does not specify actions to take within a defined completion time if the SAC requirement is not met (as there are for an LCO SAC). Nevertheless, a violation of a Directive Action SAC is a TSR violation, and timely actions would be required if violated to ensure the facility is in an analyzed safe condition. Directive Action SACs should be avoided in circumstances where maintenance or system outages will be necessary, such as taking components out of service, as this could result in a TSR violation if the Directive Action SAC could not be performed. Mechanisms to ensure compliance with Directive Action SACs may take the form of periodic review, audits, or independent verifications, as opposed to the TSR Surveillance Requirements normally conducted to support LCO compliance.

Types of Directive Action SACs are described below:

a. Operator Action SACs may be developed to control a process where an operator is expected to take an action in response to a system or process event, such as an alarm. The Operator Action statement describes what the operator is expected to do in response to the event. In such cases, the SAC basis statement in the associated TSR should provide watch station staffing expectations and training requirements, justification for why operator tasks can be accomplished within allowed response times, and justification for selecting an administrative control over an engineered control. Review mechanisms may take the form of auditing operator logbooks to confirm that operator actions have been taken, when required, and within the expected response times. The review mechanisms and periodicity should be described in the SAC basis.

b. Operating Limit SACs may be developed to control an activity where a parameter needs to remain within prescribed bounds, such as a MAR limit. The Operating Limit statement describes the operating conditions under which the operating limit is required to be met. The basis statement in the associated TSR should identify the reason for the selection of this limit and what the limit is designed to protect. Review mechanisms may be appropriate, such as using audits when the parameter is recorded, or using independent verification when the parameter is managed in real time. The review mechanisms and periodicity should be described in the SAC basis.

c. Process Control SACs may be developed when an analysis or activity such as sampling is required by the DSA to confirm compliance with the safety basis. Process Control SACs identify the analysis or activity required to demonstrate compliance with pre-established criteria and/or parameters and the conditions that require that analysis or activity. For example, a Process Control SAC might be used to control calculations prior to transferring liquid high-level radioactive waste from one tank to another. Such transfers could involve complex calculations and sampling based upon sending and receipt tank inventory constituent concentrations and volumes, waste temperatures, waste transfer volumes and receipt tank head space. These process variable inputs would be used to calculate resulting receipt tank hydrogen concentrations to ensure these concentrations are within allowable flammability levels prior to initiating a transfer. The exact manner in which the analysis or sampling has to be performed should be clearly described, or referenced, in a SAC implementing procedure.

Process Control SACs might also be used in these situations: (a) to prescribe the calculational models identified in (or referenced by) the DSA that are required for use in evaluating whether the results of these planned activities meet the allowable criteria identified in the DSA, and (b) to determine applicability of LCOs or Surveillance Requirements, when LCO applicability or frequency is determined by calculational models. In these two cases, the calculational process is expected to be an integral part of the SAC, that is, not performed outside the scope of the SAC. The results should be auditable and independently verified prior to performing the activity.

The specific quality control provisions for ensuring accurate data input, and calculational result verification should be included in the DSA, while the description of the calculational models and acceptance criteria should be provided in the SAC basis statement. Periodic review activities should rely on measurement of physical parameters (e.g., receipt tank head-space hydrogen concentration levels) subsequent to the activity.

Procedural statements written to implement Directive Action SAC statements should be formatted to aid the operator in identifying these important safety requirements, in a manner similar to that used for TSR-level controls for LCO SACs.

4.3 DEVELOPING A MATERIAL AT RISK (MAR) TSR CONTROL

In many nuclear facilities, the MAR is a major analytic assumption underlying the hazard and accident analyses. In such cases, a MAR inventory greater than assumed in the DSA would place facility in an unanalyzed condition. As such, MAR assumptions would need to be protected in a highly reliable and enforceable manner. However, it is not normally possible to control MAR with an active or passive SSC; hence, administrative controls are used. A Directive Action SAC, if necessary, is the preferred approach unless an LCO SAC can be

technically justified and defended.

An LCO SAC may be warranted if facility operations can be effectively conducted while limiting the actual MAR in the facility to a specified fraction (e.g., 90 percent) of the MAR value assumed in the safety basis. Controlling to a lower MAR limit in the LCO helps to protect the MAR value assumed in the safety basis, and provides operational attention and flexibility. However, in the event that the MAR is discovered to exceed the MAR value assumed in the safety basis, the use of an LCO format SAC would not exempt a facility from declaring a Potential Inadequacy of the Safety Analysis. In any event, facilities are expected to effectively manage MAR in a way that protects LCO SAC limits, rather than relying on unplanned LCO entry and Action Statement completion to manage MAR. Because the MAR is such an important analytical assumption, if it is credible that the MAR limit can still be exceeded, an additional TSR provision should be considered as part of the LCO SAC to protect the absolute MAR limit.

If an adequate basis showing that the DSA MAR limit can be preserved during normal operations, and suitable periodic review frequencies can be established, the use of a MAR-related LCO is acceptable. The basis for the decision to use a MAR-related LCO should be documented in the TSR basis statements. Where its use can be defended, a MAR-related LCO has the advantage of allowing the facility an action completion time, which, if met, could avert a TSR violation. However, there are feasibility limits associated with the LCO approach. For example, assume that a large facility needs to control MAR in many locations because the facility employs segmentation for hazard categorization or criticality purposes, then each location would need its own listing in the LCO. From human factors and reliability perspectives, this approach could be unduly complex and unwieldy.

In the more general case, when action times and periodic review frequencies cannot be technically supported to ensure observance of MAR limits, a Directive Action SAC may be used. Directive Action SACs do not typically support action times to allow the facility some time to correct the MAR-related exceedance. When this approach is taken, directive language should be used in the form of a “SHALL” statement to set the maximum MAR limit, as relied upon in the DSA. Relevant periodic review requirements, if any, (such as periodic audits of MAR inventory calculations and/or a NQA-1 qualified inventory control system) may be included in this type of SAC. The adequacy of selected methods and the frequency of these periodic reviews should be justified in the SAC’s basis statement.

4.4 TSR USE AND APPLICATION MODIFICATIONS FOR SACS

For both directive action SACs and LCO SACs, the “Use and Application” section of the TSR should define any relevant ground rules for treating SACs, such as when and how to report violations.

4.5 REVISING TSR DEFINITIONS TO REFLECT SACS

The “Definitions” Section of this Standard provides acceptable definitions for use in adding related terms to Section 1 of TSRs.

5 SAC VIOLATION REPORTING AND FAILURE ANALYSIS

5.1 REPORTING REQUIREMENTS FOR VIOLATIONS OF SACS

Violations of SACs covered in the TSRs are required to be reported to DOE in accordance with DOE O 232.2, Chg. 1, *Occurrence Reporting and Processing of Operations Information*.

5.2 INVESTIGATION AND REPORTING OF SAC VIOLATIONS

DOE-STD-1197-2011, *Occurrence Reporting Causal Analysis*, provides guidance on how to determine the apparent cause(s) of specific reportable occurrences, including TSR violations, and explains the structure and nodes of the Causal Analysis Tree for use in occurrence reporting and failure analysis.

Identifying the causes for SAC 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 investigators should be experts in both human performance and the process or facility involved.

TSR violations, including SAC violations, that may occur during operation of the facility, are required to be investigated to determine specific or generic causes, generic implications, and recommended corrective actions. TSR violations are reported to the DOE in accordance with 10 CFR Part 830.205 and DOE O 232.2.

6 EXAMPLES

EXAMPLE 1 – EXAMPLE LCO FORMAT FOR SACS

(TRU Waste Storage Facility)

3/4 OPERATING LIMITS AND SURVEILLANCE REQUIREMENTS

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

LCO 3.3.1: TRU waste shall be containerized and the total quantity shall be less than or equal to 1,800 Plutonium-239 Equivalent Curies (PEC).

AND

Each TRU waste 55-gallon drum shall be less than 150 PEC.

AND

Each TRU waste box shall be less than 300 PEC.

AND

Each TRU waste crate shall be less than 300 PEC.

MODE APPLICABILITY: OPERATION and WARM STANDBY

PROCESS AREA APPLICABILITY: TRU WASTE STORAGE FACILITY

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. TRU waste 55-gallon drum(s) is ≥ 150 PEC. **OR** TRU waste box(es) is ≥ 300 PEC. **OR** TRU waste crate(s) is ≥ 300 PEC.	A.1 Suspend TRU waste container movements within 10 feet of the non-compliant TRU waste container(s). **AND** A.2.1 Remove the non-compliant TRU waste container(s) from the TRU WASTE STORAGE FACILITY. **OR** A.2.2 Restore the non-compliant TRU waste container(s) to within the LCO MAR limits.	1 Hour 3 Weeks 3 Weeks
B. TRU WASTE STORAGE FACILITY MAR is not containerized or the total quantity is > 1,800 PEC.	B.1 Suspend TRU waste container receipts at the TRU WASTE STORAGE FACILITY. **AND** B.2 Restore the TRU WASTE STORAGE FACILITY to ≤ 1,800 PEC containerized waste.	1 Hour 3 Weeks

SURVEILLANCE REQUIREMENTS

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.3.1.1	Verify the MAR at the TRU WASTE STORAGE FACILITY is containerized and less than or equal to 1,800 PEC.	Monthly
SR 4.3.1.2	Verify the following MAR limits are met: • TRU waste 55-gallon drum is less than 150 PEC. • TRU waste box is less than 300 PEC. • TRU waste crate is less than 300 PEC.	Prior to receipt at the TRU WASTE STORAGE FACILITY

BASES

BACKGROUND SUMMARY	Inventory Control and Material Management provides control for the location, storage configuration, and handling of nuclear material within the TRU WASTE STORAGE FACILITY based on the quantity, type, and form. The inventory controls in this LCO, protect 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	The LCO protects the initial MAR for accident scenarios that involve the entire TRU 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 TRU 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. Accidents resulting from a breach of TRU waste containers (i.e., 55-gallon drums, boxes, and crates) can result in significant consequences to the workers and public. Specific controls and restrictions are placed on radiological material inventory (i.e., containerized waste and the TRU WASTE STORAGE FACILITY) to prevent the introduction of radioactive materials into the TRU WASTE STORAGE FACILITY that would invalidate the safety basis. [Include the basis for the decision to use a MAR-related LCO instead of a Directive Action SAC. This discussion can be included here.]
LCO 3.3.1	The total quantity of containerized TRU waste that can be in the TRU WASTE STORAGE FACILITY shall be less than or equal to 1,800 Plutonium-239 Equivalent Curies (PEC). Each TRU waste 55-gallon drum shall be less than 150 PEC and each TRU waste box and TRU waste crate shall be less than 300 PEC. The Surveillance Requirements (SRs) demonstrate compliance with the LCO Statement and this is accomplished by verifying the quantity of nuclear material within individual TRU waste containers (i.e., 55-gallon drums, boxes, and crates) complies with the limits stated above as well as the total quantity limit within the TRU WASTE STORAGE FACILITY. In the accident analysis, the DSA assumes the full facility MAR is 2,000 PEC as a very conservative value. In order to protect this assumption, the LCO for MAR is set at 90% of that value. [Include the basis showing that this LCO and its surveillance requirements would be effective in preserving the MAR below what is assumed in the safety basis.] The MAR loadings for the highest estimated single TRU containers were used in the safety analysis and 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. An increase in a specific TRU waste container MAR does not impact contiguous waste containers, other than for criticality considerations. Therefore high MAR TRU waste containers do not require segmentation except for criticality accident considerations. The Criticality Safety Program is credited for addressing criticality issues related to high MAR containers and their movement.
MODE APPLICABILITY		This LCO applies in the OPERATION and WARM STANDBY MODES because MAR may be present in the TRU WASTE STORAGE FACILITY in these MODES. Since radioactive material may be present in the TRU WASTE STORAGE FACILITY while in all MODES except DEINVENTORIED, this LCO is applicable in OPERATION and WARM STANDBY.
PROCESS AREA APPLICABILITY		TRU waste storage is only allowed in the TRU WASTE STORAGE FACILITY. Therefore, this LCO is applicable to the TRU WASTE STORAGE FACILITY.
ACTION STATEMENTS	A.1	If it is determined that; (1) TRU waste in a 55-gallon drum(s) is greater than or equal to 150 PEC, or (2) TRU waste in a box(es) is greater than or equal to 300 PEC, or (3) TRU waste in a crate(s) is greater than or equal to 300 PEC or any combination exists than action shall be taken within 1 Hour to suspend TRU waste container movements within 10 feet of the non-compliant TRU waste container(s). Suspending TRU waste container movements within 10 feet of the non-compliant container(s) minimizes TRU waste container interactions that can result in a potential radiological release. Based upon the simplicity of the container movement activities, the Completion Time of 1 Hour is considered adequate to notify workers in the vicinity to suspend TRU waste container movements and to safely secure the handling equipment and TRU waste containers involved.
	A.2.1	If it is determined that; (1) TRU waste in a 55-gallon drum(s) is greater than or equal to 150 PEC, or (2) TRU waste in a box(es) is greater than or equal to 300 PEC, or (3) TRU waste in a crate(s) is greater than or equal to 300 PEC or any combination exists than either Required Action A.2.1 or A.2.2 shall be performed but both are not required to be performed. Within 3 Weeks, the non-compliant TRU waste container shall be removed from the TRU WASTE STORAGE FACILITY. The Completion Time of 3 Weeks is considered adequate time for Facility Management to identify, communicate with, and coordinate a transfer from the TRU WASTE STORAGE FACILITY.[2]
	A.2.2	If Required Action A.2.1 is not performed than Required Action A.2.2 shall be completed within 3 Weeks. The non-compliant container(s) shall be restored to within LCO MAR limits. Compliance may be established by re-assay to obtain a more accurate count or expert review of an existing assay. The Completion Time of 3 Weeks is considered adequate time for Facility Management to re-establish container compliance.[2]

	B.1	If TRU WASTE STORAGE FACILITY MAR is not containerized or the total quantity is greater than 1,800 PEC than action shall be taken within 1 Hour to suspend TRU waste container receipts at the TRU WASTE STORAGE FACILITY. Suspending TRU waste container receipts at the TRU WASTE STORAGE FACILITY prevents increasing the MAR that may be involved in a potential hazard or accident. The Completion Time of 1 Hour is considered adequate to notify personnel to suspend TRU waste container receipts at the TRU WASTE STORAGE FACILITY and secure any receipt activities.
ACTION STATEMENTS (continued)	B.2	If TRU WASTE STORAGE FACILITY MAR is not containerized or the total quantity is greater than 1,800 PEC than action shall be taken within 3 Weeks to restore the TRU WASTE STORAGE FACILITY to less than 1,800 PEC of containerized waste. This action may involve removal of TRU waste or repackaging to be containerized. Compliance may also be established by re-assay to obtain a more accurate count or expert review of an existing assay. The Completion Time of 3 Weeks is considered adequate time for Facility Management to re-establish container compliance.[3]
SURVEILLANCE REQUIREMENTS	SR 4.3.1.1 SR 4.3.1.1 verifies that MAR at the TRU WASTE STORAGE FACILITY is containerized and is less than or equal to 1,800 PEC. Performance on a Monthly frequency provides assurance that the TRU WASTE STORAGE FACILITY complies with the MAR limits. It is not anticipated that the TRU WASTE STORAGE FACILITY MAR limit would be exceeded since TRU waste container limits are verified prior to receipt at the TRU WASTE STORAGE FACILITY. A WESE query may be used to perform SR 4.3.1.1. The Surveillance Frequency of Monthly was selected as a reasonable interval to provide alternate verification of MAR limit compliance. If SR 4.3.1.1 was not met than Condition B would be entered. SR 4.3.1.2 SR 4.3.1.2 verifies the following MAR container limits are met; (1) TRU waste in a 55-gallon drum(s) is less than 150 PEC, and (2) TRU waste in a box(es) is less than 300 PEC, and (3) TRU waste in a crate(s) is less than 300 PEC. Performance “Prior to receipt at the TRU WASTE STORAGE FACILITY” provides assurance that the TRU WASTE STORAGE FACILITY is operated within the bounds of the safety analysis. “Prior to receipt” may be accomplished by verification of shipping information “before shipment” or “at receipt” before entry into the TRU WASTE STORAGE FACILITY MAR inventory tracking. A WESE query may be used to perform SR 4.3.1.2. If SR 4.3.1.2 was not met than Condition A would be entered.	

EXAMPLE 2 – EXAMPLE DIRECTIVE ACTION FORMAT FOR SACS

5.7.3.1 Material-at-Risk Limit (Operating Limit SAC)

SAC

The facility tritium limit SHALL be < 50 grams.

BASES

Safety Function

The material-at-risk (MAR) limit is the initial assumption for bounding dose and consequences for the accident analysis performed in Chapter 3 of the DSA. The SAC for the tritium MAR limit protects this assumption and ensures that the consequences determined in the accident analysis remain valid. Exceeding this MAR limit can result in placing the facility in an unanalyzed condition. This control is designated as a SAC because it provides a safety function that cannot be performed by an engineered safety system.

Application to Safety Analysis

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. The maximum off-site mitigated dose estimate to the public is 15 rem. This estimate assumes 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. The MAR limit of 50 grams of tritium is approximately six weeks of facility throughput in fiscal year 2014 and represents approximately 10% of the maximum amount of tritium that has been historically processed in the facility.

SAC Description

This SAC is implemented by use of inventory control procedures and inventory control logs. Provisions within the associated procedures address tracking of transfers into, transfers out of, losses from, and the results of a physical inventory, which accounts for the effect of tritium decay and approved discards (e.g., waste disposal and atmospheric losses) on the calculated inventory. Accounting for inflow and outflow ensures that the facility is operating within its assumed MAR values used in analyses. The facility MAR is controlled by an NQA-1 qualified inventory control system.

The MAR limit includes tritium-containing materials being moved (e.g., in-transit) between process buildings as well as located (e.g., staged, stored) in process building within the facility. The MAR limit does not include tritium-containing material shipments/receipts staged in the Tritium Yard that have not been received and added to the facility MAR limit.

The accuracy of the inventory control procedures is ensured through the performance of periodic and conditional surveillances of inventories that include peer and independent verifications and independent reconciliation of the physical inventory. The routine updates of the inventory control procedures with the material transfer data and the physical inventory reconciliation results are adequate to provide initial and continued assurance that the safety function of this SAC is maintained.

7 REFERENCES

(1) 10 CFR Part 830, Nuclear Safety Management.

(2) DOE O 232.2, Chg. 1, *Occurrence Reporting and Processing of Operations Information*, March 2014.

(3) DOE O 420.1C, Chg. 1, *Facility Safety*, February 2015.

(4) DOE O 422.1, Chg. 2, *Conduct of Operations*, December 2014.

(5) DOE O 426.2, Chg. 1, *Personnel Selection, Training, Qualification, and Certification Requirements for DOE Nuclear Facilities*, July 2013.

(6) DOE G 423.1-1B, *Implementation Guide for Use in Developing Technical Safety Requirements*, March 2015.

(7) DOE-STD-1189-2008, *Integration of Safety into the Design Process*, March 2008.

(8) DOE-STD-1189-2016, *Integration of Safety into the Design Process*, December 2016.

(9) DOE-STD-1197-2011, *Occurrence Reporting Causal Analysis*, September 2011.

(10) DOE-STD-3009-94, CN3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, March 2006.

(11) DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analyses*, November 2014.

(12) ANSI/ANS-58.8-1994, (R2001; R2008), *Time Response Design Criteria for Safety-Related Operator Actions*