Allen, Pam, NMENV

From: Maestas, Ricardo, NMENV
Sent: Wednesday, June 25, 2014 3:52 PM
To: Allen, Pam, NMENV
Subject: FW: WIPP Information - for call today
Attachments: Nonreactor Nuke Safety Desgin Criteria g4201-1.pdf; Nonreactor Nuke Safety Desgin Criteria g4201C 20121204.pdf

Email and att. for March

From: Skibitski, Thomas, NMENV
Sent: Thursday, March 13, 2014 2:07 PM
To: Kliphuis, Trais, NMENV; Flynn, Ryan, NMENV; Kendall, Jeff, NMENV
Cc: Winchester, Jim, NMENV; Tongate, Butch, NMENV; Blaine, Tom, NMENV; Schwender, Erika, NMENV; Kieling, John, NMENV; LucasKamat, Susan, NMENV; Nelson, Morgan, NMENV; Maestas, Ricardo, NMENV; Holmes, Steve, NMENV; Ines Triay (triayin@fiu.edu)
Subject: RE: WIPP Information - for call today

Pasted below are two references from the attached documents. The question, albeit after the fact, is "Why wasn't the exhaust system designed as a safety-significant or safety-class ventilation system?" The first sentence of the last paragraph suggests it might/should have been. Please note that the above was replaced with document 4201-1C which speaks to defense in depth in the second section shown.

This may not be helpful, but it helps define the concepts.
TS

Thomas Skibitski
Chief, DOE Oversight Bureau
Office (505) 845-5932
Cell (505) 377-8135

5.2.2.1 Ventilation

In general, the safety function of ventilation and offgas systems is to provide confinement integrity and to filter exhaust, thereby preventing or mitigating uncontrolled releases of radioactive and/or hazardous materials to the environment. Ventilation and offgas systems are included as a vital part of the primary and secondary confinement design. The need for redundancy and the degree of redundancy in these systems must be determined by the safety analysis process and maintenance concerns for both active and passive components. Designs must provide for periodic maintenance, inspection, and testing of components. Adequate shielding must be included in the design of filters, absorbers, scrubbers, and other air treatment components to ensure that occupational exposure limits are not exceeded during maintenance and inspection activities.

Safety-significant and safety-class ventilation system designs must include adequate instrumentation to monitor and assess performance with necessary alarms for annunciation of abnormal or unacceptable operation. Manual or automatic protective control features must be provided to prevent or mitigate an uncontrolled release of radioactive and/or hazardous material to the environment and to minimize the spread of contamination within the facility.

Vent streams potentially containing significant concentrations of radioactive and/or hazardous materials must be processed through an offgas cleanup system before being exhausted to the environment. Cleanup systems are to remove particulates and noxious chemicals and control the release of gaseous radionuclides. The design of safety-significant and safety-class offgas systems must be commensurate with the sources and characteristics of the radioactive and chemical components of the offgas air stream to prevent or mitigate the uncontrolled releases of radioactive and/or hazardous materials to the environment.

(From g 4201C 20121204)

5.1.1 General Discussion

Defense-in-depth is a fundamental strategy for nuclear facility safety. Defense-in-depth provides layers of defense against the release of hazardous materials so that no one layer by itself is completely relied upon. All safety activities, whether organizational, behavioral or equipment-related, are subject to layers of overlapping provisions, so that if a failure should
occur it would be compensated for or corrected without causing harm to individuals or the public at large. When properly applied, the defense-in-depth strategy ensures that no single human or mechanical failure would lead to injury to individuals or to the public, or even combinations of failures that are only remotely possible would lead to little or no injury.

The strategy for defense-in-depth is twofold: first, to prevent accidents, and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions. Defense-in-depth is generally structured in five levels, as discussed below. Should one level fail, the next one comes into play.

Level 1 – Prevention of abnormal operation and failures. Accident prevention is the first priority. This is accomplished by conservative design and high quality in construction and operations and maintenance, including conservative site selection. This also includes design to minimize and control inventories of radioactive materials-at-risk. Provisions to prevent deviations of facility state from well-known operating conditions are generally more effective and more predictable than measures aimed at mitigation of such a departure.

Level 2 – Control of abnormal operation and detection of failures. This is accomplished by control, limiting and protection systems, as well as other surveillance features. Both safety systems and administrative controls are used. Multiple, diverse and independent means are provided to control and monitor facility processes.

Level 3 – Control of accidents within the design basis. This is accomplished by engineered safety features that are capable of leading the facility to a safe controlled state. A central component of defense-in-depth is the use of successive, multiple physical barriers for protection against release of radioactivity and hazardous materials. Multiple, diverse and independent means are provided
to accomplish safety functions.

Level 4 – Control of severe facility conditions. This includes prevention of accident progression and mitigation of consequences of accidents.

Level 5 – Mitigation of radiological consequences. Significant adverse consequences from significant releases of radioactive materials are mitigated by emergency procedures and emergency response. As required for emergency response, means are provided to monitor accident releases.

At each level, a combination of design features and human aspects is evident. Human aspects of defense-in-depth are brought into play to protect the integrity of the barriers. These include quality assurance (QA),

procedures, administrative controls, operating limits, safety reviews, personnel qualification and training, independent oversight, and safety culture. Design provisions (including both those for normal facility systems and those for engineered safety features) help to prevent: undue challenges to the integrity of physical barriers; failure of a barrier if it is jeopardized; and, consequential damage to multiple barriers in series.

The general objective of defense-in-depth is to ensure that a single failure (whether equipment failure or human failure) at one level of defense, or even combinations of failures at more than one level of defense, would not propagate to jeopardize defense-in-depth at subsequent levels. The independence of different levels of defense is a key element in meeting this objective. Special attention should be paid to hazards that could potentially impair several levels of defense, such as fire, earthquakes, and flooding.

DOE G 420.1-1

Approved: 3-28-00

NONREACTOR NUCLEAR SAFETY DESIGN CRITERIA AND EXPLOSIVES SAFETY CRITERIA GUIDE

for use with

DOE O 420.1, FACILITY SAFETY

U.S. DEPARTMENT OF ENERGY

Office of Environment, Safety and Health

Distribution:
All Departmental Elements

Initiated By:
Office of Environment, Safety and Health

FOREWORD

This Guide provides guidance on the application of requirements for nonreactor nuclear facilities and explosives facilities of Department of Energy (DOE) O 420.1, FACILITY SAFETY, Section 4.1, Nuclear and Explosives Safety Design Criteria. The following guidelines were established for the development of this Guide.

- This Guide provides guidance on implementing the requirements stated in DOE O 420.1, Section 4.1, as they apply to the design aspects for nuclear safety of nonreactor nuclear facilities and safety requirements for explosives facilities. The guidance provided in this Guide is restricted to the requirements identified in DOE O 420.1, Section 4.1. This Guide does *not* establish requirements.

- Safety analyses performed in accordance with DOE-STD-3009-94 establish the identification, function, and performance of safety structures, systems, and components (SSCs) and must be conducted early in the design process.

- Applicable current Rules, Standards, and Orders will be referenced herein and text and requirements from these documents will not be repeated.

- Same-subject information will be grouped in a single section and cross referenced elsewhere as required.

- Management and policy requirements will *not* be included in this document.

Throughout this Guide, the words “must” and “should” are used to identify actions that need to be accomplished to meet this guidance. The word “must” denotes actions that are required to comply with this Guide. The word “should” is used to indicate recommended practice (DOE-STD-1075-94).

Users are encouraged to submit suggestions for improving this Guide to the office of Nuclear Safety Policy and Standards.

CONTENTS

CONTENTS (continued)

TABLES

GLOSSARY

NOTE: Origins of the definitions are indicated by references shown in brackets, [ ], although in some cases the referenced Orders are being replaced. If no reference is listed, the definition originates in this Guide and is unique to its application. Terms used within this Guide that are not defined in the Glossary carry their definition from the referenced documents.

Accident. An unplanned sequence of events that results in undesirable consequences. [DOE-STD-3009-94]

Accident analysis. For the purposes of properly implementing the Unreviewed Safety Question Order, the term "accident analysis" refers to those bounding analyses selected for inclusion in the Safety Analysis Report. These analyses refer to design basis accidents (DBAs) only. [DOE 5480.21]

Accident analysis has historically consisted of the formal development of numerical estimates of the expected consequence and probability of potential accidents associated with a facility. For the purposes of this Guide, accident analysis is a follow-on effort to the hazard analysis, not a fundamentally new examination requiring extensive original work. As such, it requires documentation of the basis for assignment to a given likelihood of occurrence range (e.g., 1/y to 10^{-2}/y, 10^{-2}/y to 10^{-4}/y, 10^{-4}/y to 10^{-6}/y) in hazard analysis and performance of a formally documented consequence analysis. Consequences are compared with offsite evaluation guidelines to identify safety-class structures, systems, and components. [DOE-STD-3009-94]

ALARA. As low as reasonably achievable.

Confinement barriers.

- **Primary confinement.** Provides confinement of hazardous material to the vicinity of its processing. This confinement is typically provided by piping, tanks, gloveboxes, encapsulating material, and the like, along with any offgas systems that control effluent from within the primary confinement.

- **Secondary confinement.** Consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area. Except in the case of areas housing glovebox operations, the area inside this barrier is usually unoccupied (e.g., canyons, hot cells); it provides protection for operating personnel.

- **Tertiary confinement.** Typically provided by walls, floor, roof, and associated ventilation exhaust systems of the facility. It provides a final barrier against the release of hazardous material to the environment.

Construction. Any combination of engineering, procurement, erection, installation, assembly, or fabrication activities involved in creating a new facility or altering, adding to, or rehabilitating an existing facility. It also includes the alteration and repair (including dredging, excavating, and painting) of buildings, structures, or other real property.

Decommissioning. The process of closing and securing a nuclear facility or nuclear materials storage facility to provide adequate protection from radiation exposure and to isolate radioactive contamination from the human environment. [DOE 5480.30]

Decontamination. The act of removing a chemical, biological, or radiological contaminant from or neutralizing its potential effect on a person, object, or environment by washing, chemical action, mechanical cleaning, or other techniques. [DOE 5480.30]

Design basis. Information that identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or range of values chosen for controlling parameters as reference bounds of design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analyses (based on calculations and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals. [10 CFR 50.2]

Design basis accident. An accident postulated for the purpose of establishing functional and performance requirements for safety structures, systems, and components. [DOE-STD-3009-94]

Effluent monitoring. The collection and analysis of samples or measurements of liquid and gaseous effluents for the purpose of characterizing and quantifying contaminants, assessing radiation exposures of members of the public, providing a means to control effluents at or near the point of discharge, and demonstrating compliance with applicable standards and permit requirements. [DOE 5400.1]

Evaluation guideline. Radiation dose value against which the safety analysis evaluates. Offsite evaluation guidelines are established for the purpose of identifying and evaluating safety-class structures, systems, and components.

Explosives facility. Any facility or location used for storage or operation with explosives or ammunition.

Facility. For the purpose of this Guide, the definition most often refers to buildings and other structures, their functional systems and equipment, and other fixed systems and equipment installed therein to delineate a facility. However, specific operations and processes independent of buildings or other structures (e.g., waste retrieval and processing, waste burial, remediation, groundwater or soil decontamination, decommissioning) are also encompassed by this definition. The flexibility in the definition does not extend to subdivision of physically concurrent operations having potential energy sources that can seriously affect one another or which use

common systems fundamental to the operation (e.g., a common glovebox ventilation exhaust header). [DOE-STD-3009-94]

Fail safe. A design characteristic by which a unit or system will become safe and remain safe if a system or component fails or loses its activation energy.

Hazard. A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to an operation or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation). [DOE 5480.23]

Hazard analysis. The determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by the assessment of hazardous situations associated with a process or activity. Largely qualitative techniques are used to pinpoint weaknesses in design or operation of the facility that could lead to accidents. The Safety Analysis Report hazard analysis examines the complete spectrum of potential accidents that could expose members of the public, onsite workers, facility workers, and the environment to hazardous materials. [DOE-STD-3009-94]

Hazard classification. Evaluation of the consequences of unmitigated releases to classify facilities or operations into the following hazard categories. [DOE 5480.23]

- **Hazard Category 1:** Shows the potential for significant offsite consequences.
- **Hazard Category 2:** Shows the potential for significant onsite consequences.
- **Hazard Category 3:** Shows the potential for only significant localized consequences.

DOE-STD-1027-92 provides guidance and radiological threshold values for determining the hazard category of a facility. DOE-STD-1027-92 interprets Hazard Category 1 facilities as Category A reactors and other facilities designated as such by the Program Secretarial Officer. [DOE-STD-3009-94]

Hazardous material. For the purpose of this Guide, any solid, liquid, or gaseous material that is not radioactive but is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health.

Nonreactor nuclear facility. Those activities or operations that involve radioactive and/or fissionable materials in such form and quantity that a nuclear hazard potentially exists to the employees or the general public. Included are activities or operations that—

- produce, process, or store radioactive liquid or solid waste, fissionable materials, or tritium;
- conduct separations operations;

- conduct irradiated materials inspection, fuel fabrication, decontamination, or recovery operations;
- conduct fuel enrichment operations; and
- perform environmental remediation or waste management activities involving radioactive materials.

Incidental use and generating of radioactive materials in a facility operation (e.g., check and calibration sources, use of radioactive sources in research and experimental and analytical laboratory activities, electron microscopes, and x-ray machines) would not ordinarily require the facility to be included in this definition. [DOE 5480.23]

Public. All individuals outside the DOE site boundary. [DOE-STD-3009-94]

Risk. The quantitative or qualitative expression of possible loss that considers both the probability that an event will occur and the consequence of that event. [DOE 5480.23]

Safety analysis. A documented process: (1) to provide systematic identification of hazards within a given DOE operation; (2) to describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and (3) to analyze and evaluate potential accidents and their associated risks. [DOE 5480.23]

Safety Analysis Report. A report that documents the adequacy of safety analysis to ensure that a facility can be constructed, operated, maintained, shut down, and decommissioned safely and in compliance with applicable laws and regulations. [DOE 5480.23]

Safety basis. The combination of information relating to the control of hazards at a facility (including design, engineering analyses, and Administrative Controls) upon which DOE depends for its conclusion that activities at the facility can be conducted safely. [DOE 5480.23]

Single-failure criterion. Safety systems must perform all required safety functions for a DBA in the presence of the following.

- Any single detectable failure within the safety systems concurrent with all identifiable but undetectable failures.
- All failures caused by the single failure.
- All failures and spurious system actions that cause, or are caused by, the DBA requiring the safety function.

The single failure could occur prior to, or at any time during, the DBA for which the safety system is required to function. [ANSI/IEEE Standard 379-1994, Chapter 4]

Site boundary. A well-marked boundary of the property over which the owner or operator can exercise strict control.

ABBREVIATIONS AND ACRONYMS

AC/DC	alternating current/direct current
ACGIH	American Conference of Governmental Industrial Hygienists
ACI	American Concrete Institute
AISC	American Institute of Steel Construction
ALARA	as low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
API	American Petroleum Institute
ASHRAE	American Society of Heating, Refrigeration, and Air-Conditioning
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
AWWA	American Water Works Association
CFR	Code of Federal Regulations
DBA	design basis accident
DoD	Department of Defense
DoDESB	Department of Defense Explosives Safety Board
DOE	Department of Energy
DOE O	Department of Energy Order
DOE G	Department of Energy Guide
DOE-STD	DOE Standard
EIA	Electronic Industries Association
ERDA	Energy Research and Development Administration (predecessor to DOE)
HEPA	high-efficiency particulate air (filter)
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronic Engineers
IES	Illumination Engineering Society
ISA	Instrumentation Society of America
MOI	maximally exposed offsite individual
NCRP	National Council on Radiation Protection
NEPA	National Environmental Policy Act
NFPA	National Fire Protection Association
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulatory Guide
OSHA	Occupational Safety and Health Administration
QA	quality assurance
RAM	reliability, availability, and maintainability
RCRA	Resource Conservation and Recovery Act
SMACNA	Sheet Metal and Air Conditioning Contractors National Association
SSC	structures, systems, and components

1. INTRODUCTION

1.1 General

This Implementation Guide provides an acceptable approach for satisfying the requirements of Department of Energy (DOE) Order (O) 420.1, Facility Safety, Section 4.1, Nuclear and Explosives Safety Design Criteria. The objective of the Guide is to provide a methodology for selecting industry codes and standards for nuclear safety aspects of nonreactor nuclear facility design. The Guide stresses that safety design should be driven by safety analysis and provides interpretive guidance on the performance-level requirements of the Order. A successful safety design depends on the quality of the safety analysis and on engineering judgment in the transformation of this guidance to the final design.

This Guide is not intended to be all inclusive with respect to the nuclear/radiological safety requirements and guidance for designing a DOE nonreactor nuclear facility. Where other DOE Orders, Rules, and national and industry codes and standards contain requirements and supporting guidance pertaining to safety of nuclear facilities, such guidance will not be repeated in this document. Instead, a short discussion will point to the relevant document. Examples are found in the areas of natural phenomena hazards mitigation, fire protection, criticality safety, and explosives safety.

1.2 Applicability

The requirements of DOE O 420.1, Section 4.1, are applicable to the design and construction of new nonreactor nuclear facilities and for modifications to existing nonreactor nuclear facilities when the modifications significantly increase the probability or consequence of a nuclear accident or require a change in the Technical Safety Requirements of a facility. It is intentionally left to the judgment of the proposing contractor and the approving DOE authority to define "significant." In part, this is intended to allow upgrading of existing safety equipment or installation of minor new improvements without subjecting the process to onerous procedural requirements and thus discouraging improvements.

Modifications to facility design and construction during the design and construction phase must conform to the design requirements for new facilities.

All new construction must, as a minimum, conform to the model building codes applicable for the state or region, supplemented with additional safety requirements associated with the hazards in a facility in a graded manner.

1.3 Content

This Guide is structured to represent the progressive logic of design. Section 1, Introduction, provides a general statement regarding the intent and applicability of the Guide. The following sections provide guidance for nuclear safety design concepts or assurances, elements of design

for nuclear safety, functional design criteria, and criteria for safety structures, systems, and components (SSCs).

Contained within Section 2, Safety Analysis and Design Process, are nuclear safety design concepts that when implemented along with specific criteria should ensure a safe facility design. This section addresses the importance of starting the safety analysis as early as possible in the design and maintaining an interrelationship between the design process and the safety analysis, as they both evolve. The section provides explicit guidance for the application of the offsite evaluation guideline for the proper classification of safety class SSCs. Other concepts addressed under this section are defense in depth, system engineering, and quality assurance (QA). These are nuclear safety design concepts and strategies to be applied at the beginning and throughout the design process to ensure safety concerns are addressed and incorporated into the design as necessary.

Section 3, Elements of Design for Nuclear Safety; Section 4, Functional Design Criteria; and Section 5, Supplementary Design Criteria for Safety Structures, Systems, and Components, describe specific criteria that are to be applied, as applicable, to the facility under design. The guidance within these sections relates to safety as it applies to the overall facility and its impact on facility design.

Section 3 addresses nuclear safety criteria that should be considered during the design process such as siting, natural phenomena, architecture, accessibility and maintainability, human factors, and decontamination and decommissioning.

Section 4 is more specific to the safety function(s) that are to be performed within or by the facility under design. These nuclear safety criteria include nuclear criticality, radiation protection, hazardous material protection, effluent monitoring and control, waste management, fire protection, emergency preparedness and emergency communications, and explosives criteria and their applicability to the safety of the facility, depending on the function or mission of the facility.

Section 5 provides guidance for specific criteria requirements for the SSCs that are identified, via the safety analysis, to function as safety-class or safety-significant SSCs. These criteria are applied to those specific elements within the facility.

1.4 Compliance with DOE O 420.1 Requirements

This section provides a correlation of the requirements contained in DOE O 420.1, Section 4.1, to this Guide. The objectives of DOE O 420.1, Section 4.1, Nuclear Safety, are covered in the Introduction section defining the intent and applicability to DOE design activities.

The requirements for the development process of the safety analysis are set forth in DOE O 420.1, Section 4.1.1.1, General Requirements. Also contained in DOE O 420.1, Section 4.1.1.1, and DOE O 420.1, Section 4.1.1.2, Design Requirements, are the requirements pertaining to the implementation of defense in depth and the quality level requirements for facility design and

construction. Section 2, Safety Analysis and Design Process, of this Guide provides guidance for performing the safety analysis and maintaining an interrelationship with the design process. This Guide section also contains guidance for nuclear safety design concepts such as defense in depth, system engineering, and QA to meet the requirements set forth in DOE O 420.1, Section 4.1.

Guidance for the additional nuclear safety design requirements set forth in Section 4.1.1.2 of DOE 420.1 are addressed in detail in Section 3, Elements of Design for Nuclear Safety, Section 4, Functional Design Criteria, and Section 5, Supplementary Design Criteria for Safety Structures, Systems, and Components, of this Guide. Requirements related to the overall facility design (e.g., siting; natural phenomena; architecture; reliability, accessibility, and maintainability; and decontamination and decommissioning) are provided in Section 3 of this Guide. Section 4of this Guide provides guidance to meet the nuclear safety functional requirements of DOE O 420.1, Section 4.1.1.2, as they pertain to as low as reasonably achievable (ALARA), waste management, and other functional operations. The guidance to meet the requirements for safety SSCs to be designed so they can perform their safety functions when called upon to operate and to be designed and fabricated under a QA program as defined in Section 4.1.1.2 of DOE O 420.1 are addressed in Section 5 of this Guide.

Guidance to comply with the requirements contained in Section 4.1.2, Explosives Safety, of DOE O 420.1, Section 4.1, are provided in Section 4.8, Explosives Criteria, of this Guide.

2. SAFETY ANALYSIS AND DESIGN PROCESS

2.1 Design Process and Safety Analysis Relationship

In this section, the relationship between the facility design process and the parallel development of the facility safety analysis is discussed. Continuous coordination is necessary between these two activities throughout the project to ensure that the final design meets the mission requirements and includes the required safety features and to ensure that the principles of integrated safety management systems as described in DOE P 450.4 and DOE G 450.4-1A are implemented. The safety analysis must be performed in accordance with the guidance in DOE-STD-3009-94 and the requirements of DOE 5480.23 to develop and validate the functional and performance requirements for the safety SSCs. One of the objectives of the hazard and accident analyses is to identify the complete suite of safety SSCs for a facility and to designate them as safety class or safety significant, as appropriate to their importance and role. From the Introduction to DOE-STD-3009-94, the techniques for hazard analysis provide methodologies for comprehensive definition of the accident spectrum for workers and the public. Throughout the evaluation process, preventive and mitigative SSCs and pertinent elements of programmatic controls are identified. This identification also establishes functional requirements for SSCs, which will subsequently delineate the technical information needed to establish performance criteria. The most significant aspects of defense in depth and worker safety are subject to definition as safety-significant SSCs and coverage by Technical Safety Requirements. Safety-class designation is reserved for SSCs needed for public protection and carries with it the most stringent requirements. Demonstration of compliance with the nuclear facility design requirements of DOE O 420.1 in accordance with the guidance for performing safety analyses DOE-STD-3009-94 (Chapters 3 and 4 of the Standard) and this Implementation Guide must be shown in the Preliminary Safety Analysis Report (or a Safety Analysis Report for significant modifications to existing facilities), DOE approval of which must be received before construction can begin.

Selection and design of safety SSCs is an important part of the overall facility design process. As the facility design progresses from conceptual design through the finalization of design, designers and safety analysts must exchange information in an iterative process. Early in the conceptual design, a hazard analysis must be conducted based on the anticipated physical and chemical processes to be used in support of the overall facility mission, external human-induced hazards, and natural phenomena hazards. The hazards associated with processes may influence the design (e.g., alternative physical layouts, segmentation of facilities to isolate particularly hazardous processes, or the use of multistage or parallel processes to reduce the hazardous material in any particular process step). Natural phenomena hazards must be considered in accordance with DOE O 420.1, Section 4.4, Natural Phenomena Hazards Mitigation, and the associated Guide. External human-induced hazards peculiar to the site (such as pipelines and hazardous materials storage) must be considered.

The results of the hazard analysis must be used to identify the design basis accidents (DBAs) that in turn must be used to define the functional and performance requirements of the facility safety

SSCs. Safety SSCs required to prevent or mitigate accidents whose consequences approach or exceed offsite evaluation guidelines must be defined as safety-class SSCs. Safety-significant SSCs must be selected for worker protection and to provide defense in depth.

The defense-in-depth concept, described in Section 2.3 of this Guide, must be integrated into the facility design process. The application of the defense-in-depth concept to the facility design will help identify potential safety features to be included in the facility design. Consideration should be given to prevent or mitigate accident consequences from contaminating the environment, even when direct public or worker safety is not an issue.

Sufficient hazard and accident analyses must be completed during the preliminary design to verify and finalize the selection of safety SSCs. These hazard and accident analyses must be sufficiently complete to determine the design environmental and load conditions for safety SSCs. Accident analysis examines a limited subset of accidents (DBAs) derived from the hazard analysis. The accident analysis forms the basis for evaluating the ability of the safety SSCs to perform their safety functions. The identification of DBAs is therefore based on the hazard analysis to ensure that a reasonable spectrum of potential accidents are considered for the design. DBAs should be analyzed conservatively using the applicable deterministic phenomonological methods. During the design process, the accident analysis should also be used to establish design requirements that minimize or eliminate potential hazards. Therefore, prevention and control of potential hazards through early and iterative interaction with the design process should be a primary objective of the hazard and accident analyses.

2.1.1 Functional Classification of Safety SSCs

In Sections 2.1.2 and 2.1.3 the classification of safety SSCs as safety class or safety significant is discussed. The concept of using an evaluation guideline for identifying safety class SSCs is introduced. The use of the evaluation guideline is only one element in a larger safety SSC functional classification process that is intended to contribute to “adequate safety.” Other operational contributors are disciplined conduct of operations, training, and safety management programs such as a radiation protection program, emergency response program, etc. Some principles that should be incorporated in a functional classification process are:

- Protection of the public is contributed to by all facets of safety in design, including safety class SSCs as well as safety significant SSCs, and, in many DOE cases, by remote siting. The expectation is that public design basis accident dose consequences (considering the protection provided by safety systems) would generally be a small fraction of the evaluation guideline.

- Protection of the public is predominant in safety design; protection of workers is no less important. However, the degree of protection for facility workers achievable by SSCs is limited. Other factors such as disciplined conduct of operations, training, and safety management programs are no less important in assuring worker safety.

- In prioritization of items for a facility safety strategy:

  - Minimization of hazardous materials (material at risk) is the first priority.
  - Safety SSCs are preferred over Administrative Controls.
  - Passive SSCs are preferred over active SSCs.
  - Preventative controls are preferred over mitigative controls.
  - Facility safety SSCs are preferred over personal protective equipment.
  - Controls closest to the hazard may provide protection to both workers and the public.
  - Controls that are effective for multiple hazards can be resource effective.

2.1.2 Application of Offsite Evaluation Guidelines for Safety-Class SSCs

A computational construct using the concepts of an unmitigated accident release and an evaluation guideline has been developed to aid in the designation of safety class SSCs. The process uses the same initiating events as identified in the hazard and accident analyses discussed in Section 2.1, but for the purposes of showing which SSCs are sufficiently important to classify as safety class, it presumes that the candidate safety systems are not functional (unmitigated release). Other parameters of the analyses should conservatively reflect physical realities; e.g., energies driving the release, release fractions, etc. If the resulting site boundary dose approaches the evaluation guideline, then the candidate SSCs need to be evaluated to see if their effectiveness in preventing or mitigating the accident justifies one or more of them being designated as safety class. These analyses and evaluations should be retained as backup information to support the designations of safety class SSCs.

The evaluation guideline has been set at 25 rem total effective dose equivalent. The dose estimates compared to it are those which would be received by a hypothetical maximally-exposed individual at the site boundary from an unmitigated accidental release of radionuclides during a finite period, nominally 2 hours, but no longer than 8 hours. The time limitation is solely for the purpose of limiting the calculation to time periods for which a significant release rate might be expected and to provide a stable basis for the calculation. The 25 rem level was chosen to be representative of a potential release that could impact the offsite public and warrant special consideration of preventative and mitigative measures. The intended function of the evaluation guideline is strictly to identify safety SSCs that should be given the special designation of safety class and be subject to more rigorous design criteria as described in Section 5 of this Guide. Because of uncertainties in analysis and design parameters before final design, the 25 rem value should not be regarded as a “bright line.” If unmitigated dose results are in the rem range, then serious consideration should be given to identifying related safety SSCs as safety class. In most cases it will be found that mitigating safety class SSCs effectively reduce offsite doses far below 25 rem. Especially considering this, it should emphatically be understood that 25 rem is not an acceptance criterion for safety design.

If a postulated bounding accident for any accident scenario type could be expected to occur during facility operations, then, in addition to the evaluation guideline discussed above, it must also be considered as part of normal operations, which is governed by 10 CFR 835, Occupational Radiation Protection; unintended releases of sufficiently high frequency as considered a part of

normal operations would also be governed by this regulation. This is not to imply, however, that safety SSCs should be identified based on compliance with 10 CFR 835. Any accidents that have a significant consequence potential to the public or workers, independent of likelihood, must be thoroughly evaluated, including the identification of appropriate safety SSCs and Administrative Controls.

The relevant factors for dose calculation are discussed below, and guidance is given for each.

Dose Calculation Location

For the purposes of comparison to the evaluation guideline, the comparison point is taken to be the location of a theoretical maximally exposed offsite individual (MOI) standing at the site boundary. This location can also be beyond the DOE site boundary if a buoyant or elevated plume is not at ground level at the DOE site boundary. In such cases, the calculation location is taken at the point of maximum exposure, typically where the plume reaches ground level. With regard to members of the public who may be on-site, DOE's position on this issue is that individuals on-site, both workers and public, come under the emergency response plans and capabilities of the site. This protection, along with implementation of defense-in-depth and worker safety philosophy through safety SSCs and DOE's safety management programs address on-site safety. However, an annual assessment of any changes in the site boundary and potential effects on safety SSC classification should be performed, in association with the required annual update of the Safety Analysis Report for a facility. These may be affected by privatization and site turnover initiatives.

Atmospheric Dispersion

The 95th percentile of the distribution of doses to the MOI, accounting for variations in distance to the site boundary as a function of direction, is the comparison point for assessment against the evaluation guideline. The method used should be consistent with the statistical treatment of calculated X/Q values described in regulatory position 3 of Nuclear Regulatory Commission (NRC) Regulatory Guide 1.145 for the evaluation of consequences along the exclusion area boundary. The determination of distance to the site boundary should be made in accordance with the procedure outlined in position 1.2 of Regulatory Guide 1.145. NRC Regulatory Guide 1.23 presents acceptable means of generating the meteorological data upon which dispersion is based. Accident phenomenology may be modeled assuming straight-line Gaussian dispersion characteristics, applying meteorological data representing a 1-hour average for the duration of the accident. Accident duration is defined in terms of plume passage at the location of dose calculation, for a period not to exceed 8 hours. Prolonged effects, such as resuspension, need not be modeled. It is important to note, however, that the calculation requires MOI immersion in the main body of the plume for a period representative of its passage (subject to the 8-hour restriction). The accident progression should not be defined so that the MOI is not substantially exposed (i.e., using a release rate that is specifically intended to expose the MOI to only a small fraction of the total material released, or defining time and windspeed so that the plume has not reached the MOI). The exposure period begins from the time the plume reaches the MOI.

For ground releases, the calculated dose equates to the centerline dose at the site boundary. For elevated, thermally buoyant, or jet releases, plume touchdown may occur beyond the site boundary. As noted in the discussion of receptor location, these cases should locate the dose calculation at the point of maximum dose beyond the site boundary, which is typically at the point of plume touchdown.

Accidents with unique dispersion characteristics, such as explosions, may be modeled using phenomenon-specific codes more accurately representing the release conditions. Discussion should be provided justifying the appropriateness of the model to the specific situation. For accident phenomena defined by weather extremes, actual meteorological conditions associated with the phenomena may be used for comparison to the evaluation guideline.

Source Term

The radioactive airborne source term is typically estimated as the product of five factors: (1) material-at-risk, (2) damage ratio, (3) airborne release fraction, (4) respirable fraction, and (5) leakpath factor. Detailed discussion of these parameters is provided in DOE-HDBK-3010-94, *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*.

Material-at-Risk. The material-at-risk values used in hazard and accident analysis should represent documented maximums for a given process or activity. While DOE-STD-1027-92, Change 1, September, 1997 excludes material in qualified containers from consideration for the purposes of hazard classification, such material can be excluded in the source term for the applicable accident scenarios, only if the containers can be shown to perform their functions under the accident environments (per the Standard).

Damage Ratio. The damage ratio is that fraction of material actually impacted by the accident-generated conditions. DOE-HDBK-3010-94 notes that some degree of ambiguity can result from overlapping definitions of material at risk and damage ratio in various applications. One consistent means of definition should be used throughout.

Airborne Release Fractions and Respirable Fractions. Bounding estimates for radionuclide airborne release fractions and respirable fractions for a wide variety of material at risk and release phenomena are systematically presented in DOE-HDBK-3010-94. In those cases where there may be significant direct shine contribution to dose, that contribution should be evaluated without use of the respirable fraction.

Leakpath Factor (LPF). The leakpath factor is the fraction of material passing through some confinement deposition or filtration mechanism. Several leakpath factors may be associated with a specific accident; e.g., fraction passing from a glovebox, fraction passing from a room, fraction passing through filtration vis-a-vis door leakage. (For unmitigated accident calculations, LPF = 1.0.)

2.1.3 Safety-Significant SSCs

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

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

As a rule of thumb, safety-significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in a prompt worker fatality or serious injuries (e.g., loss of eye, loss of limb) or significant radiological or chemical exposures to workers. This rule of thumb is neither an evaluation guideline nor a quantitative criterion. It represents a threshold of concern for which safety-significant SSC designation may be warranted. Estimates of worker consequences for the purpose of a safety-significant SSC designation are not intended to require detailed analytical modeling, due to the uncertainties in analyses, especially for facility workers. Considerations should be based on engineering judgment of possible effects and the potential added value of safety-significant SSC designation. Experience has shown that safety-significant SSCs identified through defense-in-depth considerations also provide safety for workers.

2.2 External Design Constraints

The primary inputs for facility design include the DOE mission requirements, DOE O 420.1, and externally imposed regulatory inputs from Federal [e.g., Occupational Safety and Health Administration (OSHA), Environmental Protection Agency, etc.], State, and local governments where the facility is located (e.g., a stack monitor to record releases to comply with local environmental monitoring requirements), and DOE O 430.1A, LIFE CYCLE ASSET MANAGEMENT, which calls for the use of national consensus codes and standards. As a minimum, design and construction must conform to the model building codes applicable for the state or region, supplemented with additional safety requirements associated with the hazards in the facility in a graded manner.

2.3 Defense in Depth

Defense in depth includes conservative siting, minimization of material at risk, the use of conservative design margins and QA, the use of successive physical barriers for protection against the release of hazardous materials, 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 hazardous materials associated with the potential for accidents with significant public impact), the use of equipment and Administrative Controls which restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition, means to monitor accident releases required for emergency response, and the provision of emergency plans for minimizing the effects of an accident.

With respect to factors within the influence of the facility designer, defense in depth is a safety design concept or strategy that must be applied at the beginning and maintained throughout the facility design process. This safety design strategy is based on the premise that no one layer of protection is completely relied upon to ensure safe operation. By applying this safety strategy, the DOE O 420.1 objective of providing multiple layers of protection to prevent or mitigate an unintended release of radioactive material to the environment can be achieved. Conceptually, there are three levels of defense in depth.

The first level of defense consists of a well-designed facility with process design to reduce source terms, reliable SSCs that are simple to operate and maintain and resistant to degradation, and personnel well trained in operations and maintenance and committed to a strong safety culture.

The second level recognizes that failures of systems and components and human failures cannot be entirely eliminated and that protective features (e.g., engineering design features and Administrative Controls) are required. These features are provided to ensure a return to normal operation or to bring the facility to a safe condition in the event of postulated abnormal events. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such response to off-normal conditions can effectively halt the progression of events toward an accident.

The final level of defense consists of conservatively designed safety SSCs to prevent or mitigate the consequences of accidents that may be caused by errors, malfunctions, or by events that occur both internal and external to the facility.

The following are elements of defense-in-depth related to safety design and construction that must be objectives during the design process.

- **Siting.** Consider site locations that reduce the need to provide design measures to alleviate potentially hazardous conditions or to protect surrounding populations. For example, consideration of ground instability, flooding, and hazards due to nearby installations or activities.

- **Material at risk.** Apply facility and process design and Administrative Controls to minimize and control inventories of radioactive materials and their forms.

- **Conservative design.** Design conservative margins that may allow operations to deviate from normal conditions before requiring corrective actions and taking into consideration the potential degradation of elements and operational errors.

- **Quality assurance (QA).** Use QA practices for the design and construction of safety SSCs whose stringency is commensurate with anticipated hazards, including but not limited to the assurance of qualified design and construction personnel, traceability of design decisions and procurements, and documentation of changes in design and construction.

- **Physical barriers.** Design physical barriers to confine radioactive material and thereby prevent uncontrolled releases.

- **Critical safety functions.** Design to provide multiple ways for safety functions to control processes, to maintain processes in a safe state, and to confine radioactivity when accidents could have the potential for significant public radiological impact.

- **Equipment and Administrative Controls.** Include features to control process variables to values within safe conditions, to alert operating personnel of an approach toward conservative process limits, to allow timely detection of failure or malfunction of critical equipment, and to allow for the imposition of Administrative Controls assumed in the hazard analysis, and/or accident analysis.

- **Emergency features.** Include alarms and monitors to alert workers and the public to the existence of unsafe conditions and to record the sequence and severity of an accident. Evacuation considerations incorporated into the facility design are to be coordinated with the development of the emergency plan.

The detailed design criteria requirements for these defense-in-depth elements that must be used are defined in Section 3, Elements of Design for Nuclear Safety; Section 4, Functional Design Criteria; and Section 5, Supplementary Design Criteria for Safety Structures, Systems, and Components, of this Guide.

2.4 Systems Engineering

The systems engineering process covers a broad range of activities that involves the design and management of a total facility. For the purpose of this Guide, the focus will be on those elements of systems engineering that relate to nuclear safety and should be considered as part of the overall facility system engineering activities. The systems engineering activities relating to nuclear safety include the following:

- identifying and integrating facility nuclear safety requirements;

- coordinating multidisciplinary teamwork in implementing facility safety requirements;

- providing nuclear safety-related interface management;

- providing configuration management to include the establishment of baseline configuration; and

- coordinating technical reviews of the facility nuclear safety features.

The application of systems engineering activities to the nuclear safety aspects of facility design should be graded and commensurate with the facility hazards and complexity. The goal is to ensure that the systems engineering activities include consideration of the appropriate facility safety features. Electronic Industries Association Interim Standard, System Engineering, and the

applicable Guides for DOE O 430.1A should be used for guidance in developing systems engineering actives to enhance the facility safety design.

2.5 Quality Assurance

As required by 10 CFR 830.120, Quality Assurance Requirements, nuclear facilities must develop and implement a QA program that meets the requirements contained therein. Supplemental information and acceptable methods for implementing these requirements are found in Implementation Guide For Use with 10 CFR 830.120, G-830.120. QA encompasses all those planned and systematic actions and controls necessary to ensure that risk to the public health and safety and the environment are controlled and that the safety, reliability, and performance are realized through the application of effective management systems. The "graded approach" should be applied when identifying QA requirements for SSCs; that is, the scope and breadth of the requirements contained within the QA program should be adjusted to reflect the importance of the safety function of the SSCs.

The degree of implementation of the QA Program should evolve concurrently with the project through its life cycle. Specifically, the QA requirements identified for the design, fabrication, construction, and modification of an SSC must be documented and supported by the facility's safety analysis.

Document and change control for project design documents and supporting documentation must be provided by the design activity during the design. By the start of construction, document and change control must be provided by an appropriate QA configuration management program. Subsequent changes to project design and supporting documents must be made by means of a formal change control program in accordance with 10 CFR 830.120. Additional QA criteria for safety SSCs are found in Section 5, Supplementary Design Criteria for Safety Structures, Systems, and Components, of this Guide.

3. ELEMENTS OF DESIGN FOR NUCLEAR SAFETY

3.1 General

This section provides design guidance and identifies key documents that contain safety design requirements for the design and construction of DOE nonreactor nuclear facilities. The predominant model building codes in the region must govern on issues not covered in this Guide. Section 4.2, Fire Protection, of DOE O 420.1 must apply for fire protection and life safety criteria.

When developing the safety aspects of the facility design, there is a logical sequence of design considerations to follow. First, the radioactive and/or hazardous material inventory should be minimized and material forms considered. Next, conservative design margins should be applied as appropriate. Finally, appropriate preventive and mitigative features should be considered. Successful application of these principles and features into the facility design will result in a safe facility design.

3.1.1 Radioactive and/or Hazardous Material Inventory

The basic and most effective means of controlling the hazards inherent in the facility is the restriction of inventories and forms of radioactive and/or hazardous materials. Emphasis should be placed on limiting the quantities of radioactive and/or hazardous materials in both process and storage areas. Material may be rendered less hazardous by maintaining it in more stabilized and less dispersible forms. For example, a quantity of plutonium stored in metal form presents less of a hazard than the same quantity stored in its oxide form.

3.1.2 Conservative Facility Design

The next area of emphasis should be conservative design margins that account for deviations from normal process parameters. The facility design also should accommodate means such as monitors and automatic and manual controls to restrict deviations from normal operations and to assist recovery during the early stages of an accident sequence. Conservative design features apply to safety SSCs as described in Section 5.1.1.1 of this Guide.

3.1.3 Preventive Features

To prevent abnormal facility conditions from progressing to accidents, preventive features should be considered in the design. The objective of these features is to provide a return to normal operation or return to a safe condition. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such response to off-normal conditions can effectively halt the progression of events toward an accident.

3.1.4 Mitigating Features

Safety SSCs must be provided to mitigate consequences of accidents that may still occur despite the application of the preceding conventions. The safety SSCs must be identified through the safety analysis (see Section 2.1 of this Guide).

3.2 Siting Criteria Development

The following factors should be considered in determining facility site suitability and in establishing facility safety design criteria:

- the site boundary and land-use characteristics of the site surroundings, including properties at risk from accidental exposures, public exclusion zones (access control), population-center distances, and population density;
- proximity of services such as the fire department and emergency medical centers;
- utility systems essential to support safety class SSCs;
- physical characteristics of the site, including topography, meteorology, and hydrology;
- geological and subsurface elements such as earthquake loading, soil bearing design capacity, rock or other bearing stratum, and groundwater elevations;
- natural phenomena hazards as discussed in Section 3.3, Natural Phenomena Hazards, of this Guide and DOE O 420.1, Section 4.4, Natural Phenomena Hazards Mitigation, including seismic activity, wind, hurricane, tornado, flood, hail, volcanic ash, lightning, and snow;
- emergency response considerations, including population sheltering or shielding parameters and evacuation delay times and rates for the public and colocated workers;
- potential human-induced hazards from nearby facilities or activities such as industrial and military facilities, aircraft impacts, pipelines, and transportation routes;
- proximity and hazard to other facilities (from the proposed facility); and
- site-related assumptions of the Environmental Impact Statement.

For the purpose of this Guide, a radiological siting criterion of 25 rem, 50-year total effective dose equivalent must be used, from releases over the course of postulated design basis accidents from uptakes at the site boundary that could be delivered during a one year period.

3.3 Natural Phenomena Hazards

3.3.1 General Application

Safety SSCs must be designed and constructed to withstand the effects of natural phenomena hazards. Fundamental requirements for natural phenomena hazards are specified in the regional model building codes. The natural phenomena design requirements for safety SSCs as specified in DOE O 420.1, Section 4.4, and the associated DOE Standards must apply to safety SSCs as determined by the methodology described in DOE-STD-3009-94. The safety-class or safety-significant designation is the basis for selecting the specified natural phenomena design requirements found in the referenced DOE Standards.

3.3.2 Primary Applicable Requirements

- DOE O 420.1, Section 4.4, and its Guide
- DOE-STD-1020-94, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*
- DOE-STD-1021-93, *Natural Phenomena Hazards Performance Categorization Guidelines for Structures, Systems, and Components*
- DOE-STD-1022-94, *Natural Phenomena Hazards Site Characterization Criteria*
- DOE-STD-1023-95, *Natural Phenomena Hazards Assessment Criteria*
- DOE-STD-1024-92, *Guidelines for Use of Probabilistic Seismic Hazard Curves at Department of Energy Sites for Department of Energy Facilities*

3.3.3 Other Considerations

Design considerations for volcanic eruption and ash fall, lightning strikes, range fires, snow loads, and extreme temperatures are not provided in DOE O 420.1, Section 4.4, and other associated standards. Criteria for the assessment and mitigation of these hazards must be developed on a site-specific basis and approved by DOE prior to use. Lightning protection systems must be considered for buildings and structures that contain, process, and store radioactive, explosive, and similarly hazardous materials. Lightning protection systems must be designed to comply with National Fire Protection Association (NFPA) 780. (See DOE O 420.1, Sections 4.3 and 4.4.)

Design considerations should be given to the interaction of more than one event, particularly those more likely to occur simultaneously. For example, heavy rains usually accompany tornadoes or high winds; excessive roof loads may result from rain and accumulated volcanic ash; and upstream dams may fail due to seismic events.

3.4 Architectural

The type and level of hazards should be determined for each functional area, the attendant degree of risk established, and the possibility of cross contamination considered. Wherever possible, work areas with compatible contaminants should be located together to simplify design criteria related to air supply and exhaust, waste disposal, decontamination, and cross contamination.

Radioactive and hazardous material contamination control requirements should be considered in the design to minimize the potential for contamination spread.

Office areas should be located in common-use facilities (e.g., data computation and processing, word processing, etc.) and away from process areas to minimize risks to workers of exposure to radioactive and/or hazardous materials.

3.4.1 Building Layout

The building layout should provide protection from the hazards associated with handling, processing, and storing of radioactive and/or hazardous materials. In addition, the following items should be considered in the facility safety design.

- Additional space should be provided for temporary or additional shielding in the event radiation levels are higher than anticipated.

- The arrangement and location of hazardous process equipment and its maintenance provisions should provide appropriate protective and safety measures as applicable.

- The building design should accommodate prompt return to a safe condition in emergencies and allow ready access for and protection of workers in areas where manual corrective actions are required and in areas that contain radiation monitoring equipment readouts.

- Facility layout should provide specific control and isolation, if possible, of quantities of flammable, toxic, and explosive gases, chemicals, and other hazardous materials admitted to the facility.

3.4.2 Access Control

The facility design should accommodate the requirements for safeguards and security, emergency egress, and area access control for worker protection. Where these requirements may appear to conflict, life safety must take precedence. For example, safeguards and security requirements would minimize the number of entrances and exits, but for worker safety, the emergency-egress requirements would provide an adequate number of exits. Specific requirements for access control must be implemented as specified by 10 CFR 835 for radiological hazards, by the Resource Conservation and Recovery Act (RCRA) for hazardous waste treatment, storage, and

disposal facilities, and by 29 CFR 1910 and 1926 (OSHA) for hazardous material locations within operating facilities and construction sites.

Where access control is provided for control rooms that contain safety-class SSC controls and monitoring, the same level of qualification must be considered for the access control features. Access controls must not prevent operator actions required to achieve and maintain a facility in a safe condition.

3.5 Accessibility and Maintainability

Section 4.1.1.2 of DOE O 420.1 requires that facilities be designed to facilitate inspection, testing, maintenance, and repair and replacement of safety SSCs to assure their continued function, readiness for operation, and accuracy. The facility design must include provisions for accessibility and maintainability that include but are not limited to the following:

- Surveillance equipment should be located and sufficient space provided for relative ease of routine testing and maintenance activities.

- Accessible inspection covers to allow for visual inspection should be provided and located such that necessary routine inspections can be conducted with minimum disruption to the facility or equipment operation. Examples include ducting and process piping systems.

- The facility design should include features that provide for ease of routine maintenance without a subsequent mission reduction. Examples include providing sufficient clearance around equipment to accommodate change out of large components and providing permanent ladder(s) and platform(s) access to lubrication and equipment areas.

A Reliability, Availability, and Maintainability (RAM) program should be established in accordance with the guidance of DOE RELIABILITY, AVAILABILITY, AND MAINTAINABILITY GUIDELINES (Draft) and graded as to the complexity and hazards of the facility. The purpose of a RAM program is to help ensure that the project will be free of RAM-related problems that could prevent achieving health, safety, environmental, performance, schedule, and economic goals.

3.6 Human Factors Engineering

Appropriate human factors engineering principles and criteria should be integrated into the design, operation, and maintenance of DOE facilities. The human factor elements that should be considered include, but are not limited to, the following: equipment labeling, workplace environment (temperature and humidity, lighting, noise, vibration, and aesthetics), human dimensions, operating panels and controls, component arrangement, warning and annunciator systems, and communication systems. The applicable criteria found in Nuclear Regulatory Guide (NUREG) 0700, MIL-STD-1472D [Department of Defense (DoD)], and American

National Standards Institute (ANSI)/Institute of Electrical and Electronic Engineers (IEEE) 1023 should be considered in the design of these elements.

3.7 Design to Facilitate Deactivation, Decontamination, and Decommissioning

3.7.1 Deactivation

Deactivation is the process of removing hazardous materials and neutralizing hazardous conditions at the end of a facility's life or mission prior to decontamination and decommissioning. Design to facilitate deactivation would incorporate facility features that aid in the removal of surplus radioactive and chemical materials; storage tank cleanout and maintenance; stabilization of contamination and process materials; and the removal of hazardous, mixed, and radioactive wastes. In general, these features would reduce the physical risks and hazards associated with facility decontamination and decommissioning and would also be called for when designing for ease of maintenance during operation.

3.7.2 Decontamination

In accordance with DOE O 420.1, the facility design must incorporate measures to simplify decontamination of areas that may become contaminated with radioactive or hazardous materials. Items such as service piping, conduits, and ductwork should be kept to a minimum in potential contamination areas and should be arranged to facilitate decontamination. Walls, ceilings, and floors in areas vulnerable to contamination should be finished with washable or strippable coverings. Metal liners should be used in areas that have the potential to become highly contaminated. Cracks, crevices, and joints should be filled and finished smooth to prevent accumulation of contaminated material. The facility design should incorporate features that will facilitate decontamination to achieve facility decommissioning, to increase the potential for other uses, or both.

3.7.3 Decommissioning

Design features consistent with the requirements of DOE O 435.1, RADIOACTIVE WASTE MANAGEMENT, should be developed during the planning and design phases based on decommissioning requirements or a conversion method leading to other facility uses. The following design principles should be considered:

- Use of localized liquid-transfer systems with emphasis on localized batch solidification of liquid waste to avoid long runs of buried contaminated piping. Special provisions should be included in the design to ensure the integrity of joints in buried pipelines.

- Location of exhaust filtration components of the ventilation systems at or near individual enclosures to minimize long runs of internally contaminated ductwork.

- Equipment, including effluent decontamination equipment, that precludes, to the extent practicable, the accumulation of radioactive or other hazardous materials in relatively

inaccessible areas, including curves and turns in piping and ductwork. Accessible, removable covers for inspection and cleanouts are encouraged.

- Use of modular radiation shielding in lieu of or in addition to monolithic shielding walls.
- Provisions for flushing and/or cleaning contaminated or potentially contaminated piping systems.
- Provisions for suitable clearances, where practical, to accommodate remote handling and safety surveillance equipment required for future decontamination and decommissioning.
- Use of lifting lugs on large tanks and equipment.
- Piping systems that carry contaminated or potentially contaminated liquid should be free draining via gravity.

4. FUNCTIONAL DESIGN CRITERIA

4.1 Nuclear Criticality Safety

4.1.1 Conditions that Initiate Requirements of this Section

Any DOE facility that may produce, process, store, transfer, dispose, or otherwise handle sufficient quantities of fissionable material that present a concern for accidental criticality must be designed to meet the requirements of DOE O 420.1, Section 4.3, Nuclear Criticality Safety.

4.1.2 Primary Applicable Requirements

DOE O 420.1, Section 4.3, contains requirements that facilities be designed in such a manner that the probability of a criticality accident is acceptably low and, to the extent practical, the public, the workers, and the environment are protected from damaging effects and undue hazards that may arise from a criticality accident as required; that no single credible event or failure must result in a criticality accident having unmitigated consequences; and that criticality accident alarm systems and criticality detection systems be included. See DOE O 420.1, Section 4.3, and its supporting standards for details.

4.2 Radiation Protection

4.2.1 Primary Applicable Requirements

The control of radiological exposures of workers, the public, and the environment must be in accordance with Section 4.1.1.2 of DOE O 420.1, 10 CFR 835, and 10 CFR 834 (Proposed). Additional guidance is contained in the *DOE Radiological Control Manual* (DOE/EH-0256T).

4.2.2 General Application

The primary objective of radiological protection is to minimize personnel external and internal exposures to radioactive materials; provide adequate radiation posting, sampling, monitoring, and notification or alarm capabilities; and apply ALARA principles. Radiation protection should be provided through facility physical design (e.g., shielding, remote handling, area layout, equipment layout, confinement, and ventilation) and supplemented by cautionary systems. ALARA principles to minimize personnel exposures must be applied to all equipment and facility designs.

Specific criteria for monitoring and entry control systems, posting and labeling of radioactive materials, nuclear accident dosimetry, and ALARA applications must be applied as required by 10 CFR 835.

Offsite dose limits used to assess acceptability of the facility safety design during normal operations and anticipated operational occurrences must comply with 10 CFR 834 (Proposed).

Physical layout and details of proven radiological equipment designs are contained in the DOE adopted IAEA Safety Series 30 Standard and Faust (1988).

The projected dose rates must be based on occupancy, duration, and frequency of exposure and must not exceed values specified in 10 CFR 835. This may require that shielding be provided for areas requiring normal and intermittent access, such as those for preventive maintenance, component changes, or adjustment of systems and equipment. The type of shielding should be determined by the characteristics of the radiation, structural requirements, fire protection requirements, and radiation damage potential. Shielding should also be installed to minimize nonpenetrating external radiation exposures to the skin and lens of the eye where required. In most cases, confinement barriers or process equipment provide this function. Where shielding is an integral part of the facility structure, it must be designed and installed to at least the same level of natural phenomenon qualification as the facility structure. Additional guidance is contained in ANSI/ANS 6.4.2. Where shields are identified as safety class, the additional requirements stated in Section 5 of this Guide.

Occupied operating areas for normal operating conditions must be designed not to exceed the airborne concentration limits of 10 CFR 835. Respirators should not be required under normal operating conditions except as a precautionary measure. Engineered controls and features should be designed with consideration of contaminant chemical forms to minimize potential inhalation of radioactive materials.

Devices to monitor individual exposures to external radiation and to warn personnel of radioactive contamination must be used in accordance with 10 CFR 835. Air sampling equipment should be placed in strategic locations to detect and evaluate airborne contaminant conditions at work locations. Continuous air monitors with preset alarms should be provided to give early warning of significant releases of radioactive materials. Air monitoring and warning systems must comply with the requirements of 10 CFR 835 with consideration for additional guidance contained in ANSI N13.1.

Breathing-air supply systems, if required, must comply with 29 CFR 1910.134.

4.2.3 Special Considerations and Good Engineering Practices

American Nuclear Society document ANS 11.16 contains guidance on functional designs based on both DOE and NRC experiences. DOE/EH-0256T provides details on radioactive material identification, storage, and transport. These documents provide descriptions and details of use-proven principles and designs and identify considerations that affect configuration, hardware selection, installation, maintenance, and controls that can be used in developing a sound functional design.

Shielding should be designed to limit the total external dose during normal operations to the annual exposure limit values as specified in 10 CFR 835. Design of facilities and shields applicable to machines and sources is summarized as good practices in NCRP Report 49. Additional guidance is contained in ANSI N43.2.

Guidance on ventilation design is provided by an ACGIH document (ACGIH 2092-1998) and ERDA 76-21. Alarms for loss of ventilation or differential pressure must be provided on primary confinement systems (gloveboxes or hoods) and should be considered on secondary confinement systems (rooms). ANSI/ASME N509 contains requirements for the design of nuclear facility air cleaning systems and ANSI/ASME N510 contains requirements for testing air cleaning systems.

Change rooms for changing into and out of protective clothing should be designed to ensure that clean clothing (personal clothing) and contaminated clothing (protective clothing) are segregated. The design objective is to ensure that storage of contaminated protective clothing will control contamination so that it does not spread beyond the storage container. The change room exhaust air should be high-efficiency particulate air (HEPA) filtered as applicable if dispersible radionuclides are handled in the process areas it serves.

Personnel decontamination facilities should be located close to areas that are potential sources of contamination. Safety showers may be used if water collection from their use is controlled. Portable personnel decontamination equipment should be considered for facilities with no permanent structures.

Respiratory protection should be provided to maintenance personnel where potentially significant exposures exist for maintenance operations and design constraints preclude the ability to perform maintenance either remotely or in a glovebox. However, every reasonable effort should be made to allow routine maintenance activities to be conducted without the need for respiratory protection.

4.3 Hazardous Material Protection

This section provides functional design guidance for hazardous material protection other than radioactive material protection. While not controlled by DOE O 420.1, Section 4.1, directly, these considerations may indirectly relate to nuclear safety in that hazardous material releases may cause or exacerbate nuclear accidents. The hazard analysis must establish any potential for hazardous material release accidents that cause or exacerbate a nuclear accident. This potential must be considered in the accident analysis and the selection of safety SSCs.

4.3.1 Conditions that Initiate Requirements of this Section

Any facility where personnel could potentially be exposed to hazardous materials listed in 29 CFR 1910 at concentrations approaching the listed permissible exposure limits (8-hour, time-weighted average, normal operations) must comply with the requirements of the applicable laws for hazardous material protection.

4.3.2 Primary Applicable Requirements

Requirements for design of engineered controls for hazardous material protection are contained in 29 CFR 1910, Subparts G, H, and Z.

4.3.3 General Application

Ventilation systems are engineering controls commonly used to prevent worker exposure to hazardous materials and are used in combination with personal protective equipment and operational procedures. 29 CFR 1910, Subpart G, 1910.94, requires that where ventilation is used to control worker exposures, it must be adequate to reduce the hazardous material concentrations of air contaminants to the degree that the hazardous material no longer poses a health risk to the worker (i.e., concentrations at or below the permissible exposure limits). 29 CFR 1910, Subpart Z, 1910.1000, requires that wherever engineering controls are not sufficient to reduce exposures to such levels, they must be used to reduce exposures to the lowest practicable level and supplemented by work practice controls. The design should ensure that respirators are not required for normal operating conditions or routine maintenance activities except as a precautionary measure.

Ventilation systems for hazardous material protection should use exhaust hoods to control concentrations of hazardous materials from discrete sources, or should control the number of air changes per hour for an entire room or bay. Air flow and other design requirements for specific types of systems must comply with 29 CFR 1910, Subparts G and H. 29 CFR 1910, Subpart Z, provides requirements for monitoring and alarm systems for facilities that manage or use specific hazardous materials. Additional guidance on design of ventilation systems for hazardous material protection is provided in ANSI Z9.2 and ASHRAE 62. Decontamination facilities, safety showers, and eyewashes to mitigate external exposures to hazardous materials must be provided where mandated by 29 CFR 1910, Subparts H and Z. These systems must be designed in accordance with the requirements of ANSI Z358.1 and ANSI Z124.2.

4.3.4 Special Considerations and Good Engineering Practices

Facilities with hazardous material exposure concerns should be designed to minimize personnel exposures, both external and internal, and to provide adequate monitoring and notification capabilities to inform workers of unsafe conditions. Hazardous material protection should be provided through facility design (e.g., remote handling, area and equipment layout, spill-control features, confinement, ventilation, etc.). Occupied spaces should be designed to preclude locations where low oxygen content or air displacement may occur or where reactive, combustible, flammable, or explosive gas, vapor, or liquid accumulation might occur.

Safety controls and features should be designed to consider contaminant chemical forms and minimize the potential for inhalation and contact under all conditions. Directed ventilation flow paths should be used to move contaminants away from worker breathing zones. The design should ensure that ventilation flow will cascade from clean areas to contaminated areas to preclude contamination spread. Uniform distribution of incoming air and/or air mixing equipment should be provided to ensure that no pockets of stagnant air exist in areas where workers are present.

4.4 Effluent Monitoring and Control

4.4.1 Applicability

This section applies to any DOE facility that produces airborne or liquid radioactive and/or hazardous material effluents, including contaminated storm water, under normal operating conditions.

4.4.2 Special Considerations and Good Engineering Practices

Liquid process wastes containing radioactive and/or hazardous material should be collected and monitored near the source of generation before batch transfer via appropriate pipelines or portable tanks to a liquid-waste treatment facility. Waste storage tanks and transfer lines must be designed and constructed so that any leakage should be detected, contained, and collected for removal before it reaches the environment. Double-walled transfer pipelines or multiple encasements should be used for high-level radioactive liquid wastes and other liquid wastes that have the potential to cause significant localized consequences as defined by safety analysis, or significant exposures during the implementation of mitigating measures in the event of an accidental release. Provisions should be made for the collection, removal, and appropriate disposition of infiltration into the annulus of double-walled pipelines. Radioactive- and hazardous-waste collection, transfer, and storage systems must be designed to avoid the dilution of radioactive or hazardous waste by waste of lower concentrations of radioactivity, toxicity, or other hazard. Emphasis should be placed on reducing radioactive constituents in liquid effluents released to surface waters or soil columns to levels ALARA.

All airborne effluents from areas in which hazardous or radioactive materials are managed other than in closed containers should be exhausted through a ventilation system designed to remove particulate material, vapors, and gases, as necessary, to comply with applicable release requirements and to reduce releases of radioactive materials to levels ALARA. The design of airborne-effluent systems should preclude holdup of particulate materials in offgas and ventilation ductwork and include provisions to continuously monitor buildup of material and material recovery. The design of systems must also preclude the accumulation of potentially flammable quantities of gases generated by radiolysis or chemical reactions within process equipment.

The design capacity for effluent monitoring and control systems must be consistent with the needs for handling process effluents during normal operations, anticipated operational occurrences, and DBA conditions. Alarms must be provided that will annunciate in the event concentrations of radioactive or hazardous materials above specified limits are detected in the effluent stream. Appropriate manual or automatic protective features must be provided to prevent an uncontrolled release of radioactive and/or hazardous material to the environment or the workplace. Portions of effluent management systems and components that are required to control or limit the release of radioactive or hazardous materials to the environment or for safe operation of the system must be provided with redundancy where required by applicable federal, state, and local environmental regulations and permits. Effluent monitoring and control systems

must be designed to allow periodic maintenance, inspection, and testing of components and to maintain occupational radiation doses ALARA during these operations. Appropriate nuclear criticality safety provisions must be applied to the design of airborne effluent systems. This includes design to preclude the holdup or collection of fissile material and other material capable of sustaining a chain reaction in portions of the system not geometrically favorable and design to ease of recovery of these materials in case of an accident as well as during normal operations.

The design of safety SSCs, as identified in the facility-specific safety analysis, must comply with the requirements of Section 5 of this Guide. Safety-class effluent monitoring and control SSCs are generally designed to operate in conjunction with physical barriers to form a confinement system to limit the release of radioactive or other hazardous material to the environment and to prevent or minimize the spread of contamination within the facility. Adequate instrumentation and controls must be provided to assess system performance and to allow the necessary control of system operation. Equipment in safety-class systems must be appropriately qualified or protected to ensure reliable operation during normal operating conditions, during anticipated operational occurrences, and during and following a design basis earthquake. Safety-class air filtration units, effluent transport systems, or effluent collection systems must be designed to remain functional throughout DBAs and to retain collected radioactive and hazardous materials after the accident.

4.5 Waste Management

This section applies to any DOE facility that under normal operating conditions produces containers of wastes having constituents that are regulated as radioactive, hazardous, or mixed waste. The design of waste management systems must be in accordance with the requirements of DOE O 435.1 and the Federal, State, and local requirements referenced therein.

Unless it can be demonstrated that the risk is acceptable, waste management and storage systems and associated support systems should be designed to remain functional following a DBA and should facilitate the maintenance of a safe shutdown condition. For high-level waste containment systems, at least one confinement barrier should be designed to withstand the effects of DBAs.

4.6 Fire Protection

4.6.1 General Application

Facility design must comply with the applicable fire protection requirements contained in DOE O 420.1, Section 4.2, Fire Protection; DOE O 440.1A, WORKER PROTECTION MANAGEMENT FOR DOE FEDERAL AND CONTRACTOR EMPLOYEES; and their companion document, DOE G 440.1-5, IMPLEMENTATION GUIDE FOR USE WITH DOE ORDERS 420.1 AND 440.1, FIRE SAFETY PROGRAM. Acceptable methods for fire protection design may be found in DOE-STD-1066-99, *Fire Protection Design Criteria*.

4.6.2 Fire Hazard Analysis

A fire hazard analysis must be prepared for each DOE facility in accordance with DOE O 420.1, Section 4.2, and should be initiated early in the design process and closely coordinated with the safety analysis effort as discussed in Section 2.1, Design Process and Safety Analysis Relationship, of this Guide.

4.7 Emergency Preparedness and Emergency Communications

4.7.1 Conditions that Initiate Requirements of this Section

This section applies to any DOE facility that must respond to internal or external emergency events to control acute exposures to radiation in excess of the annual exposure limits or to hazardous materials in excess of Permissible Exposure Limits, or to preclude multiple fatalities.

4.7.2 Primary Applicable Requirements

Provisions for emergency preparedness are contained in the requirements of DOE O 151.1, COMPREHENSIVE EMERGENCY MANAGEMENT SYSTEMS, which address installation of an Emergency Operations Center. Primary and backup means of communications with the Emergency Operations Center, provisions for evacuation and accountability; and adequate equipment and supplies for emergency response personnel to carry out their respective duties and responsibilities related to nonreactor nuclear facility must be provided in the facility design consistent with DOE O 151.1.

4.7.3 General Application

Emergency evacuation annunciation systems must conform with ANSI/ANS N2.3. General communication system installation requirements must be per NFPA 72, Section 3-12, which describes the minimum requirements for transmission of alarm conditions to building occupants, and Sections 6-3 and 6-4, which include minimum requirements for audibility above background noise and the use of visual signals, including minimum light intensities.

For facilities handling dispersible materials, meteorological data necessary to control consequences from an emergency event should be obtained from either the nearest U.S. Geological Survey or local (onsite) meteorological stations.

4.8 Explosives Criteria

The design and construction of all new DOE explosives facilities and modifications to existing explosives facilities must conform to the DOE explosives safety requirements established in the DOE EXPLOSIVES SAFETY MANUAL, DOE M 440.1-1. Facility structural design and construction must comply with the requirements of TM5-1300 (DoD), *Structures to Resist the Effects of Accidental Explosions,* and DOE/TIC-11268, *A Manual for the Prediction of Blast and Fragment Loading of Structures*. Blast resistant design for personnel and facility protection must

be based on the TNT equivalency of the maximum quantity of explosives and propellants permitted. In accordance with TM5-1300, the TNT equivalency must be increased by 20 percent for design purposes.

The technical basis for establishing explosives quantity–distance separation for facility location, design, and operation (under normal and potential DBA conditions) must follow the stricter of the criteria provided in DoD 6055.9-STD, *Department of Defense Ammunition and Explosives Safety Standards*. DoD 6055.9 specifies the minimum distance for protection from hazardous fragments to facility boundaries, critical facility, and inhabited structures unless it can be shown that there will be no hazardous fragments or debris at lesser distances. The method of calculation presented in the DoD Explosive Safety Board (DoDESB) Technical Paper No. 13 may be used to establish a smaller fragment exclusion zone. It is not intended that these minimum fragment distances be applied to operating facilities or dedicated support functions within an operating line. The criteria presented in DOE M 440.1-1 must apply for these exposures.

For an unproven facility design, either a validated model or a full-scale test is required to ensure structural adequacy unless a high degree of confidence can be provided by calculations or other means. The contract administrator (head of field organization) with the advice of competent engineering review must concur in any determination regarding test requirements.

When an explosives facility is also a nonreactor nuclear facility, the requirements for nonreactor nuclear facilities must also apply.

5. SUPPLEMENTARY DESIGN CRITERIA FOR SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS

This section provides supplementary guidance for the design and construction of safety SSCs to ensure reliable performance of their safety function under those conditions and events for which they are intended. Design methods and criteria commonly used to ensure required availability are discussed in Section 5.1, General Requirements, of this Guide. Discipline-specific consensus codes and standards (e.g., electrical, mechanical, and structural) are presented in Section 5.2, Specific Criteria, of this Guide. These design methods, design criteria, and consensus codes and standards are the minimum set of requirements that must be applied when designing safety SSCs.

5.1 General Requirements

Safety SSCs and their associated support systems must be designed, fabricated, erected, and tested to standards and quality requirements commensurate with their importance to safety. An acceptable level of assurance that the safety SSCs will perform their intended safety function can be achieved by meeting the requirements contained within the following sections.

5.1.1 Assurance of Safety Function

Safety SSCs must be designed to reliably perform their safety function under those conditions and events for which their safety function is intended. The following subsections must be applied to the design of safety SSCs to most effectively enhance system availability and provide for robust design. Further design guidance can be found in IAEA Standard No. 50-P-1 and ANSI/IEEE 603.

5.1.1.1 Conservative Design Features

Safety SSCs must be designed to withstand all design basis loadings with an appropriate margin of safety. The design should incorporate, commensurate with the importance of the safety function, multiple levels of protection against normal, anticipated, and accident conditions. For example, while built-in process controls may maintain pressure within a conservative limit, the design may also require provisions for relief valves, automatic shutdown capability, or other preventive features.

The design of safety-class SSCs must incorporate suitably conservative criteria contained in applicable DOE Orders and Standards addressing safety functions (e.g., natural phenomena design mitigation).

5.1.1.2 Design Against Single-Point Failure

The facility and its systems must be designed to perform all safety functions with the reliability indicated by the safety analysis. The single-point failure criterion, requirements, and design

analysis identified in ANSI/IEEE 379 must be applied during the design process as the primary method of achieving this reliability.

5.1.1.3 Environmental Qualification

Environmental qualification must be used to ensure that safety-class SSCs can perform all safety functions, as determined by the safety analysis, with no failure mechanism that could lead to common cause failures under postulated service conditions. The requirements from ANSI/IEEE 323 for mild environmental qualification must be used unless the environment in which the SSC is located changes significantly as a result of the DBAs. In general, qualification for mild environments should consist of two elements:

- Ensuring that all equipment is selected for application to the specific service conditions based on sound engineering practices and manufacturers' recommendations.

- Ensuring that the system documentation includes controls that will preserve the relationship between equipment application and service conditions.

5.1.1.4 Safe Failure Modes

The facility design must provide reliable safe conditions and sufficient confinement of hazardous material during and after all DBAs. At both the facility and SSC level, the design must ensure that more probable modes of failure (e.g., fail to open versus fail to close) will increase the likelihood of a safe condition.

5.1.2 Support System and Interface Design

Safety SSCs often rely upon other SSCs to support their operation. Therefore, it is important to identify these support systems and the associated interfaces between safety and nonsafety SSCs. The following subsections address the design considerations for these related systems.

5.1.2.1 Support Systems

In some cases, safety SSCs rely upon supporting SSCs to perform their intended safety function. These support SSCs may be classified as safety-class or safety-significant SSCs. For example, a safety-class designation may be appropriate for an instrumentation and control (I&C) system that supports a tritium containment system if it can be demonstrated that failure of the I&C support system can lead to either failure or reduced availability of the safety-class containment barrier. In general, the following classification criteria apply.

- Support SSCs to safety-class SSCs must be classified as safety class if their failures can prevent a safety-class SSC from performing its safety functions.

- Support SSCs to safety-significant SSCs that mitigate or prevent accidents with the potential for significant onsite consequences should be classified as safety-significant if their failures prevent a safety-significant SSC from performing its safety functions.

- Support SSCs to safety-significant SSCs that mitigate or prevent accidents with the potential for significant localized consequences need not be classified as safety significant.

5.1.2.2 Interface Design

A nuclear safety design goal is to minimize interfaces between safety-class, safety-significant, and nonsafety SSCs. Ideally, safety SSCs should not have any interfaces; however, this is not always practical. Interfaces, such as pressure retention boundaries, integrity of fluid systems, electrical equipment, I&C, and mechanical and support systems, exist between safety SSCs and between safety SSCs and nonsafety SSCs. These interfaces must be evaluated to identify SSC failures that would prevent the safety SSCs from performing their intended safety function. For these SSC failures, isolation devices, interface barriers, or design class upgrades should be provided to ensure safety SSC protection and reliability. In many cases, systems may consist of a group of subsystems, where each subsystem supports the operation of the whole system. For example, an auxiliary power diesel generator system may consist of lubricating oil, fuel oil, diesel engine, jacket cooling, and room ventilation subsystems. System interface evaluations should clearly define these boundaries. In all instances, a case-by-case evaluation should be performed.

5.1.3 Quality Assurance

The QA requirements for the design, fabrication, construction, and modification of safety SSCs are developed using the facility safety analysis. At the earliest stages of the design, a hazard analysis, which identifies the functional requirements of safety SSCs, should be used as a basis for determining appropriate QA requirements.

As the design progresses, more detailed safety analyses will be performed to develop the basis for safety SSCs performance requirements. Once the safety SSCs and their performance requirements are identified, a set of detailed QA requirements can then be specified. As part of the safety analysis, a list of all safety-class SSCs must be prepared and maintained for the life of the project through decommissioning. This listing must identify the functions, performance requirements, and natural phenomena design requirements for each safety-class SSC and the associated QA requirements. These detailed component-specific requirements are typically contained in consensus codes and standards (e.g., ANSI/IEEE). A similar listing of all safety-significant SSCs should also be prepared.

In most cases, components used in DOE nonreactor nuclear facilities will be “off the shelf”; that is, they will not be subjected to the rigorous Nuclear Quality Assurance (NQA)-1-based requirements for “nuclear-grade” components. Therefore, safety SSC quality standards can

either be design based or achieved through testing, vendor control, and inspection. However, the requirements of 10 CFR 830.120 still apply to safety SSCs.

5.2 Specific Criteria

The application of design criteria to safety SSCs entails the selection of appropriate and relevant criteria commensurate with the levels of safety. A purely prescriptive approach to the use of national codes and standards may fail to provide the appropriate level of safety. While national codes and standards will provide guidance and the basic design criteria for most systems, blanket application of such individual codes and standards or collections thereof is not necessary. It is necessary to tailor selections of codes and standards for each specific application based on the required safety function.

Note that the safety analysis conducted in accordance with DOE-STD-3009-94 that results in a particular safety classification is also the same analysis used to identify and define design criteria. Safety analyses identify the functions that must be performed and the conditions under which these functions must perform. These analyses will then result in both the functional safety classification and the identification of the appropriate and relevant criteria to ensure the prescribed safety functions can be performed.

Categorization and listing of design codes and standards as a portion of the design criteria process are performed to ensure that a correct and appropriate level of engineering design detail and attention are used for each safety classification. The intent is to specify the design codes and standards that will ensure that each safety SSC will perform its required safety function, including due consideration of the intangible areas of influence.

The national codes and standards listed in the following sections provide guidance on the minimum aggregation of codes, standards, and standard practices that should be considered in identifying the design criteria and other considerations for each specific SSC commensurate with its function. Additional design criteria may be applied as necessary to perform the safety function.

Specific design criteria for safety SSCs often relate to a confinement function. Generally, three confinement systems are used to achieve the complete confinement system objective. The terms confinement and confinement barriers used in the following sections are used in the context of the three types of confinement: primary, secondary, and tertiary (as defined in the glossary).

5.2.1 Structural

Structures classified as safety class or safety significant normally provide a passive confinement barrier and do not require redundancy in their design. The design of safety-significant and safety-class structures must ensure satisfaction of the functional requirements for the specific confinement system of which they are a part. In addition, safety-class confinement barriers must be designed to withstand likely secondary events as well as primary events with an appropriate margin of safety. Potential secondary events might be fire, explosion, or nuclear criticality

caused by the primary event. Likely secondary events are those with a probability greater than 0.1, given the primary event. See Table 5.1 for the relevant codes and refer to Section 4.4 of DOE O 420.1 and Section 3.3 of this Guide for additional natural phenomena hazards design guidance information.

Table 5.1. Codes for Safety-Significant and Safety-Class Structures.

Structures	Safety Significant	Safety Class
Concrete	ACI-318	ANSI/ACI-349
Steel	AISC-M011	ANSI/AISC-N690

5.2.2 Mechanical

Mechanical equipment classified as safety significant or safety class provides both passive and active safety functions. The redundancy criteria as described in Section 5.1.1.2 of this Guide must be applied to the design of safety-class SSCs that provide an active safety function. The redundancy criteria should be considered in the design of safety-significant SSCs that provide an active safety function. Redundancy criteria are generally not applied to the design of safety SSCs that provide a passive safety function.

5.2.2.1 Ventilation

In general, the safety function of ventilation and offgas systems is to provide confinement integrity and to filter exhaust, thereby preventing or mitigating uncontrolled releases of radioactive and/or hazardous materials to the environment. Ventilation and offgas systems are included as a vital part of the primary and secondary confinement design. The need for redundancy and the degree of redundancy in these systems must be determined by the safety analysis process and maintenance concerns for both active and passive components. Designs must provide for periodic maintenance, inspection, and testing of components. Adequate shielding must be included in the design of filters, absorbers, scrubbers, and other air treatment components to ensure that occupational exposure limits are not exceeded during maintenance and inspection activities.

Safety-significant and safety-class ventilation system designs must include adequate instrumentation to monitor and assess performance with necessary alarms for annunciation of abnormal or unacceptable operation. Manual or automatic protective control features must be provided to prevent or mitigate an uncontrolled release of radioactive and/or hazardous material to the environment and to minimize the spread of contamination within the facility.

Vent streams potentially containing significant concentrations of radioactive and/or hazardous materials must be processed through an offgas cleanup system before being exhausted to the

environment. Cleanup systems are to remove particulates and noxious chemicals and control the release of gaseous radionuclides. The design of safety-significant and safety-class offgas systems must be commensurate with the sources and characteristics of the radioactive and chemical components of the offgas air stream to prevent or mitigate the uncontrolled releases of radioactive and/or hazardous materials to the environment. See Table 5.2 for the relevant codes.

Table 5.2. Codes for Safety-Significant and Safety-Class Ventilation System Components.

Ventilation	Safety Significant	Safety Class
Ducts	SMACNA Manual	SMACNA Manual
Fans	ASHRAE Handbook	ASHRAE Handbook; ANSI/ANI-59.2
Filtration	ASHRAE-52.1; Mil-F-51068F; ANSI/ASME-N509 and N510; DOE NE STD-F3-45	ASHRAE-52.1; Mil-F-51068F; ANSI/ASME-N509 and N510; DOE NE STD-F3-45

5.2.2.2 Process Equipment

The usual safety function of process equipment is to provide primary confinement and prevent or mitigate radioactive and/or hazardous material releases to the environment. Process equipment that would be required to provide primary confinement includes the following: piping, tanks, pressure vessels, pumps, valves, and gloveboxes. These examples represent process system components that could be used to contain radioactive or toxic materials directly. Process equipment for some applications can provide secondary confinement. Examples include double-walled piping systems, double-walled tanks, and gloveboxes.

Safety-class and safety-significant process equipment providing passive confinement (piping, tanks, holding vessels, etc.) must be designed to suitably conservative criteria; redundancy in their design is not required. The redundancy criteria as described in Section 5.1.1.2 of this Guide must be applied to the design of safety-class SSCs that involve active confinement process equipment (pumps, valves, etc.). The redundancy criteria should be considered in the design of safety-significant SSCs that involve active confinement process equipment. See Table 5.3 for the relevant codes.

Table 5.3. Codes for Safety-Significant and Safety-Class Process Equipment.

Process Equipment	Safety Significant	Safety Class
Pressure vessels	ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 or 2	ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 or 2
Tanks (0-15 psig)	API-620; ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 or 2	API-620; ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 or 2
Tanks (containing flammable liquids)	ANSI/API-620; ANSI/API-650; NFPA 30	ANSI/API-620; ANSI/API-650; NFPA 30
Tanks (atmospheric pressure)	ANSI/API-650; AWWA-D100; ANSI/ASME-B96.1	ANSI/API-650; AWWA-D100; ANSI/ASME-B96.1
Pumps	ANSI/API; ANSI/ASME B73.1M, B73.2M; ASME Boiler and Pressure Vessel Code, Section VIII; AWWA; Hydraulic Institute Standards	ANSI/API; ANSI/ASME B73.1M, B73.2M; ASME Boiler and Pressure Vessel Code, Section VIII; AWWA; Hydraulic Institute Standards
Piping	ANSI/ASME B31.3	ANSI/ASME B31.3; ANSI-N278.1
Valves	ANSI/ASME B16.5, B31.3	ANSI/ASME B16.5, B31.3
Heat exchangers	ASHRAE Handbook; ASME Boiler and Pressure Vessel Code, Section VIII, Division 1; TEMA B, C, or R	ASHRAE Handbook; ASME Boiler and Pressure Vessel Code, Section VIII, Division 1; TEMA B, C, or R
Gloveboxes	ANSI/ASTM C852; ANS 11.16	ANSI/ASTM C852; ANS 11.16

5.2.2.3 Mechanical Handling Equipment

Safety-significant and safety-class handling equipment (cranes, manipulators, etc.) will only be classified as such if their failure would create a radiological material release exceeding the guidelines for either classification. The safety-significant classification, as a defense-in-depth provision, will be the more common classification for remote material handling equipment.

Failure modes for mechanical handling equipment used to move radioactive materials must address mid-operational failures, and designs must include recovery methods for such occurrences. Designs must accommodate periodic maintenance and inspection. See Table 5.4 for the relevant codes.

Table 5.4. Codes for Safety-Significant and Safety-Class Handling Equipment.

Handling Equipment	Safety Significant	Safety Class
Cranes	CMAA; ANSI/ASME NOG-1; ANSI/ASME B30.2; DOE-STD-1090-96	CMAA Nuclear Sections; ANSI/ASME NOG-1; ANSI/ASME B30.2; DOE-STD-1090-96
Other equipment	ANSI N 14.6; AISC M011	ANSI N14.6; AISC M011

5.2.3 Electrical

The safety function of an electrical power system is to provide power to systems and components that require electrical power in order to perform their safety functions. A safety-significant or safety-class electrical power system is defined as the system or component that provides actuation or motive force to safety equipment. These systems consist of onsite AC/DC power supply systems and associated distribution systems and components (e.g., conduits, wiring, cable trays, etc.).

Safety-class electrical power must be designed against single-point failure in accordance with the criteria in Section 5.1.1.2 of this Guide. Redundancy requirements for electrical systems pertain to normal and alternative power sources and should be analyzed on a case-by-case basis. For safety-significant systems, redundancy is not required if it can be shown that there is sufficient response time to provide an alternative source of electrical power.

Environmental capability of safety-class electrical equipment must be demonstrated by testing, analysis, and operating experience, or a combination of these methods in accordance with Section 5.1.3 of this Guide.

For the commercial nuclear industry, a multitude of ANSI/IEEE Standards define the requirements for the manufacture, installation, and testing of reactor Safety Class 1E electrical systems and components. The Safety Class 1E requirements may not be directly applicable to the safety-class category defined for nonreactor nuclear facilities. These standards, however, contain useful and significant information that should be considered. Table 5.5 lists a minimal set of national codes and standards that should be addressed for safety-significant and safety-class electrical systems, keeping in perspective the applicable use of ANSI/IEEE standards for Safety Class 1E components. Table 5.6 presents a list of ANSI/IEEE standards that can be used for guidance in specific applications. Before using these standards, their applicability to the design(s) being considered should be reviewed.

Table 5.5. Codes for Safety-Significant and Safety-Class Electrical Systems.

Electrical	Safety Significant	Safety Class
Hardware	NFPA 70; NFPA 110; NFPA 780; IES Lighting Handbook; ANSI C2; ANSI/IEEE C37; ANSI/IEEE -80, -141, -142, -242, -399, -493, -577	NFPA 70; NFPA 110; NFPA 780; IES Lighting Handbook; ANSI C2; ANSI/IEEE C37; ANSI/IEEE-80, -141, -142, -242, -308, -338, -379, -384, -399, -493, -577, -603

Table 5.6. ANSI/IEEE Standards to be Used as Guidance for Both Safety-Significant and Safety-Class Electrical Systems, as Appropriate.

Electrical	Safety Significant and Safety Class
Guidance standards for use as applicable for specific hardware	ANSI/IEE -323, -334, -336, -344, -381, -382, -383, -420, -450, -484, -535, -628, -649, -650, -833, -934, -944, -946

5.2.4 Instrumentation, Control, and Alarm Systems

The safety functions of instrumentation, control, and alarm systems are to provide information on out-of-tolerance conditions/abnormal conditions; ensure the capability for manual or automatic actuation of safety systems and components; ensure safety systems have the means to achieve and maintain a fail-safe shutdown condition on demand under normal or abnormal conditions; and/or actuate alarms to reduce public or site-personnel risk (e.g., effluent monitoring components and systems).

The design of safety-class and safety-significant instrumentation and control systems must incorporate sufficient independence, redundancy, diversity, and separation to ensure that all safety-related functions associated with such equipment can be performed under postulated accident conditions as identified in the safety analysis. Safety-significant components should be evaluated as to the need for redundancy on a case-by-case basis. Under all circumstances, safety-class instrumentation, controls, and alarms must be designed so that failure of nonsafety equipment will not prevent the former from performing their safety functions.

Safety-significant and safety-class instrumentation, control, and alarm-system designs must ensure accessibility for inspection, maintenance, calibration, repair, or replacement.

Safety-class instrumentation, control, and alarm systems must provide the operators sufficient time, information, and control capabilities to perform the following safety functions:

- Readily determine the status of critical facility parameters to ensure compliance with the limits specified in the Technical Safety Requirements.

- Initiate automatic or manual safety functions.

- Determine the status of safety systems required to ensure proper mitigation of the consequences of postulated accident conditions and/or to safely shut down the facility.

ANSI/IEEE standards contain design, installation, and testing requirements that should be considered for instrumentation, control, and alarm components without invoking all of the Safety Class 1E requirements. See Table 5.7 for the relevant codes.

Table 5.7. Codes for Safety-Significant and Safety-Class Instrumentation, Control, and Alarm Components.

Instruments, Controls, and Alarms	Safety Significant	Safety Class
Hardware	NFPA-70, -110; ANSI C2; ANSI/ANS-8.3, -N42.18, -N13.1; ANSI/ISA-Series; ANSI/IEEE-141, -142, -242, -493, -1050	NFPA-70, -110; ANSI C2; ANSI/ANS-8.3, -N42.18, -N13.1; ANSI-N320, -N323; ANSI/ISA-Series; ANSI/IEEE-141, -142, -242, -323, -336, -338, -344, -379, -384, -493, -1050

APPENDIX A

REFERENCES

Code of Federal Regulations

- 10 Code of Federal Regulations (CFR) 50.2, Definitions (1999).
- 10 CFR 830.120, Quality Assurance Requirements (1999).
- 10 CFR 834, Radiation Protection of Public and the Environment (Proposed Rule), Federal Register, 3-25-93.
- 10 CFR 835, Occupational Radiation Protection (1999).
- 29 CFR 1910, Occupational Safety and Health Standards: Subpart G, Occupational Health and Environmental Control; Subpart H, Hazardous Materials; and Subpart Z, Toxic and Hazardous Substances (1994).
- 29 CFR 1910.134, Respiratory Protection (1999).
- 29 CFR 1926, Safety and Health Regulations for Construction (1999).

American Conference of Governmental Industrial Hygienists

- ACGIH 2092-1998. *Industrial Ventilation: A Manual of Recommended Practices*, American Conference of Governmental Industrial Hygienists, Cincinnati, Ohio, 1998.

American National Standards Institute/American Concrete Institute

- ACI-318-99. *Building Code Requirements for Reinforced Concrete with Commentary,* American Concrete Institute, Detroit, Mich., 1999.
- ANSI/ACI 349-85. *Code Requirements for Nuclear Safety Related Concrete Structures (ACI 349-85) and Commentary (ACI 349R-85),* American National Standards Institute, New York, 1985.

American National Standards Institute/American Institute of Steel Construction

- AISC M011-1980. *Manual of Steel Construction Allowable Stress Design*, American Institute of Steel Construction, Chicago, latest edition.

- ANSI/AISC N690-1994. *Specifications for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities,* American National Standards Institute, New York, 1994.

American National Standards Institute/American Nuclear Society

- ANSI C2-1997. *National Electrical Safety Code,* American National Standards Institute, New York, 1997.

- ANSI N14.6-1993. *Radioactive Materials—Special Lifting Devices for Shipping Containers Weighing 10,000 Pounds (4500 kg) or More,* American National Standards Institute, New York, 1993.

- ANSI N43.2-1989. *Radiation Safety for X-ray Diffraction and Fluorescence Analysis Equipment,* American National Standards Institute, New York, 1989.

- ANSI N278.1-1975 (R 1992). *Self-Operated and Power-Operated Safety-Related Valves Functional Specification Standard,* American National Standards Institute, New York, 1992.

- ANSI N320-1979 (R1993). *Performance Specifications for Reactor Emergency Radiological Monitoring Instrumentation,* American National Standards Institute, New York, 1993.

- ANSI N323-1978 (R1993). *Radiation Protection Instrumentation Test and Calibration,* American National Standards Institute, New York.

- ANSI Z9.2-1979 (R 1991). *Fundamentals Governing the Design and Operation of Local Exhaust Systems,* American National Standards Institute, New York, 1991.

- ANSI Z124.2-1995. *Plastic Shower Receptors and Shower Stalls,* American National Standards Institute, New York, 1995.

- ANSI Z358.1-1998. *Emergency Eyewash and Shower Equipment,* American National Standards Institute, New York, 1998.

- ANS 11.16. *Design Guides for Radioactive Material Handling Facilities and Equipment,* American Nuclear Society, La Grange Park, Ill., 1988.

- ANSI/ANS 6.4.2-1985 (R 1997). *Specification for Radiation Shielding Materials,* American Nuclear Society, La Grange Park, Ill., 1997.

- ANSI/ANS 8.3-1997. *Criticality Accident Alarm Systems,* American Nuclear Society, La Grange Park, Ill., 1997.

- ANSI/ANS 59.2-1985. *Safety Criteria for Nuclear Power Plants—HVAC Systems Located Outside Primary Containment,* American National Standards Institute, New York, 1985.

- ANSI/ANS N2.3-1979. *Immediate Evacuation Signal for Use in Industrial Installations,* American Nuclear Society, La Grange Park, Ill., 1979.

- ANSI/ANS N13.1-1969 (R 1999). *Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities,* American National Standards Institute, New York, 1999.

- ANSI/ANS N42.18 (R 1991). *Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents,* American National Standards Institute, New York, 1991.

American National Standards Institute/American Petroleum Institute

- ANSI/API-620-1998. *Rules for Design and Construction of Large, Welded, Low-Pressure Storage Tanks,* American Petroleum Institute, Washington, D.C., 1998.

- ANSI/API-650-1998. *Welded Steel Tanks for Oil Storage,* American Petroleum Institute, Washington, D.C., 1998.

American National Standards Institute/American Society of Mechanical Engineers

- ASME F00230. *Boiler and Pressure Vessel Code,* American Society of Mechanical Engineers, Fairfield, N.J. 1986.

- ANSI/ASME B16.5-1998. *Pipe Flanges and Flanged Fittings (Includes Revision Service),* American Society of Mechanical Engineers, New York, 1998.

- ANSI/ASME B30.2-1996 (R 1998). *Overhead and Gantry Cranes,* American National Standards Institute, New York, 1998.

- ANSI/ASME B31.3-1996. *Process Piping,* American Society of Mechanical Engineers, New York, 1996.

- ANSI/ASME B73.1M-1991 (R 1992). *Horizontal End Suction Centrifugal Pumps for Chemical Process,* American National Standards Institute, New York 1992.

- ANSI/ASME B73.2M-1991. *Specifications for Vertical In-Line Centrifugal Pumps for Chemical Process,* American National Standards Institute, New York, 1991.

- ANSI/ASME B96.1-1993. *Welded Aluminum-Alloy Storage Tanks,* American National Standards Institute, New York, 1993.

- ANSI/ASME N509 (R 1996). *Nuclear Power Plant Air-Cleaning Units and Components,* American Society of Mechanical Engineers, New York, 1996.

- ANSI/ASME N510-1995. *Testing of Nuclear Air-Cleaning Systems,* American Society of Mechanical Engineers, New York, 1995.

- ANSI/ASME NOG-1-1998. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder),* American National Standards Institute, New York, 1998.

American National Standards Institute/American Society for Testing and Materials

- ANSI/ASTM C852-93 (R 1997). *Standard Guide for Design Criteria for Plutonium Gloveboxes,* American Society for Testing and Materials, Philadelphia, PA, 1997.

American National Standards Institute/Institute of Electrical and Electronic Engineers

- ANSI/IEEE C37 series. *Circuit Breakers, Switchgears, Substations, and Fuses,* American National Standards Institute, (standards on switchgear as required) New York, 1998.

- ANSI/IEEE 80-1986 (R 1991). *Safety in AC Substation Grounding,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 141-1993. *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants (Red Book),* American National Standards Institute, New York, 1993.

- ANSI/IEEE 142-1991. *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 242-1986 (R 1991). *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 308-1980 (R 1991). *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 323-1990 (R 1996). *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1996.

- ANSI/IEEE 334-1994. *IEEE Standard for Qualifying Continuous Duty Class 1E Motors for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1994.

- ANSI/IEEE 336-1985 (R 1991). *IEEE Standard for Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 338-1987 (R 1993). *IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems,* American National Standards Institute, New York, 1993.

- ANSI/IEEE 344-1987 (R 1993). *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1993.

- ANSI/IEEE 379-1994. *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,* American National Standards Institute, New York, 1994.

- ANSI/IEEE 382-1985 (R 1996). *IEEE Standard for Qualification of Actuators for Power-Operated Valve Assemblies with Safety-Related Functions for Nuclear Power Plants,* American National Standards Institute, New York, 1996.

- ANSI/IEEE 383-1974 (R 1992). *IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1992.

- ANSI/IEEE 384-1992. *IEEE Standard for Criteria for Independence of Class 1E Equipment and Circuits,* American National Standards Institute, New York, 1992.

- ANSI/IEEE 399-1997. *Recommended Practice for Power Systems Analysis (IEEE Brown Book),* American National Standards Institute, New York, 1997.

- ANSI/IEEE 450-1987 (R 1995). *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications,* American National Standards Institute, New York, 1995.

- ANSI/IEEE 484-1987 (R 1996). *Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications,* American National Standards Institute, New York, 1996.

- ANSI/IEEE 493-1997. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (IEEE Gold Book),* American National Standards Institute, New York, 1997.

- ANSI/IEEE 535-1986 (R 1994). *IEEE Standard for Qualification of Class 1E Lead Storage Batteries for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1994.

- ANSI/IEEE 577-1976 (R 1993). *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1993.

- ANSI/IEEE 603-1998. *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1998.

- ANSI/IEEE 628-1987 (R 1993). *IEEE Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1993.

- ANSI/IEEE 649-1991. *IEEE Standard for Qualifying Class 1E Motor Control Centers for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 650-1991. *IEEE Standard for Qualification of Class 1E Static Battery Chargers and Inverters for Nuclear Power Generating Stations,* American National Standards Institute, New York, 1991.

- ANSI/IEEE 833-1988 (R 1994). *IEEE Recommended Practice for the Protection of Electric Equipment in Nuclear Power Generating Stations from Water Hazards,* American National Standards Institute, New York, 1994.

- ANSI/IEEE 934-1987 (R 1993). *Requirements for Replacement Parts for Class 1E Equipment in Nuclear Power Generating Stations,* American National Standards Institute, New York, 1993.

- ANSI/IEEE 944-1986 (R 1996). *IEEE Recommended Practice for the Application and Testing of Uninterruptible Power Supplies for Power Generating Stations,* American National Standards Institute, New York, 1996.

- ANSI/IEEE 946-1993. *IEEE Recommended Practice for the Design of DC Auxiliary Power Systems for Generating Stations,* American National Standards Institute, New York, 1993.

- ANSI/IEEE 1023-1988 (R 1995). *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations,* American National Standards Institute, New York, 1995.

- ANSI/IEEE 1050-1989 (R 1996). *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations,* American National Standards Institute, New York, 1996.

American Society of Heating, Refrigerating and Air Conditioning Engineers

- ASHRAE Handbook. *Fundamentals* (Inch-Pound Edition), R.A. Parsons, ed., American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc., Atlanta, 1997.

- ASHRAE Standard 52.1-1992. *Gravimetric and Dust-Spot Procedures for Testing Air Cleaning Devices Used in General Ventilation for Removing Particulate Matter,* American Society of Heating, Refrigerating, and Air Conditioning Engineers, Inc., Atlanta, 1992.

- ASHRAE Standard 62-99. *Ventilation for Acceptable Indoor Air Quality (Includes Supplement ANSI/ASHRAE 62A-1991),* American Society of Heating, Refrigerating, and Air Conditioning Engineers, Inc., Atlanta, 1999.

American Water Works Association

- AWWA D100-84. *Welded Steel Tanks for Water Storage,* American Water Works Association, Denver, 1984.

- AWWA D100a-89. *Welded Steel Tanks for Water Storage (Supplement to ANSI/AWWA D100-84),* American Water Works Association, Denver, 1989.

- AWWA D100-96. *Welded Steel Tanks for Water Storage (Includes Supplement to ANSI/AWWA D100a-89),* American Water Works Association, Denver, 1996.

- AWWA standards on pumps as required, American Water Works Association, Denver.

Crane Manufacturers Association of America

- CMAA. Crane Manufacturers Association of America, Charlotte, N.C., standards as required.

Department of Defense

- DoD 6055.9-STD. *DoD Ammunition and Explosives Safety Standards*, Department of Defense, Washington, D.C., 1997.

- DoD Explosives Safety Board Technical Paper No. 13. Department of Defense, Washington, D.C.

- MIL-F-51068F. *Filters, Particulate [High-Efficiency Fire Resistant]*, Department of Defense, Washington, D.C., 8-11-88.

- MIL-STD-1472D. *Human Engineering Design Criteria for Military Systems, Equipment, and Facilities*, Department of Defense, Washington, D.C., 3-14-89.

- TM 5-1300, NAVFAC P-397, AFM 22. *Structures to Resist the Effects of Accidental Explosions*, Departments of the Army, the Navy, and the Air Force, Chairman, Department of Defense Explosives Safety Board, Alexandria, Va.

Department of Energy

- DOE. RELIABILITY, AVAILABILITY, AND MAINTAINABILITY GUIDELINES (Draft), Department of Energy, Washington, D.C., March 1988.

- DOE O 151.1, COMPREHENSIVE EMERGENCY MANAGEMENT SYSTEMS, Department of Energy, Washington, D.C., 8-21-96.

- DOE O 420.1. FACILITY SAFETY, Department of Energy, Washington, D.C., 10-13-95.

- DOE O 430.1A. LIFE CYCLE ASSET MANAGEMENT, Department of Energy, Washington, D.C., 10-14-98.

- DOE O 435.1. RADIOACTIVE WASTE MANAGEMENT, Department of Energy, Washington, D.C., 7-9-99.

- DOE O 440.1A. WORKER PROTECTION MANAGEMENT FOR DOE FEDERAL AND CONTRACTOR EMPLOYEES, Department of Energy, Washington, D.C., 9-30-95.

- DOE G 440.1-5. IMPLEMENTATION GUIDE FOR USE WITH DOE ORDERS 420.1 AND 440.1, FIRE SAFETY PROGRAM, Department of Energy, Washington, D.C., 9-30-95.

- DOE P 450.4, SAFETY MANAGEMENT SYSTEM POLICY, Department of Energy, Washington, D.C., 1-15-96.

- DOE G 450.4-1A, INTEGRATED SAFETY MANAGEMENT SYSTEM GUIDE, Department of Energy, Washington, D.C., 5-27-99.

- DOE 5400.1, GENERAL ENVIRONMENTAL PROTECTION PROGRAM, Department of Energy, Washington, D.C., 6-29-90.

- DOE 5480.21. UNREVIEWED SAFETY QUESTIONS, Department of Energy, Washington, D.C., 12-24-91.

- DOE 5480.23. NUCLEAR SAFETY ANALYSIS REPORTS, Change 1, Department of Energy, Washington, D.C., 3-10-94.

- DOE 5480.30. NUCLEAR REACTOR SAFETY DESIGN CRITERIA, Department of Energy, Washington, D.C., 1-19-93.

- DOE/EH-0256T. *Radiological Control Manual*, Department of Energy, Washington, D.C., April 1994.

- DOE-HDBK-3010-94, *Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*, Department of Energy, Washington, D.C., December 1994.

- DOE-STD-1090-99. *Hoisting and Rigging (Formerly Hoisting and Rigging Manual)*, Department of Energy, Washington, D.C., March 1999.

- DOE M 440.1-1. DOE EXPLOSIVES SAFETY MANUAL, Department of Energy, Washington, D.C., 9-30-95.

- DOE-STD-3020-97. *Specifications for HEPA Filters Used by DOE Contractors,* Department of Energy, Washington, D.C., January 1997.

- DOE-STD-1020-94. *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities,* Department of Energy, Washington, D.C., April 1994.

- DOE-STD-1021-93. *Natural Phenomena Hazards Performance Categorization Guidelines for Structures, Systems, and Components,* Revision 1, Department of Energy, Washington, D.C., July 1993.

- DOE-STD-1022-94. *Natural Phenomena Hazards Characterization Criteria,* Department of Energy, Washington, D.C., March 1994.

- DOE-STD-1023-95. *Natural Phenomena Hazards Assessment Criteria,* Department of Energy, Washington, D.C., September 1995.

- DOE-STD-1024-92. *Guidelines for Use of Probabilistic Seismic Hazard Curves at Department of Energy Sites for Department of Energy Facilities,* Department of Energy, Washington, D.C., December 1992.

- DOE-STD-1027-92. *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports,* Department of Energy, Washington, D.C., December 1992.

- DOE-STD-1066-99. *Fire Protection Design Criteria,* Department of Energy, Washington, D.C., July 1999.

- DOE-STD-1075-94. *Standard for Developing and Issuing DOE Safety Guides and Implementation Guides,* Department of Energy, Washington, D.C., July 1994.

- DOE-STD-3009-94. *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, Department of Energy, Washington, D.C., July 1994.

- DOE/TIC-11268. *A Manual for the Prediction of Blast and Fragment Loading of Structures*, Department of Energy, Washington, D.C., 11-80.

Electronic Industries Association

- EIA/IS-632. *Systems Engineering*, Electronic Industries Association Interim Standard, Washington, D.C., 12-94.

Energy Research and Development Administration

- ERDA 76-21. Burchsted, C.A., *Nuclear Air Cleaning Handbook: Design, Construction, and Testing of High-Efficiency Air-Cleaning Systems for Nuclear Application* (Oak Ridge National Laboratory, Oak Ridge, Tenn.), 2nd ed., Energy Research and Development Administration, Washington, D.C., 1976.

Faust

- Faust, L.G., et al., *Health Physics Manual of Good Practices for Plutonium Facilities*, PNL-6534, Pacific Northwest Laboratories, Richland, Wash., 5-88.

Hydraulic Institute Standards

- Hydraulic Institute Standards, Cleveland, standards as required.

Illuminating Engineering Society

- Rea, M.S. *Lighting Handbook: Reference and Application,* Illuminating Engineering Society of North America, New York, 1993.

International Atomic Energy Agency

- IAEA Safety Series 30. *Manual on the Safety Aspects of the Design and Equipment of Hot Laboratories,* International Atomic Energy Agency, Vienna, 1981.

- IAEA Safety Series 50-P-1. *Application of Single Failure Criterion: Safety Practice,* International Atomic Energy Agency, Vienna, 1990.

Instrument Society of America

- Instrument Society of America, Research Triangle Park, N.C., standards as required.

National Council on Radiation Protection and Measurements

- NCRP Report 49. *Structural Shielding Design and Evaluation for Medical Use of X Rays and Gamma Rays of Energies Up to 10 MeV,* National Council on Radiation Protection and Measurements, Bethesda, Md., 1976.

National Environmental Policy Act

- NEPA, National Environmental Policy Act, Public Law 89-753, 43 U.S.C. 431, et seq.

National Fire Protection Association

- NFPA 30. *Flammable and Combustible Liquids Code,* National Fire Protection Association, Quincy, Mass., 1996.

- NFPA 70. *National Electrical Code,* National Fire Protection Association, Quincy, Mass., 1996.

- NFPA 72. *National Fire Alarm Code,* National Fire Protection Association, Quincy, Mass., 1993.

- NFPA 110. *Emergency and Standby Power Systems,* National Fire Protection Association, Quincy, Mass., 1996.

- ANSI/NFPA 780-1995. *Installation of Lightning Protection Systems (Revision and Redesignation of ANSI/NFPA 780-1989,* National Fire Protection Association, Quincy, Mass., 1995.

Nuclear Regulatory Commission

- NUREG-0700. *Guidelines for Control Room Design Reviews,* Nuclear Regulatory Commission, Washington, D.C., 9-81.

Resource Conservation and Recovery Act

- RCRA, Resource Conservation and Recovery Act of 1976 (41 U.S.C., Sec. 6901, et seq.), as amended.

Sheet Metal and Air Conditioning Contractors National Association

- SMACNA, Sheet Metal and Air Conditioning Contractors National Association, Chantilly, Va., manuals as required.

Tubular Exchanger Manufacturers Association

- TEMA, Tubular Exchanger Manufacturers Association, Inc., Tarrytown, N.Y., standards on heat exchangers Classes B, C, and R.

NOT
MEASUREMENT
SENSITIVE

DOE G 420.1-1A
12-4-2012

NONREACTOR NUCLEAR SAFETY DESIGN GUIDE for use with DOE O 420.1C, *FACILITY SAFETY*

This Guide describes suggested non-mandatory approaches for meeting requirements. Guides are not requirements documents and are not to be construed as requirements in any audit or appraisal for compliance with the parent Policy, Order, Notice, or Manual.

U.S. DEPARTMENT OF ENERGY
Office of Health, Safety and Security

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Health, Safety and Security

FOREWORD

This Guide provides an acceptable approach for safety design of Department of Energy (DOE) hazard category 1, 2 and 3 nuclear facilities for satisfying the requirements of DOE Order 420.1C, *Facility Safety*, Attachment 2, Chapter I, *Nuclear Safety Design Criteria*.

DOE guides are part of the DOE Directives System and are issued to provide supplemental information regarding the Department's requirements as contained in rules, orders, notices, and technical standards. Guides also provide acceptable methods for implementing these requirements.

This Guide may be used by all DOE personnel and contractors, including personnel and contractors for the National Nuclear Security Administration (NNSA). Throughout this document, references to a contractor or a DOE contractor apply to a contractor for NNSA, as well.

This Guide does not establish or invoke any new requirements.

Beneficial comments (recommendations, additions, deletions, and any pertinent data) that may improve this document should be sent to:

HS-31/GTN
U.S. Department of Energy
Washington, D.C. 20585
Phone (301) 903-3331
Facsimile (301) 903-6172

Contents

1. OBJECTIVE

To provide an acceptable approach for safety design of Department of Energy (DOE) hazard category 1, 2 and 3 nuclear facilities satisfying the requirements of DOE Order (O) 420.1C, *Facility Safety*, Attachment 2, Chapter I, *Nuclear Safety Design Criteria*.

2. APPLICABILITY

This Guide (G) has the same applicability as Attachment 2, Chapter I of DOE O 420.1C, i.e.,

(1) new hazard category 1, 2, and 3 nuclear facilities as defined by 10 Code of Federal Regulations (C.F.R.) Part 830, *Nuclear Safety Management*; and,

(2) major modifications to hazard category 1, 2, and 3 nuclear facilities, as defined in 10 C.F.R. Part 830, that could substantially change the approved facility safety basis.

Design criteria related to natural phenomena hazard (NPH) mitigation, fire protection, and criticality safety can affect, or relate to, nuclear safety design criteria. These design requirements are contained in other parts of DOE O 420.1C and are not addressed in this Guide. For example, the use of non-nuclear building design requirements contained in International Building Code (IBC) or other government and non-government standards is not addressed in this Guide.

3. BACKGROUND AND OVERVIEW OF THIS GUIDE

3.1 Background

10 C.F.R. Part 830 establishes the Federal regulations that ensure the essential requirements for the protection of workers, the public, and the environment are systematically executed and maintained, including a requirement for the preparation and approval of a Preliminary Documented Safety Analysis for new nuclear projects. The regulations address requirements for nuclear safety design.

DOE O 420.1C establishes facility safety requirements in five major categories: (i) nuclear safety design criteria; (ii) fire protection; (iii) criticality safety; (iv) NPH mitigation; and, (v) the cognizant system engineer program (note: this topic is not addressed in this Guide). Each chapter in Attachment 2 of the Order provides fundamental and essential requirements, which provide the foundation for safety design. Additionally, Attachment 3 to DOE O 420.1C provides design criteria for safety structures, systems, and components (SSCs) and relevant design codes and standards.

Each chapter's requirements are further addressed in DOE technical standards (STDs) and guides, such as this Guide for nuclear safety design criteria, DOE-STD-1066-2012, *Fire Protection,* for fire protection requirements, and DOE-STD-1020-2012, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities,* for NPH mitigation requirements.

The criteria for nuclear safety design are not limited to Chapter I in Attachment 2 of DOE O 420.1C. DOE O 420.1C has other requirements which are contained in Chapter II (fire protection), Chapter III, (nuclear criticality safety), and Chapter IV (NPH mitigation) that are applicable to the nuclear facility safety design. In addition, DOE O 420.1C and DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, dated 09-29-10, require implementation of DOE-STD-1189-2008, *Integration of Safety into the Design Process*, for the design of new hazard category 1, 2, and 3 nuclear facilities and major modifications of existing facilities. DOE O 413.3B requires a design code of record (COR) for nuclear facilities to be initiated during the conceptual design, placed under configuration control during preliminary design, and maintained throughout its remaining life-cycle. The COR will include the identification of guides and standards used for the design. It is the responsibility of the users to document the bases for their decisions in the selection and implementation of the guides and standards. It is DOE's responsibility to review and approve the safety design bases that result from these decisions.

3.2 Organization

The following two sections of this Guide correspond with the two main requirements sections (3.a and 3.b) of Chapter I of Attachment 2 of DOE O 420.1C. Specifically:

- Section 4 provides guidance on integration of safety with design, and
- Section 5 provides guidance on nuclear facility design.

Appendices A through D of this Guide contain the Confinement Ventilation System Design and Performance Criteria, Definitions, Abbreviations and Acronyms, and References, respectively.

4. GUIDANCE FOR INTEGRATION OF SAFETY WITH DESIGN

Attachment 2, Chapter I of DOE O 420.1C requires integration of safety into the design early and throughout the design process consistent with DOE-STD-1189-2008. DOE-STD-1189-2008 provides detailed criteria and guidance on integrating safety into the design process. Appendices A through D of that standard contain requirements and guidance on the classification of safety functions and the SSCs selected to provide those functions.

10 C.F.R. 830, DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, and DOE-STD-1189-2008 provide criteria and guidance for the performance of a safety analysis to identify the major facility safety functions needed, and to identify safety-class (SC) and safety-significant (SS) SSCs needed to fulfill the safety functions. One of the objectives of the hazard and accident analyses is to identify the complete suite of safety SSCs for a facility and to designate them as SC or SS, as appropriate to their importance and role. Functional and design requirements specifically address the pertinent design parameters related to the safety function that is relied upon. These design requirements should also be included in SSC design documents. Chapter 7 of DOE-STD-1189-2008 provides guidance on important project interfaces relating to safety and design, including associated directives and requirements related to design.

5. GUIDANCE FOR NUCLEAR SAFETY DESIGN

5.1 Multiple Layers of Protection and Defense-in-Depth

Attachment 2, Chapter I of DOE O 420.1C requires that nuclear facility design includes multiple layers of protection (otherwise known as defense-in-depth) in the facility design to prevent or mitigate the unintended release of radioactive materials into the environment. The following is a general discussion followed by a more detailed discussion of each of the defense-in-depth elements.

5.1.1 General Discussion

Defense-in-depth is a fundamental strategy for nuclear facility safety. Defense-in-depth provides layers of defense against the release of hazardous materials so that no one layer by itself is completely relied upon. All safety activities, whether organizational, behavioral or equipment-related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. When properly applied, the defense-in-depth strategy ensures that no single human or mechanical failure would lead to injury to individuals or to the public, or even combinations of failures that are only remotely possible would lead to little or no injury.

The strategy for defense-in-depth is twofold: first, to prevent accidents, and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions. Defense-in-depth is generally structured in five levels, as discussed below. Should one level fail, the next one comes into play.

Level 1 – Prevention of abnormal operation and failures. Accident prevention is the first priority. This is accomplished by conservative design and high quality in construction and operations and maintenance, including conservative site selection. This also includes design to minimize and control inventories of radioactive materials-at-risk. Provisions to prevent deviations of facility state from well-known operating conditions are generally more effective and more predictable than measures aimed at mitigation of such a departure.

Level 2 – Control of abnormal operation and detection of failures. This is accomplished by control, limiting and protection systems, as well as other surveillance features. Both safety systems and administrative controls are used. Multiple, diverse and independent means are provided to control and monitor facility processes.

Level 3 – Control of accidents within the design basis. This is accomplished by engineered safety features that are capable of leading the facility to a safe controlled state. A central component of defense-in-depth is the use of successive, multiple physical barriers for protection against release of radioactivity and hazardous materials. Multiple, diverse and independent means are provided to accomplish safety functions.

Level 4 – Control of severe facility conditions. This includes prevention of accident progression and mitigation of consequences of accidents.

Level 5 – Mitigation of radiological consequences. Significant adverse consequences from significant releases of radioactive materials are mitigated by emergency procedures and emergency response. As required for emergency response, means are provided to monitor accident releases.

At each level, a combination of design features and human aspects is evident. Human aspects of defense-in-depth are brought into play to protect the integrity of the barriers. These include quality assurance (QA), procedures, administrative controls, operating limits, safety reviews, personnel qualification and training, independent oversight, and safety culture. Design provisions (including both those for normal facility systems and those for engineered safety features) help to prevent: undue challenges to the integrity of physical barriers; failure of a barrier if it is jeopardized; and, consequential damage to multiple barriers in series.

The general objective of defense-in-depth is to ensure that a single failure (whether equipment failure or human failure) at one level of defense, or even combinations of failures at more than one level of defense, would not propagate to jeopardize defense-in-depth at subsequent levels. The independence of different levels of defense is a key element in meeting this objective. Special attention should be paid to hazards that could potentially impair several levels of defense, such as fire, earthquakes, and flooding.

5.1.2 Appropriate Site Selection

Attachment 2, Chapter I of DOE O 420.1C requires designers to choose an appropriate site location. The following factors should be considered in determining facility site suitability, as well as when establishing facility safety designs criteria:

- the site boundary and land-use characteristics of the site surroundings, including properties at risk from accidental exposures, public exclusion zones (access control), population-center distances, and population density;

- physical characteristics of the site, including topography, meteorology, and hydrology;

- geological and subsurface elements, such as the potential for fault rupture and the severity of vibratory ground motions from earthquakes, soil bearing design capacity, rock or other bearing stratum, ground settlement, and groundwater elevations;

- NPHs as discussed in Attachment 2, Chapter IV of DOE O 420.1C, including earthquakes, volcanic ejection, wind, flood, snow, hail, precipitation, and lightning;

- utility systems essential to support SC SSCs, such as electrical power supply and water supply;

- proximity of services, such as the fire department and emergency medical centers;

- emergency response considerations, including population sheltering or shielding parameters and evacuation delay times and rates for the public and co-located workers;

- potential human-induced hazards from nearby facilities or activities, such as industrial and military facilities (including other DOE facilities), aircraft impacts, pipelines, and transportation routes;

- proximity of nearby facilities and the hazards both to and from the proposed facility; and,

- site-related assumptions of the related environmental impact statement.

5.1.3 Minimization of Material-at-risk

The basic and most effective means of controlling the hazards inherent in the facility is the restriction of inventories and forms of radioactive and/or hazardous materials. Attachment 2, Chapter I of DOE O 420.1C requires emphasis to be placed on limiting the quantity and form of radioactive and/or hazardous materials in both process and storage areas consistent with mission needs. Materials may be rendered less hazardous by maintaining them in more stabilized and less dispersible forms.

5.1.4 Conservative Design Margins

The application of conservative design margins is required in Attachment 2, Chapter I of DOE O 420.1C. Conservative design provides a margin between the anticipated operating and accident conditions (covering normal operation as well as postulated incidents and accidents) and the failure conditions of the equipment. SSCs that provide a layer of protection are conservatively designed using established codes and standards that embody design margins. Appropriate conservative assumptions and safety margins are applied for SSC design, including design calculations, design analyses, and identification of design basis. The design of SSCs should incorporate suitably conservative criteria from applicable industry standards and design codes, and applicable DOE directives and technical standards. Where codes and standards are not complete, they should be supplemented with appropriate conservative design criteria. Where applications are unique or first-of-a-kind, additional efforts, such as testing or increased safety margins, should be taken to demonstrate conservatism of design. This should apply to all facets of the design including safety and non-safety SSCs.

Further, the facility design should accommodate means, such as monitors and automatic and manual controls, to restrict deviations from normal operations and to assist recovery during the early stages of an accident sequence.

5.1.5 Quality Assurance

The application of QA is required in Attachment 2, Chapter I of DOE O 420.1C. QA practices and requirements should be applied to the design and construction of SSCs at a level commensurate with the safety function of the SSC, including, but not limited to, the assurance of qualified design and construction personnel, the traceability of design decisions and procurements, and the documentation of changes in design and construction. Refer to section 7.1 of DOE-STD-1189-2008 for more specific guidance in implementing QA during the design process.

10 C.F.R. 830, Subpart A, *Quality Assurance Requirements*, requires designers to develop and implement a QA program that meets the requirements contained therein. These requirements are further refined in DOE O 414.1D, *Quality Assurance*, dated 04-25-11, which requires the use of American Society of Mechanical Engineers (ASME) NQA-1-2008 with the NQA-1a-2009 addenda (or a later edition*), Quality Assurance Requirements for Nuclear Facility Applications*, Part I and applicable requirements of Part II for select facilities. It is important to identify and implement the specific, applicable QA requirements and processes implemented early in the design process for nuclear facilities. Designers should work with their QA organizations to ensure these processes address and implement the applicable NQA-1 requirements.

The procurement of components will in most cases be 'off-the-shelf' and should follow the procurement process specified in the quality assurance program. For facilities that are required to meet the requirements of NQA-1, this should include the Commercial Grade Dedication (CGD) process requirements specified in NQA-1. A CGD process takes time to develop and implement; therefore, at the earliest possible stage, design personnel should establish a qualified CGD process if it will be used for the project.

Once the safety SSCs and their performance requirements are identified, a more detailed set of QA requirements can be specified. As part of the safety analysis, a list of all SC SSCs should be prepared and maintained for the life of the project through decommissioning. This listing should identify the safety functions, performance requirements, NPH design requirements, and QA requirements for each SC SSC. Many of the detailed component-specific requirements for safety SSCs are identified in applicable consensus codes and standards. A similar listing of all SS SSCs should also be prepared, including a discussion of any defense-in-depth role of the SS SSC. As the design progresses, more detailed safety analyses will be performed to develop the basis for safety SSCs performance requirements, and QA requirements can be refined as necessary. QA requirements should also be applied to non-safety SSCs commensurate with importance to facility operational requirements.

The design activity should implement a configuration management process consistent with the requirements of DOE O 420.1C and DOE O 413.3B where applicable, including design, change, document, and work control. Subsequent changes to project design and supporting documents should be made by means of a formal change control program in accordance with the requirements of NQA-1, where applicable, as well as the approved configuration management program.

5.1.6 Multiple Physical Barriers

Attachment 2, Chapter I of DOE O 420.1C requires the design to include multiple physical barriers to confine radioactive and other hazardous materials and, thereby, prevent uncontrolled releases. Physical barriers can include hazardous materials containers, gloveboxes, passive facility structural elements, and confinement ventilation systems (CVS). Confinement systems are discussed in more detail in Section 5.3 of this Guide.

5.1.7 Multiple Means to Achieve Safety Functions

Attachment 2, Chapter I of DOE O 420.1C requires that the design provide multiple means to ensure safety functions are met. These means consist of (1) controlling the process; (2) shutting down the process in a safe shutdown state, if the process control is challenged; (3) using preventive and mitigative safety features, if the safe shutdown is challenged; and, (4) monitoring the post-accident condition, if necessary.

5.1.7.1 Preventive Features

To prevent abnormal facility conditions from progressing to accidents, preventive features should be considered in the design. The objective of these features is to provide a return to normal operation or to a safe condition. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such responses to off-normal conditions should effectively halt and reverse the progression of events toward an accident. If these features are engineering controls (i.e., SSCs) they may need to be designated as SC or SS, as determined by the safety analysis.

5.1.7.2 Mitigating Features

Safety SSCs should be provided to mitigate consequences of accidents that may occur despite the application of the preceding conventions.

5.1.8 Equipment and Administrative Controls

Attachment 2, Chapter I of DOE O 420.1C requires the design to provide features to: control process variables to values within safe conditions; alert operating personnel of an approach toward conservative process limits; and, allow timely detection of failure or malfunction of critical equipment.

DOE-STD-1186-2004, *Specific Administrative Controls*, provides guidance on the selection and design of administrative controls. Where specific administrative controls are determined to be necessary, the design should provide adequate time for the operating personnel to take action.

5.1.9 Accident Release Monitoring

Attachment 2, Chapter I of DOE O 420.1C requires that provisions for monitoring during and after accident releases be included in the design as required for emergency response. DOE O 151.1C, *Comprehensive Emergency Management Systems,* dated 11-02-05, provides additional design feature for accident monitoring requirements.

5.1.10 Emergency Planning

Attachment 2, Chapter I of DOE O 420.1C requires that emergency plans be established for minimizing the effects of an accident. DOE O 151.1C provides detailed requirements for emergency planning. See Section 5.4.8 of this Guide and Section 7.12 of DOE-STD-1189-2008 for additional guidance.

5.2 Hierarchy of Controls

DOE-STD-1189-2008 provides a control selection strategy that addresses hazardous material release events, based on the following order of preference at all stages of design development:

- minimization of hazardous materials is the first priority;
- safety-SSCs are preferred over administrative controls;
- passive SSCs are preferred over active SSCs;
- preventive controls are preferred over mitigative controls;
- facility safety SSCs are preferred over personal protective equipment (PPE).

In addition, the following should be considered during design development:

- controls closest to the hazard are preferred since they may provide protection to the largest population of potential receptors, including workers and the public; and,
- controls that are effective for multiple hazards are preferred since they can be resource effective.

5.3 Radioactive Material Confinement

Attachment 2, Chapter I of DOE O 420.1C requires hazard category 1, 2, and 3 nuclear facilities with uncontained radioactive materials (as opposed to materials determined by safety analyses to be adequately contained within qualified drums, grout, or vitrified materials) to have the means to confine the uncontained radioactive materials to minimize their potential release in facility effluents during normal operations, as well as, during, and following accidents up to and including design basis accidents (DBAs).

Further, DOE O 420.1C requires confinement design to include the following:

- For a specific nuclear facility, the number, arrangement, and characteristics of confinement barriers, as determined on a case-by-case basis;
- The type, quantity, form, and conditions for dispersing the radioactive materials in the confinement system design; and,
- An active CVS as the preferred design approach for nuclear facilities with potential for radiological release.

CVSs are among the most important mitigating systems for protecting the public and co-located workers, and are generally relied upon as the final safety barrier to the release of hazardous materials.

Active confinement ventilation systems are the preferred alternative for nuclear facilities with potential for radiological release. They provide a positive means for ensuring the control of radioactive materials for operational and design basis events.

Alternate confinement approaches may be acceptable if a technical evaluation demonstrates that the alternate confinement approach results in very high assurance of confinement of the radioactive materials. The technical justification should address how the passive facility confinement design results in very high assurance of the confinement of radioactive materials when compared with active systems for all operational activities and DBAs. This technical justification should also include the consideration of conservative evaluations of accident conditions, including energy sources associated with the accident and post-accident recovery, building integrity, and building re-entry activities (see DNFSB/TECH 34, *Confinement of Radioactive Materials at Defense Nuclear Facilities,* for additional discussion). Furthermore, the evaluation should demonstrate how post-accident monitoring and off-site dose measurements will be performed to support potential worker and public evacuation.

When an active confinement ventilation strategy is selected as a means of confining radioactive materials, designers should use Appendix A, *Confinement Ventilation Systems Design and Performance Criteria,* of this Guide.

5.4 Other General Design Considerations and Practices

5.4.1 Design to Facilitate Deactivation, Decontamination, and Decommissioning

Attachment 2, Chapter I of DOE O 420.1C requires the design to include considerations related to deactivation, decontamination, and decommissioning requirements.

5.4.1.1 Deactivation

Deactivation is the process of removing hazardous materials and neutralizing hazardous conditions at the end of a facility's life or mission prior to decontamination and decommissioning. A design to facilitate deactivation should incorporate facility features that aid in: the removal of surplus radioactive and chemical materials; storage tank cleanout and maintenance; stabilization of contamination and process materials; and, the removal of hazardous, mixed, and radioactive wastes. In general, these features should reduce the physical risks and hazards associated with facility decontamination and decommissioning and would also be called for when designing for ease of maintenance during operation.

5.4.1.2 Decontamination

The facility design should incorporate measures to simplify decontamination of areas that may become contaminated with radioactive or hazardous materials. Items such as service piping, conduits, and ductwork should be kept to a minimum in potential contamination areas and should be arranged to facilitate decontamination. Walls, ceilings, and floors in areas vulnerable to contamination should be finished with washable or strippable coverings. Metal liners should be used in areas that have the potential to become highly contaminated. Cracks, crevices, and joints should be filled and finished smooth to prevent accumulation of contaminated materials. The

facility design should incorporate features that will facilitate decontamination to achieve facility decommissioning, to increase the potential for other uses, or both.

5.4.1.3 Decommissioning

Design features consistent with the requirements of DOE O 435.1, Chg 1, *Radioactive Waste Management*, dated 07-09-99, should be developed during the planning and design phases, based on decommissioning requirements or a conversion method leading to other facility uses. The following design principles should be considered:

- Use of localized liquid-transfer systems with emphasis on localized batch solidification of liquid waste to avoid long runs of buried contaminated piping. Special provisions should be included in the design to ensure the integrity of joints in buried pipelines;
- Location of exhaust filtration components of the ventilation systems at, or near, individual enclosures to minimize long runs of internally contaminated ductwork;
- Equipment, including effluent decontamination equipment that precludes, to the extent practicable, the accumulation of radioactive or other hazardous materials in relatively inaccessible areas, including curves and turns in piping and ductwork;
- Accessible, removable covers for inspection and cleanouts are encouraged;
- Use of modular radiation shielding in lieu of, or in addition to, monolithic shielding walls;
- Provisions for flushing and/or cleaning contaminated, or potentially contaminated, piping systems;
- Provisions for suitable clearances, where practical, to accommodate equipment removal and access for remote handling and safety surveillance equipment planned for use in future decontamination and decommissioning;
- Use of lifting lugs on large tanks and equipment; and,
- Piping systems that carry contaminated, or potentially contaminated, liquid should be free draining via gravity.

5.4.2 Design to Facilitate Inspection, Testing, and Maintenance

Attachment 2, Chapter I of DOE O 420.1C requires that facilities be designed to facilitate inspection, testing, maintenance, and repair and replacement of safety SSCs to ensure their continued function, readiness for operation, and accuracy. The facility design should include provisions for accessibility and maintainability that include, but are not limited to, the following:

- Surveillance equipment should be located and sufficient space provided for relative ease of routine testing and maintenance activities;

- Accessible inspection covers to allow for visual inspection should be provided and located such that necessary routine inspections can be conducted with minimum disruption to the facility or equipment operation, for example, flow test ports in ducting;

- The facility design should include features that provide for ease of routine maintenance without a subsequent mission reduction. Examples include providing sufficient clearance around equipment to accommodate the change out of large components and providing permanent ladder(s) and platform(s) to access lubrication and equipment areas;

- The facility design should consider the choice of manufacturer or software producer regarding future maintainability and availability of spare parts;

- The facility design should include provisions for integrated testing at the system level to verify safety functions; and,

- The facility design should use a reliability, maintainability and availability program to achieve operational needs for the design life of the desired end product, expected normal and worst-case operating conditions, and expected downtime for either corrective or preventive maintenance actions.

5.4.3 Design for Radiation Protection and Contamination Control

Attachment 2, Chapter I of DOE O 420.1C requires the design to include considerations related to radiation protection and contamination control requirements. 10 C.F.R. Part 835, *Occupational Radiation Protection,* also provides requirements for radiological protection.

The primary objective of radiological protection is to minimize external and internal personnel exposures to radioactive materials. This objective is accomplished through multiple features and measures, such as: providing adequate radiation posting, sampling, monitoring, and notification or alarm capabilities; applying as low as reasonably achievable (ALARA) principles; incorporating facility and system radiation protection features into the designs; and, through other measures. Typical radiation protection design features should include: shielding; remote handling; area and equipment layout to prevent radiation streaming; passive confinement structures and containers; active confinement ventilation negative pressure cascades; and, exhaust high-efficiency particulate air (HEPA) filtration, supplemented by cautionary systems. ALARA principles to minimize personnel exposures should be applied to all equipment and facility designs. The following are design considerations that support meeting these objectives:

- The type and level of hazards should be determined for each functional area, the attendant degree of risk identified, and the possibility of cross-contamination considered. Wherever possible, work areas with compatible contaminants should be

located together to simplify design criteria related to air supply and exhaust, waste disposal, decontamination, and cross-contamination;

- Radioactive and other hazardous materials contamination control requirements should be considered together in the design to minimize the potential for contamination spread from either source;

- Office areas should be located in separate common-use facilities (e.g., data computation and processing, word processing, etc.) and away from process areas, if practicable, to minimize risks to workers from radioactive and/or hazardous materials;

- The building layout should provide protection from the hazards associated with handling, processing, and storing of radioactive and/or hazardous materials. In addition, the following items should be considered in the facility safety design:

    - Additional space should be provided for temporary or additional shielding in the event radiation levels are higher than anticipated;

    - The arrangement and location of hazardous process equipment and its maintenance provisions should provide appropriate protective and safety measures as applicable;

    - The building design should accommodate prompt return to a safe condition in emergencies, and should allow ready access for, and protection of, workers in areas where manual corrective actions are necessary, as well as in areas that contain radiation monitoring equipment readouts.

    - Facility layout should provide specific control and isolation, if possible, of quantities of flammable, toxic, and explosive gases, chemicals, and other hazardous materials admitted to the facility; and,

    - For some facilities, integration of security considerations with radiation protection considerations can be important in building layout and structural design.

Specific criteria for radiation monitoring and entry and exit control systems, posting and labeling of radioactive materials and spaces, nuclear accident dosimetry, and ALARA applications should be applied as required by 10 C.F.R. Part 835.

Physical layout and details of proven radiological equipment designs for plutonium facilities are contained in DOE-STD-1128-2008, *Guide of Good Practices for Occupational Radiological Protection in Plutonium Facilities.*

10 C.F.R. Part 835 requires that the projected dose rates are based on occupancy, duration, and frequency of exposure. If dose projections exceed values specified in 10 C.F.R. Part 835, shielding should be used for areas that need to be accessed normally or intermittently, such as

those for preventive maintenance, component changes, or adjustment of systems and equipment. The type of shielding should be determined by the characteristics of the radiation, structural requirements, fire protection requirements, and radiation damage potential. Shielding should also be installed to minimize non-penetrating external radiation exposures to the skin and lens of the eye, where necessary. In most cases, confinement barriers or process equipment provide this function. Where shielding is an integral part of the facility structure, it should be designed and installed to at least the same level of natural phenomenon qualification as the facility structure. Additional guidance is contained in American National Standards Institute/American Nuclear Society (ANSI/ANS) 6.4.2-2006, *Specification for Radiation Shielding Materials*.

Occupied operating areas for normal operating conditions should be designed not to exceed the airborne concentration limits of 10 C.F.R. Part 835. Respirators should not be needed under normal operating conditions except as a precautionary measure. Engineered controls and features should be designed with consideration of contaminant chemical forms to minimize potential inhalation of radioactive materials and to minimize potential chemical degradation of such engineered features.

Devices to monitor individual exposures to external radiation and to warn personnel of radioactive contamination are to be used in accordance with 10 C.F.R. Part 835. Air sampling equipment should be placed in strategic locations to detect and evaluate airborne contaminant conditions at work locations. Continuous air monitors with preset alarms should be provided to give early warning of significant releases of radioactive materials. Air monitoring and warning systems are to be used in compliance with the requirements of 10 C.F.R. Part 835.

Breathing-air supply systems, if needed, are to comply with the requirements of the Occupational Safety and Health Administration's (OSHA) 29 C.F.R. Part 1910, *Occupational Safety and Health Standards*, Section 134, *Respiratory Protection.*

DOE-STD-1098-2008, *Radiological Control*, provides details on radioactive material identification, storage, and transport. In addition, DOE-STD-1098-2008 provides descriptions and details of use-proven principles and designs and identifies considerations that affect configuration, hardware selection, installation, maintenance, and controls that can be used in developing a sound functional design.

- Shielding should be designed to limit the total external dose during normal operations to the annual exposure limit values as specified in 10 C.F.R. Part 835. Design of facilities and shields applicable to machines and sources is summarized as good practices in applicable National Council on Radiation Protection reports. Additional guidance is contained in ANSI N43.2, *Radiation Safety for X-ray Diffraction and Fluorescence Analysis Equipment*.

- Guidance on ventilation design is provided in the American Conference of Governmental Industrial Hygienists (ACGIH) 2096 *Industrial Ventilation: A Manual of Recommended Practice for Design, 27th Edition* and DOE Handbook (HDBK)-1169-2003, *Nuclear Air Cleaning Handbook*. Alarms for loss of ventilation or differential pressure should be provided on primary confinement systems (gloveboxes or hoods) and secondary confinement systems (rooms). ASME

AG-1, *Code on Nuclear Air and Gas Treatment*, contains requirements for the design of nuclear facility air cleaning systems and acceptance requirements for testing air cleaning systems.

- Change rooms for changing into and out of protective clothing should be designed to ensure that clean clothing (personal clothing) and contaminated clothing (protective clothing) are segregated. The design objective is to ensure that storage of contaminated protective clothing will control contamination so that it does not spread beyond the storage container. The change room exhaust air should be HEPA-filtered, as applicable, if dispersible radionuclides are handled in the process areas it serves.

- Personnel decontamination facilities should be located close to areas that are potential sources of contamination. Safety showers may be used if water collection from their use is controlled. Portable personnel decontamination equipment should be considered for facilities with no permanent structures.

- Respiratory protection should be provided to maintenance personnel in areas where the potential for significant exposures exist for maintenance operations and where design constraints preclude the ability to perform maintenance either remotely or in a glovebox. However, every reasonable effort should be made to allow routine maintenance activities to be conducted without the need for respiratory protection.

5.4.4 Design for Access Control

While not controlled by DOE O 420.1C requirements, the design should include considerations related to access control requirements.

The facility design should accommodate the requirements for: safeguards and security; access by emergency responders under normal and accident conditions; emergency egress; and, area access control for worker protection. Where these requirements conflict, life safety should take precedence. For example, safeguards and security requirements would minimize the number of entrances and exits, but for worker safety, the emergency-egress requirements would provide an adequate number of exits. Specific requirements for access control are to be implemented as specified by 10 C.F.R. Part 835 for radiological hazards, by the Resource Conservation and Recovery Act for hazardous waste treatment, storage, and disposal facilities, and by OSHA's 29 C.F.R. Part 1910, Occupational Safety and Health Standards and Part 1926, Safety and Health Regulations for Construction, for hazardous material locations within operating facilities and construction sites.

Whereas access control is provided for control rooms that contain SC and SS SSC controls and monitoring, the same level of qualification is to be considered for access control features. Access controls are to be designed and implemented so as not to prevent operator actions that would be necessary to achieve and maintain a facility in a safe condition.

5.4.5 Design for Non-Radioactive, Hazardous Material Protection

This section provides functional design guidance for hazardous material protection other than radioactive material protection. DOE-STD-1189-2008 (as invoked by DOE O 420.1C and DOE O 413.3B) requires that the hazard analysis identifies any potential for hazardous material release accidents that cause or exacerbate a nuclear accident. This potential is to be considered in the accident analysis and the selection of safety SSCs. In addition, Attachment 2, Chapter I of DOE O 420.1C requires that nuclear facilities be designed to protect against chemical hazards and toxicological hazards consistent with DOE-STD-1189-2008. Appendix B of DOE-STD-1189-2008 provides additional guidance for protection against chemical hazards and toxicological hazards.

Requirements for design of engineered controls for hazardous material protection are contained in the IBC, 10 C.F.R. Part 851, *Worker Safety and Health Program*, and 29 C.F.R. Part 1910, Subparts G, H, and Z.

Ventilation systems are engineering controls commonly used to prevent worker exposure to hazardous materials and may be used in combination with personal protective equipment and operational procedures. Where ventilation is used to control worker exposures, 29 C.F.R. Part1910, Subpart G 1910.94, *Ventilation*, requires that it is adequate to reduce the hazardous materials concentrations of air contaminants to the degree that the hazardous materials no longer poses a health risk to the worker (i.e., concentrations at, or below, the permissible exposure limits). Wherever engineering controls are not sufficient to reduce exposures to such levels, 29 C.F.R. Part 1910, Subpart Z, 1910.1000, *Air Contaminants*, requires that they be used to reduce exposures to the lowest practicable level and be supplemented by work practice controls. The design should ensure that respirators are not needed for normal operating conditions or routine maintenance activities except as a precautionary measure.

Ventilation systems for hazardous material protection should use exhaust hoods to control concentrations of hazardous materials from discrete sources, or should control the number of air changes per hour for an entire room or bay. Air flow and other design requirements for specific types of systems are required to comply with 29 C.F.R. Part 1910, Subparts G and H. 29 C.F.R. Part 1910, Subpart Z, provides requirements for monitoring and alarm systems for facilities that manage or use specific hazardous materials. Additional guidance on design of ventilation systems for hazardous material protection is provided in ANSI/American Industrial Hygiene Association (AIHA) Z9.2-2012, *Fundamentals Governing the Design and Operation of Local Exhaust Ventilation Systems* and the American Society of Heating, Refrigeration and Air Conditioning (ASHRAE) 62.1-2010, *Ventilation for Acceptable Indoor Air Quality*. Decontamination facilities, safety showers, and eyewashes to mitigate external exposures to hazardous materials are required where mandated by 29 C.F.R. Part 1910, Subparts H and Z. These systems should be designed in accordance with the requirements of ANSI Z358.1-2009, *American National Standard for Emergency Eyewash and Shower Equipment.*

Facilities with hazardous material exposure concerns should be designed to minimize personnel exposures, both external and internal, and to provide adequate monitoring and notification capabilities to inform workers of unsafe conditions. Hazardous material protection should be provided through facility design (e.g., remote handling, area and equipment layout, spill-control

features, confinement, ventilation, specific code requirements for hazardous materials, etc.). Occupied spaces should be designed to preclude locations where low oxygen content or air displacement may occur or where reactive, combustible, flammable, or explosive gas, vapor, or liquid accumulation might occur.

Safety controls and features should be designed to consider contaminant chemical forms and minimize the potential for inhalation and contact under all conditions. Directed ventilation flow paths should be used to move contaminants away from worker breathing zones. The design should ensure that ventilation flow will cascade from clean areas to contaminated areas to preclude contamination spread. Uniform distribution of incoming air and/or air mixing equipment should be provided to ensure that no pockets of stagnant air exist in areas where workers are present. Air flow arrangements that are designed to ensure that air flow from the cleanest area to contaminated areas should be evaluated to ensure that the ventilation arrangement will not inhibit/compromise exiting under fire conditions.

DOE G 440.1-1B, *Worker Safety and Health Program for DOE (Including the National Nuclear Security Administration) Federal and Contractor Employees*, dated 10-20-2011, provides additional information on hazardous material protection vis-à-vis 10 C.F.R. Part 851 compliance.

5.4.6 Design for Effluent Monitoring and Control

This section applies to any DOE facility that produces airborne or liquid radioactive and/or hazardous material effluents, including contaminated storm water. Attachment 2, Chapter I of DOE O 420.1C provides high level requirements for managing uncontained radioactive materials. DOE O 435.1 and DOE Manual (M) 435.1-1, *Radioactive Waste Management Manual*, dated 07-09-99, provide requirements and guidance to ensure a radioactive release is managed in a manner that is protective of worker and public health and safety, and the environment.

Liquid process wastes containing radioactive and/or hazardous materials should be collected and monitored near the source of generation before a batch transfer via appropriate pipelines or portable tanks to a liquid-waste treatment facility. Waste storage tanks and transfer lines should be designed and constructed such that any leakage could be detected, contained, and collected for removal, before it reaches the environment. Double-walled transfer pipelines or multiple encasements should be used for high-level radioactive liquid wastes and other liquid wastes that have the potential to cause significant localized consequences, or significant exposures during the implementation of mitigating measures in the event of an accidental release. Provisions should be made for the collection, removal, and appropriate disposition of infiltration into the annulus of double-walled pipelines. Radioactive- and hazardous-waste collection, transfer, and storage systems should be designed to avoid the dilution of radioactive or hazardous waste due to waste of lower concentrations of radioactivity, toxicity, or other hazard. Airborne effluents from areas in which hazardous or radioactive materials are managed, are exhausted through a ventilation system designed to remove particulate materials, vapors, and gases. Such a system should comply with applicable release requirements (e.g. state or local limits) and should reduce releases of radioactive materials to ALARA levels. The design of airborne-effluent systems should preclude holdup of particulate materials in off-gas and ventilation ductwork and include provisions to continuously monitor the buildup of materials and material recovery. The design of

systems should also preclude the accumulation of potentially flammable quantities of gases generated by radiolysis or chemical reactions within process equipment.

The design capacity for effluent monitoring and control systems should be consistent with the needs for handling process effluents during normal operations, anticipated operational occurrences, and DBA conditions. Alarms should be provided that will annunciate in the event concentrations of radioactive or hazardous materials above specified limits are detected in the effluent stream. Appropriate manual or automatic protective features should be provided to prevent an uncontrolled release of radioactive and/or hazardous materials into the environment or the workplace. Portions of effluent management systems and components that are necessary to control, or limit, the release of radioactive or hazardous materials into the environment, or for safe operation of the system, should be provided with redundancy where required by applicable Federal, state, and local environmental regulations and permits. Effluent monitoring and control systems are designed to allow periodic maintenance, inspection, and testing of components and to maintain ALARA occupational radiation doses during these operations. Appropriate nuclear criticality safety provisions should be applied to the design of airborne effluent systems. This includes a design that precludes the holdup or collection of materials capable of sustaining a chain reaction in portions of the system not geometrically favorable. This also includes a design to ease in-situ measurement and recovery of these materials.

Effluent monitoring and control SSCs are generally designed to operate in conjunction with physical barriers to form a confinement system to limit the release of radioactive or other hazardous materials into the environment and to prevent or minimize the spread of contamination within the facility.

Adequate instrumentation and controls (I&C) should be provided to assess system performance and to allow the necessary control of system operations. Equipment in safety systems is required to be appropriately qualified or protected to ensure reliable operation during normal operating conditions; during anticipated operational occurrences, and during and following DBAs, including a design basis earthquake. SC air filtration units, effluent transport systems, or effluent collection systems are to be designed to remain functional throughout DBAs and to retain collected radioactive and hazardous materials after the accident, as required by DOE O 420.1C.

5.4.7 Design for Waste Management

This section applies to any DOE facility that, under normal operating conditions produces wastes having constituents that are regulated as radioactive, hazardous, or mixed-waste. DOE O 435.1, and the Federal, state, and local requirements referenced therein, specify the criteria for the design of waste management systems. Waste management and storage systems, along with associated support systems, should be designed to remain functional following a DBA and should facilitate the maintenance of a safe shutdown condition and post-accident recovery activities. For high-level waste containment systems, at least one confinement barrier should be designed to withstand the effects of DBAs.

DOE M 435.1-1, *Radioactive Waste Management Manual*, dated 06-06-2011, addresses waste minimization.

5.4.8 Design for Emergency Preparedness and Emergency Communications

Attachment 2, Chapter I of DOE O 420.1C requires establishing emergency plans for minimizing the effects of an accident. Provisions for emergency preparedness are contained in the requirements of DOE O 151.1C, which address installation of an emergency operations center. Primary and backup means of communications with the emergency operations center, provisions for evacuation and accountability, as well as adequate equipment and supplies for emergency response personnel to carry out their respective duties and responsibilities related to nonreactor nuclear facility, are to be provided in the facility design in accordance with DOE O 151.1C requirements.

Emergency evacuation annunciation systems and general communication systems should be installed per the applicable National Fire Protection Association codes listed in DOE-STD-1066-2012. Installation requirements for transmission of alarm conditions to building occupants should be considered public mode systems and address topics such as: protection of circuits; minimum audibility requirements above background noise; voice intelligibility; and, visual signals, including minimum light intensities.

For facilities handling dispersible materials, meteorological data necessary to predict consequences from an emergency event should be obtained from the following sources in order of preference: (1) site specific information; (2) the nearest U.S. Geological Survey; (3) local (on-site) meteorological stations; (4) National Oceanic and Atmospheric Administration.

5.4.9 Human Factors Engineering

Appropriate human factors engineering principles and criteria should be integrated into the design, operation, and maintenance of DOE facilities. The human factor elements that should be considered include, but are not limited to, the following: equipment labeling; workplace environment (temperature and humidity, lighting, noise, vibration, and aesthetics); human dimensions; operating panels and controls; component arrangement; warning and annunciator systems; and, communication systems. The applicable criteria found in the following standards should be considered in the design of these elements: Nuclear Regulatory Guide (NUREG) 0700, *Human-System Interface Design Review Guidelines*; MIL-STD-1472F, *Department of Defense Design Criteria Standard: Human Engineering*; and Institute of Electrical and Electronics Engineers (IEEE) Std. 1023-2004, *IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and other Nuclear Facilities*. DOE-STD-1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities* also provides additional guidance for human factors engineering.

5.4.10 Design of Support Systems and System Interfaces

Safety SSCs often rely upon other SSCs to support their operation. Therefore, it is important to identify these supporting systems and the associated interfaces between safety and non-safety SSCs. The following subsections address the design considerations for these related systems.

5.4.10.1 Support Systems

In some cases, safety-SSCs rely upon supporting SSCs to perform their intended safety function. Attachment 3 of DOE O 420.1C requires that support SSCs be designed as SC or SS SSCs if their failures prevent safety-SSCs or specific administrative controls from performing their safety functions. For example, a SC designation may be appropriate for an I&C system that supports a tritium containment system if failure of the I&C support system could lead to either failure or reduced availability of the SC containment barrier. However, if the support system would not lead to immediate failure of the safety-SSC, such as for a heat tracer on a fire protection line, combined with a safety alarm, providing adequate time for restoration action, the support system may not need to be classified as a safety-SSC. The classification of the supporting SSCs would be at same level as the safety-SSCs or specific administrative controls that they could impact.

5.4.10.2 Interface Design

A nuclear safety design goal is to minimize interfaces between SC, SS, and non-safety SSCs. Interfaces, such as pressure retention boundaries, integrity of fluid systems, electrical equipment, I&C, and mechanical and support systems, exist between safety SSCs and non-safety SSCs. These interfaces should be evaluated to identify SSC failures that would prevent the safety SSCs from performing their intended safety function. For these SSC failures, isolation devices, interface barriers, or design class upgrades should be provided to ensure safety SSC protection and availability. In many cases, systems may consist of a group of subsystems, where each subsystem supports the operation of the whole system. For example, an auxiliary power diesel generator system may consist of lubricating oil, fuel oil, diesel engine, jacket cooling, and room ventilation subsystems. System interface evaluations should clearly define these boundaries. In all instances, a case-by-case evaluation should be performed.

5.4.10.3 System Interaction

DOE-STD-1020-2012 provides guidance and requirements on system interaction including potential interaction of non-safety SSCs and safety-SSCs.

5.4.11 Design of Mechanical Handling Equipment

Mechanical handling equipment (cranes, manipulators, etc.) should only be classified as SC or SS if their failure would create a hazardous material release exceeding the guidelines for either classification (see DOE-STD-1189-2008, Appendix C). The SS classification, as a defense-in-depth provision, will be the more common classification for remote material handling equipment.

Failure modes for mechanical handling equipment used to move radioactive materials should address mid-operational failures, and designs should include recovery methods.

Designs should accommodate periodic maintenance and inspection.

5.4.12 Design of Ventilation Systems

In general, the safety function of ventilation and off-gas systems is to provide confinement integrity and to filter exhaust, thereby preventing or mitigating uncontrolled releases of radioactive and/or hazardous materials into the environment. Ventilation and off-gas systems are included as a vital part of the primary and secondary confinement design. The need for redundancy should be determined by the safety analysis process and maintenance concerns for both active and passive components. Designs should provide for periodic maintenance, inspection, and testing of components. Adequate shielding should be included in the design of filters, absorbers, scrubbers, and other air treatment components to ensure that occupational exposure limits are not exceeded during maintenance and inspection activities.

SC and SS ventilation system designs should include adequate instrumentation to monitor and assess performance with necessary alarms for annunciation of abnormal or unacceptable operation. Manual or automatic protective control features should be provided to prevent or mitigate an uncontrolled release of radioactive and/or hazardous materials into the environment and to minimize the spread of contamination within the facility.

Vent streams potentially containing significant concentrations of radioactive and/or hazardous materials should be processed through an off-gas cleanup system before being exhausted into the environment. Cleanup systems are to remove particulates and noxious chemicals and control the release of gaseous radionuclides. The design of SC and SS off-gas systems should be commensurate with the sources and characteristics of the radioactive and chemical components of the off-gas air stream to prevent or mitigate the uncontrolled releases of radioactive and/or hazardous materials into the environment.

Appendix A of this Guide provides additional design and performance criteria for SC and SS ventilation systems[1].

5.4.13 Environmental Qualifications

Attachment 3 of DOE O 420.1C requires the design to use the IEEE STD 323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, or other applicable standards, to ensure that safety-class SSCs can perform all safety functions, as determined by the safety analysis, with no failure mechanism that could lead to common cause failures under postulated service conditions (e.g., temperature, humidity, radiation). For equipment located in a mild environment, and which has no significant aging mechanisms, a qualified life is not required by IEEE STD 323.

For safety-significant SSCs that are located in a mild environment, the SSCs should be selected for application to the specific service conditions based on sound engineering practices and manufacturers' recommendations. Safety-significant SSCs located in a harsh environment,

---

[1] Appendix A was derived from guidance developed by the Department for review of confinement ventilation systems as part of the Department's implementation plan in response to Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2004-2, *Active Confinement Systems*.

however, should be evaluated for qualified life using manufacturers' recommendations or other appropriate methods.

System documentation should be maintained preserving the relationship between equipment application and service conditions.

5.4.14 Design of Electrical Systems

The safety function of an electrical power system is to provide power to systems and components that require electrical power in order to perform their safety functions, and such power systems should be classified as SC or SS accordingly. These systems consist of on-site AC/DC power supply systems and associated distribution systems and components (e.g., conduits, wiring, cable trays, etc.).

Attachment 3 of DOE O 420.1C requires that the single failure criterion, requirements, and design analysis identified in IEEE 379-2000, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Stations Safety Systems*, be applied to SC electrical systems and components. Redundancy requirements for electrical systems pertain to normal and alternative power sources and should be analyzed on a case-by-case basis. For SS systems, redundancy may not be needed if it can be shown that there is sufficient response time to provide a readily available and defined alternative source of electrical power.

For the commercial nuclear industry, a multitude of ANSI/IEEE standards define the requirements for the design, manufacturing, installation, and testing of reactor Safety Class 1E electrical systems and components. The Safety Class 1E requirements may not be directly applicable to the SC category defined for nonreactor nuclear facilities. These standards, however, contain useful and significant information that should be considered. Attachment 3 of DOE O 420.1C lists a set of national codes and standards to be used for SC and SS electrical systems, keeping in perspective the applicable use of ANSI/IEEE standards for Safety Class 1E components.

Environmental capability of SC and SS electrical equipment in harsh environments should be demonstrated using the guidance stated in Section 5.4.13 of this Guide.

5.4.15 Design of Instrumentation, Controls, and Alarm Systems

The safety functions of instrumentation, control, and alarm systems are to: provide information on out-of-tolerance conditions/abnormal conditions; ensure the capability for manual or automatic actuation of safety systems and components; ensure safety systems have the means to achieve and maintain a fail-safe shutdown condition on demand under normal or abnormal conditions; and/or, actuate alarms to reduce public or site-personnel risk (e.g., effluent monitoring components and systems).

Attachment 3 of DOE O 420.1C requires the design of SC I&C systems to incorporate sufficient independence, redundancy, diversity, and separation to ensure that all safety-related functions associated with such equipment can be performed as defined in the safety analysis. DOE O 420.1C also requires SS I&C components to be evaluated as to the need for

redundancy on a case-by-case basis. DOE-STD-1195-2011 provides an acceptable method for achieving high reliability of SS safety instrumented systems.

DOE O 420.1C requires SC and SS instrumentation, controls, and alarms to be designed so that failure of non-safety equipment will not prevent the former from performing their safety functions.

DOE O 420.1C requires SC and SS instrumentation, control, and alarm-systems to be designed to ensure accessibility for inspection, maintenance, calibration, repair, or replacement.

SC and SS instrumentation, control, and alarm systems should provide the operators sufficient time, information, and control capabilities to perform the following safety functions:

- Readily determine the status of critical facility parameters to ensure compliance with the limits specified in the technical safety requirements;
- Initiate manual safety functions (e.g., take the necessary actions credited in the DSA); and,
- Determine the status of safety systems required to ensure proper mitigation of the consequences of postulated accident conditions and/or to safely shut down the facility.

ANSI/IEEE and ANSI/ISA standards contain design, installation, and testing requirements that should be considered for instrumentation, control, and alarm components without invoking all of the Safety Class 1E requirements.

5.4.16 Equivalencies for Codes and Standards

The facility design authority (as defined in DOE O 413.3B) is required to select and use an appropriate set of codes and standards to establish the COR and the design criteria, which provide assurance that the SSCs will reliably perform their intended functions. DOE technical standards and industry codes and standards are considered applicable when they provide relevant design requirements for the safety SSCs that are being designed. Applicable DOE technical standards and industry codes and standards contain requirements that are appropriate for the design materials, configuration, and service conditions; and provide design requirements that ensure that the desired SSC functions are achieved. In cases where the facility design uses alternative codes and standards to those identified in Attachment 3 of DOE O 420.1C, an approved equivalency is required by Attachment 1 of DOE O 420.1C. In such cases, the alternative codes and standards would be included in the COR.

Justification of equivalent codes and standards should demonstrate that the proposed design of the SSCs meets, or exceeds, the level of safety (e.g., meets, or exceeds, the level of protection) provided by the normally applied codes and standards. Evaluation of the level of safety should address:

- Critical safety attributes of the SSCs;
- Critical characteristics of the SSCs that are important to design, material, and performance of the SSCs;
- The reliability of safety SSCs; and,
- The margins of safety to failure of the SSCs (e.g., pressure, temperature, environmental conditions, and other design loads) provided by application of the code.

For individual components, equivalency should be demonstrated by defining and verifying that the substitute component meets or exceeds these characteristics. Equivalencies should be well documented with a technical basis and should receive peer review by a technically capable and experienced designer.

APPENDIX A: CONFINEMENT VENTILATION SYSTEMS DESIGN AND PERFORMANCE CRITERIA

The following table presents the design and performance criteria that should be used in the design and construction of new active confinement ventilation systems (CVSs) based on the safety classification of the system. Note: This table presents a summary of key design attributes; see DOE Handbook (HDBK) 1169-2003, *Nuclear Air Cleaning Handbook* for more complete design guidance.

Table A-1. Confinement Ventilation System Design and Performance Criteria

DESIGN/ PERFORMANCE	SAFETY CLASS	SAFETY SIGNIFICANT	DEFENSE-IN-DEPTH/OTHER	DISCUSSION	REFERENCE
Ventilation System – General Criteria					
Pressure differential should be maintained between zones and atmosphere	Applies	Applies	Applies	Number of zones as credited by accident analysis to control hazardous material release; demonstrate by use considering potential in-leakage	DOE-HDBK-1169 (2.2.9); ASHRAE Design Guide
Materials of construction should be appropriate for normal, abnormal and accident conditions	Applies	Applies	Applies		DOE-HDBK-1169 (2.2.5); ASME AG-1
Exhaust system should withstand anticipated normal, abnormal and accident system conditions and maintain confinement integrity	Applies	Applies	Applies	As required to prevent accident release	DOE-HDBK-1169-2003 (2.4); ASHRAE Design Guide
CVSs will have appropriate filtration to minimize release	Applies	Applies	Applies	Address: 1) type of filter (e.g., HEPA, sand, sintered metal); 2) filter sizing (flow capacity and pressure drop); 3) decontamination factor vs. accident analysis assumptions	DOE-HDBK-1169-2003 (2.2.1); ASME AG-1

Ventilation System – Instrumentation and Control					
Provide system status instrumentation and/or alarms	Applies	Applies	Applies	Address key information to ensure system operability (e.g., system delta-P, filter pressure drop)	DOE-HDBK-1169-2003; ASME AG-1: ASHRAE Design Guide (Section 4)
Interlock supply and exhaust fans to prevent positive pressure differential	Applies	Applies	Applies		DOE-HDBK-1169-2003; ASHRAE Design Guide (Section 4)
Post-accident indication of filter break-through	Applies	Applies	Does Not Apply	Instrumentation supports post-accident planning and response; should be considered critical instrumentation for SC	DNFSB/TECH-34
Reliability of control system to maintain confinement function under normal, abnormal and accident conditions	Applies	Applies	Applies	Address, for example, impacts of potential common mode failures from events that would require active confinement function	DOE-HDBK-1169-2003 (2.4)
Control components should fail safe	Applies	Applies	Applies		DOE-HDBK-1169-2003 (2.4)
Resistance to Internal Events – Fire					
CVSs should withstand credible fire events and be available to operate and maintain confinement	Applies	Applies	Does Not Apply	Required for new facilities; as required for existing facilities (discretionary). Address protection of filter media.	DOE-HDBK-1169-2003 (10.1); DOE-STD-1066-2012
CVSs should not propagate spread of fire	Applies	Applies	Applies	Required for new facilities; as required for existing facilities (discretionary). Address fire barriers, fire dampers arrangement	DOE-HDBK-1169-2003 (10.1); DOE-STD-1066-2012

Resistance to External Events - Natural Phenomena - Seismic					
CVSs should safely withstand earthquakes	Applies	Applies	Does Not Apply	If the active CVS system is not credited in a seismic accident condition there is no need to evaluate that performance and/or design attribute for the CVS (discretionary). Also, any seismic impact on the CVS performance will be based on the current functional requirements in the documented safety analysis (DSA). NOTE: Seismic requirements may apply to defense-in-depth items indirectly for the protection of safety SSCs.	DOE O 420.1C; DOE-HDBK-1169-2003 (9.2); ASME AG-1
Resistance to External Events - Natural Phenomena – Tornado/Wind					
CVS should safely withstand tornado depressurization	Applies	Applies	Does Not Apply	If the active CVS is not credited in a tornado condition there is no need to evaluate that performance and/or design attribute for the CVS (discretionary). Also, any tornado impact on the CVS performance will be based on the current functional requirements in the DSA.	DOE O 420.1C; DOE-HDBK-1169-2003 (9.2)
CVS should withstand design wind effects on system performance	Applies	Applies	Does Not Apply	If the active CVS is not credited in a wind condition there is no need to evaluate that performance and/or design attribute for the CVS (discretionary). Also, any wind impact on the CVS performance will be based on the current natural phenomena analysis in the DSA.	DOE O 420.1C; DOE-HDBK-1169-2003 (9.2)

Other Natural Phenomena Events (e.g., flooding, precipitation)					
CVS should withstand other natural phenomena events considered credible in the DSA where the CVS is credited	Applies	Applies	Does Not Apply	If the active CVS is not credited for this event there is no need to evaluate that performance and/or design attribute for the CVS (discretionary). Also, any wind impact on the CVS performance will be based on the current NP analysis in the DSA.	DOE O 420.1C; DOE-HDBK-1169-2003 (9.2)
Range Fires/Dust Storms					
Administrative controls should be established to protect CVSs from barrier threatening events	Applies	Applies	Does Not Apply	Ensure appropriately thought out response to external threat is defined (e.g., pre-fire plan)	DOE O 420.1C

Testability					
Design supports the periodic inspection & testing of filters and housing, and tests and inspections are conducted periodically	Applies	Applies	Applies	Ability to test for leakage per intent of N510	DOE-HDBK-1169-2003 (2.3.8); ASME AG-1; ASME N510
Instrumentation required to support system operability is calibrated	Applies	Applies	Applies	Credited instrumentation should have specified calibration/surveillance requirements. Non-safety instrumentation should be calibrated as necessary to support system functionality.	DOE-HDBK-1169-2003 (2.3.8)
Integrated system performance testing is specified and performed	Applies	Applies	Does Not Apply	Required responses assumed in the accident analysis are periodically confirmed including any time constraints	DOE-HDBK-1169-2003 (2.3.8)
Maintenance					
Filter service life program should be established	Applies	Applies	Applies	Filter life (shelf life, service life, total life) expectancy should be determined. Consider filter environment, maximum delta-P, radiological loading, age, and potential chemical exposure.	DOE-STD-1169-2003 (3.1 & APP C)

Single Failure					
Failure of one component (equipment or control) will not affect continuous operation	Applies	Does Not Apply	Does Not Apply	Address potential failures (example failures - fan, backup power supply, switchgear)	DOE O 420.1C, Attachment 2, Chapter I
Automatic backup electrical power will be provided to all critical instruments and equipment required to operate and monitor the CVS	Applies	Does Not Apply	Does Not Apply		DOE-HDBK-1169-2003 (2.2.7)
Backup electrical power will be provided to all critical instruments and equipment required to operate and monitor the CVS	Does Not Apply	Applies	Does Not Apply	NOTE: Safety class is addressed through previous line.	DOE-HDBK-1169-2003 (2.2.7)
Other Credited Functional Requirements					
Address any specific functional requirements for the CVS (beyond the scope of those above) credited in the DSA	Applies	Applies	Does Not Apply		10 C.F.R. 830, Subpart B

APPENDIX B: DEFINITIONS

NOTE: Origins of the definitions are indicated by references shown in brackets [ ] although in some cases the referenced orders are being replaced. If no reference is listed, the definition originates in this Guide and is unique to its application. Terms used within this Guide that are not defined in this Appendix carry their definition from the referenced documents.

Accident. An unplanned sequence of events that results in undesirable consequences. [DOE-STD-3009-94]

Accident Analysis. Accident analysis has historically consisted of the formal development of numerical estimates of the expected consequence and probability of potential accidents associated with a facility. Accident analysis is a follow-on effort to the hazard analysis, not a fundamentally new examination requiring extensive original work. As such, it requires documentation of the basis for assignment to a given likelihood of occurrence range in hazard analysis and performance of a formally documented consequence analysis. Consequences are compared with the Evaluation Guideline to identify safety-class structures, systems, and components. [DOE-STD-3009-94]

Confinement Barriers.

- Primary confinement. Provides confinement of hazardous material to the vicinity of its processing. This confinement is typically provided by piping, tanks, gloveboxes, encapsulating material, and the like, along with any off-gas systems that control effluent from within the primary confinement.

- Secondary confinement. Consists of a cell or enclosure surrounding the process material or equipment along with any associated ventilation exhaust systems from the enclosed area.

- Tertiary confinement. Typically provided by walls, floor, roof, and associated ventilation exhaust systems of the facility. It provides a final barrier against the release of hazardous materials into the environment.

Construction. Any combination of engineering, procurement, erection, installation, assembly, or fabrication activities involved in creating a new facility or altering, adding to, or rehabilitating an existing facility. It also includes the alteration and repair (including dredging, excavating, and painting) of buildings, structures, or other real property.

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 C.F.R. Part 830 Subpart B, Appendix A]

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 C.F.R. Part 830 Subpart B, Appendix A]

Design Basis. Information that identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or range of values chosen for controlling parameters as reference bounds of design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analyses (based on calculations and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals. [10 C.F.R. Part 50.2]

Effluent Monitoring. The collection and analysis of samples or measurements of liquid and gaseous effluents for the purpose of: characterizing and quantifying contaminants; assessing radiation exposures of members of the public; providing a means to control effluents at, or near, the point of discharge; and, demonstrating compliance with applicable standards and permit requirements.

Evaluation Guideline. Radiation dose value against which the safety analysis evaluates. Off-site evaluation guidelines are established for the purpose of identifying and evaluating safety-class structures, systems, and components.

Explosives Facility. A structure or defined area used for explosives storage or operations. Excluded are explosives presenting only localized, minimal hazards as determined by the Authority Having Jurisdiction. Examples of excluded items may include user quantities of small arms ammunition, commercial distress signals, or cartridges for cartridge actuated tools, etc. [DOE-STD-1212-2012]

Facility. For the purpose of this Guide, the definition most often refers to buildings and other structures, their functional systems and equipment, and other fixed systems and equipment installed therein to delineate a facility. However, specific operations and processes independent of buildings or other structures (e.g., waste retrieval and processing, waste burial, remediation, groundwater or soil decontamination, decommissioning) are also encompassed by this definition. The flexibility in the definition does not extend to subdivision of physically concurrent operations having potential energy sources that can seriously affect one another or which use common systems fundamental to the operation (e.g., a common glovebox ventilation exhaust header). [DOE-STD-3009-94]

Fail-Safe. A design characteristic by which a unit or system will become safe, and remain safe, if a system or component fails or loses its activation energy.

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

Hazard Analysis. The determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by the assessment of hazardous situations associated with a process or activity. Largely qualitative techniques are used to pinpoint weaknesses in design or operation of the facility that could lead to accidents. The hazard analysis examines the complete spectrum of potential accidents that could expose members of the public,

on-site workers, facility workers, and the environment to hazardous materials. [DOE-STD-3009-94]

Hazard Categorization. Evaluation of the consequences of unmitigated releases to classify facilities or operations into the following hazard categories: [10 C.F.R. Part 830, Subpart B, Appendix A]

- *Hazard Category 1: Has the potential for significant off-site consequences.*
- *Hazard Category 2: Has the potential for significant on-site consequences.*
- *Hazard Category 3: Has the potential for only significant localized consequences.*

DOE-STD-1027-92 provides guidance and radiological threshold values for determining the hazard category of a facility. DOE-STD-1027-92, Chg 1, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, interprets Hazard Category 1 facilities as Category A reactors and other facilities designated as such by the Program Secretarial Officer. [DOE-STD-3009-94]

Hazardous Material. Any solid, liquid, or gaseous material that is radioactive, toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health.

Major Modification. A modification to a DOE nuclear facility that substantially changes the existing safety basis for the facility. [10 C.F.R. Part 830.3]

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 C.F.R. Part 830.3]

Public. All individuals outside the DOE site boundary. [DOE-STD-3009-94]

Safety Analysis. A documented process: (1) to provide systematic identification of hazards within a given DOE operation; (2) to describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and, (3) to analyze and evaluate potential accidents and their associated risks. [DOE-STD-3009-94]

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 C.F.R. Part 830.3]

Safety-class SSCs. *Safety-class structures, systems, and components* means the 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 C.F.R. Part 830.3]

Safety-significant SSCs. *Safety-significant structures, systems, and components* means the structures, systems, and components which are not designated as safety-class structures, systems, and components, but whose preventive or mitigative function is a major contributor to defense-in-depth and/or worker safety as determined from safety analyses. [10 C.F.R. Part 830.3]

Safety SSCs. Safety-class and safety-significant SSCs.

Single-failure Criterion. Safety-class systems are able to perform all required safety functions for a design basis accident (DBA) in the presence of the following:

- Any single detectable failure within the safety-class systems concurrent with all identifiable but undetectable failures.
- All failures caused by the single failure.
- All failures and spurious system actions that cause, or are caused by, the DBA requiring the safety-class system function.

The single failure could occur prior to, or at any time during, the DBA for which the safety system is required to function. [ANSI/IEEE Standard 379-2000]

Site Boundary. A well-marked boundary within which the owner and operator can exercise control without the aid of outside authorities. A public road or waterway traversing a DOE site is considered to be within the DOE site boundary if, when necessary DOE or the site contractor has the capability to control the road during accident or emergency conditions. [DOE-STD-3009-94].

APPENDIX C: ABBREVIATIONS AND ACRONYMS

ACGIH	American Conference of Governmental Industrial Hygienists
ACI	American Concrete Institute
AGS	American Glovebox Society
AIHA	American Industrial Hygiene Association
AISC	American Institute of Steel Construction
ALARA	as low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
API	American Petroleum Institute
ASHRAE	American Society of Heating, Refrigeration, and Air-Conditioning
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
AWWA	American Water Works Association
C.F.R.	Code of Federal Regulations
CGD	Commercial Grade Dedication
CMAA	Crane Manufacturers Association of America
COR	Code of Record
CVS	Confinement Ventilation System
DBA	design basis accident
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DSA	Documented Safety Analysis
G	Guide (DOE directive)
HEPA	high-efficiency particulate air (filter)
I&C	instrumentation and control
IBC	International Building Code
IEEE	Institute of Electrical and Electronics Engineers
ISA	International Society of Automation
M	Manual
NCRP	National Council on Radiation Protection
NFPA	National Fire Protection Association
NNSA	National Nuclear Security Administration
NPH	Natural Phenomena Hazard
NUREG	Nuclear Regulatory Guide
O	Order (DOE directive)
QA	quality assurance
RCRA	Resource Conservation and Recovery Act
SC	safety-class
SS	safety-significant
SSC	structures, systems, and components
STD	Standard (DOE directive)

APPENDIX D: REFERENCES

Note: The following is a list of references referenced in this Guide and/or DOE O 420.1C, *Facility Safety.*

Public Law

- P.L. 106-65, *National Defense Authorization Act for Fiscal Year 2000, Title XXXII,* National Nuclear Security Administration, as amended.
- P.L. 94-580, *Resource Conservation and Recovery Act of 1976 (RCRA),* 41 U.S.C., Sec. 6901, et seq.), as amended.
- P.L. 83-703, *Atomic Energy Act of 1954.*

Executive Orders (E.O.) and Federal Policies

- E.O. 12344*, Naval Nuclear Propulsion Program.*
- *Federal Wildland Fire Management Policy and Implementing Actions*. (Available from National Interagency Fire Center)
- *Secretarial Delegation Order Number 00-033.00B*, dated 07-20-09.

Code of Federal Regulations (C.F.R.)

- 10 C.F.R. Part 830*, Nuclear Safety Management.*
- 10 C.F.R. Part 830*,* Section 830.120*, Quality Assurance Requirements.*
- 10 C.F.R. Part 835, *Occupational Radiation Protection.*
- 10 C.F.R. Part 851, *Worker Safety and Health Program.*
- 29 C.F.R. Part 1910*, Occupational Safety and Health Standards.*
- 29 C.F.R. Part 1910, Subpart G, Section 1919.94, *Occupational Health and Environmental Control.*
- 29 C.F.R. Part 1910, Subpart H, Section 1910.101, *Hazardous Materials.*
- 29 C.F.R. Part 1910, Subpart Z, Section 1910.100, *Toxic and Hazardous Substances.*
- 29 C.F.R. Part 1910, Section 1910.134*, Respiratory Protection.*
- 29 C.F.R. Part 1926*, Safety and Health Regulations for Construction.*

- 48 C.F.R. Part 970, Section 970.5223-1, *Integration of Environment, Safety, and Health into Work Planning and Execution.*

American Conference of Governmental Industrial Hygienists (ACGIH)

- ACGIH 2096, *Industrial Ventilation: A Manual of Recommended Practices for Design*, January 2010.

American Glovebox Society

- AGS-G006-2005, *Standard of Practice for the Design and Fabrication of Nuclear Application Gloveboxes*, 2005.

American Concrete Institute (ANSI/ACI)

- ACI-318-11, *Building Code Requirements for Structural Concrete and Commentary*, 2011.

- *ANSI/ACI 349-06, Code Requirements for Nuclear Safety-Related Concrete Structures (ACI 349-06) and Commentary, 2006.*

American National Standards Institute/American Institute of Steel Construction (AISC)

- AISC 325:2011, *Steel Construction Manual*, 2011.

- AISC 360:2010, *Specification for Structural Steel Buildings*, 2010.

- AISC N690:2006, *Specification for Safety-Related Steel Structures for Nuclear Facilities*, 2006.

American National Standards Institute (ANSI)

- ANSI N13.1-2011, *Guide to Sampling and Monitoring Releases of Airborne Radioactive Substances from the Stacks and Ducts of Nuclear Facilities*, 2011.

- ANSI N14.6, *Special Lifting Devices for Shipping Containers Weighing 10,000 Pounds (4500 kg) or More*, 1993.

- ANSI N43.2,-2001 (R2010), *Radiation Safety for X-ray Diffraction and Fluorescence Analysis Equipment*, 2001.

- ANSI N278.1-1975 (R1992), *Self-Operated and Power-Operated Safety-Related Valves Functional Specification Standard*, 1975.

- ANSI N323D-2002, *American National Standard for Installed Radiation Protection Instrumentation*, 2003.

- ANSI/AIHA Z9.2-2012, *Fundamentals Governing the Design and Operation of Local Exhaust Ventilation Systems,* 2012.

- ANSI Z358.1-2009, *American National Standard for Emergency Eyewash and Shower Equipment,* 2009.

- ANSI/ANS-1-2000 (R2007), *Conduct of Critical Experiments,* 2000.

- ANSI/ANS-6.4.2-2006, *Specification for Radiation Shielding Materials,* 2006.

- ANSI/ANS 8 series standards.

- ANSI/ANS-8.3-1997 (R2003), *Criticality Accident Alarm System,* 2003.

- ANSI/ ANS-14.1-2004 (R2009), *Operation of Fast Pulse Reactors,* 2004.

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

- ANSI/ANS 58.9-2002 (R 2009), *Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems,* 2009.

- ANSI/ANS-59.3-1992 (R2002), *Nuclear Safety Criteria for Control Air Systems,* 1992.

American Petroleum Institute (API)

- API-Std 620, *Design and Construction of Large, Welded, Low-Pressure Storage Tanks,* 2008.

- API-Std 650, *Welded Tanks for Oil Storage,* 2007.

American Society of Mechanical Engineers (ASME)

- ASME AG-1-2009, *Code on Nuclear Air and Gas Treatment,* 2009.

- ASME BPVC, *ASME 2013 Boiler and Pressure Vessel Code,* 2013.

- ASME B16.5-2009, *Pipe Flanges and Flanged Fittings: NPS ½ through NPS 24 Metric/Inch Standard,* 2009.

- ASME B30.2-2005, *Overhead and Gantry Cranes (Top Running Bridge, Single or Multiple Girder, Top Running Trolley Hoist),* 2005.

- ASME B31.3-2012, *Process Piping,* 2012.

- ASME B73.1-2001 (R2007), *Specifications for Horizontal End Suction Centrifugal Pumps for Chemical Process,* 2002.

- ASME B73.2-2003 (R2009), *Specification for Vertical In-Line Centrifugal Pumps for Chemical Process,* 2005.

- ASME NOG-1-2010. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder),* 2010.

- ASME NUM-1-2009, *Rules for Construction of Cranes, Monorails, and Hoists (with Bridge or Trolley or Hoist of the Underhung Type),* 2010.

- ASME NQA 1-2008 with 2009 Addenda, *Quality Assurance Requirements for Nuclear Facility Applications, Part I and applicable requirements of Part II,* 2009.

American Society for Testing and Materials (ASTM)

- ASTM C852-09, *Standard Guide for Design Criteria for Plutonium Gloveboxes,* 2009.

- ASTM C1455-07, *Standard Test Method for Nondestructive Assay of Special Nuclear Material Holdup Using Gamma-Ray Spectroscopic Methods,* 2007.

American National Standards Institute/International Society of Automation (ISA)

- ANSI/ISA 7.0.01-1996, *Quality Standard for Instrument Air,* 1996.

- ANSI/ISA 18.1-1979 (R2004*), Annunciator Sequences and Specifications,* 1979.

- ANSI/ISA 67.01.01-2002 (R2007), *Transducer and Transmitter Installation for Nuclear Safety Applications,* 2002.

- ANSI/ISA S67.02.01-1999, *Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants,* 1999.

- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements (ISA 84.00.01),* 2004.

- ANSI/ISA 67.04.01-2006 (R2011), *Setpoints for Nuclear Safety-Related Instrumentation,* 2006.

American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE)

- ASHRAE Handbook, Fundamentals (Inch-Pound Edition), 2009.

- ASHRAE Standard 62.1-2010, *Ventilation for Acceptable Indoor Air Quality,* 2010.

American Water Works Association (AWWA)

- AWWA D100-11, *Welded Carbon Steel Tanks for Water Storage,* 2011.

Crane Manufacturers Association of America (CMAA)

- CMAA Crane Manufacturers Association of America, standards as applicable.

Department of Defense

- MIL-STD-1472F, *Department of Defense Design Criteria Standard: Human Engineering,* August 1999.

Department of Energy (DOE)

- DOE P 420.1, *Department of Energy Nuclear Safety Policy,* Department of Energy, Washington, D.C., dated 2-8-2011.

- DOE O 151.1C, *Comprehensive Emergency Management Systems,* Department of Energy, Washington, D.C., dated 11-2-2005.

- DOE O 226.1B, *Implementation of Department of Energy Oversight Policy,* Department of Energy, Washington, D.C., dated 4-25-2011.

- DOE O 227.1, *Independent Oversight Program,* Department of Energy, Washington, D.C., dated 8-30-2011.

- DOE O 251.1C, *Departmental Directives Program*, Department of Energy, Washington, D.C., dated 1-15-2009.

- DOE O 410.1, *Central Technical Authority Responsibilities Regarding Nuclear Safety Requirements,* Department of Energy, Washington, D.C., dated 6-28-2007.

- DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets,* Department of Energy, Washington, D.C., dated 11-29- 2010.

- DOE O 414.1D, *Quality Assurance,* Department of Energy, Washington, D.C., dated 4-25-2011.

- DOE O 420.1C. *Facility Safety*, Department of Energy, Washington, D.C., dated 12-4-2012.

- DOE O 420.2C, *Safety of Accelerator Facilities*, Department of Energy, Washington, D.C., dated 7-21-2011.

- DOE O 426.1 Chg 1, *Federal Technical Capability*, Department of Energy, Washington, D.C., dated 11-20-2011.

- DOE O 426.2, *Personnel Selection, Training, Qualification, and Certification Requirements for DOE Nuclear Facilities,* Department of Energy, Washington, D.C., dated 4-21-2010.

- DOE O 433.1B, *Maintenance Management Program for DOE Nuclear Facilities,* Department of Energy, Washington, D.C., dated 4-21-2010.

- DOE O 435.1, Chg 1, *Radioactive Waste Management,* Department of Energy, Washington, D.C., dated 7-9-1999.

- DOE O 452.1D, *Nuclear Explosive and Weapon Surety Program,* Department of Energy, Washington, D.C., dated 4-14-2009.

- DOE O 452.2D, *Nuclear Explosive Safety,* Department of Energy, Washington, D.C., dated 4-14-2009.

- DOE O 5480.30, Chg 1, *Nuclear Reactor Safety Design Criteria,* Department of Energy, Washington, D.C., dated 4-19-1993.

- DOE M 435.1-1, Chg 2, *Radioactive Waste Management Manual,* Department of Energy, Washington, D.C., dated 7-9-1999.

- DOE G 414.1-2B Chg 1, *Quality Assurance Program Guide,* Department of Energy, Washington, D.C., dated 8-16-2011.

- DOE G 440.1-1B, *Worker Safety and Health Program for DOE (Including the National Nuclear Security Administration) Federal and Contractor Employees,* Department of Energy, Washington, D.C., dated 11-20-2011.

- DOE-STD-1020-2012, *Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities,* Department of Energy, Washington, D.C., 2012.

- DOE-STD-1027-1992, Chg 1, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports,* Department of Energy, Washington, D.C., 1997.

- DOE-STD-1066-2012, *Fire Protection Design Criteria,* Department of Energy, Washington, D.C., 2012.

- DOE-STD-1073-2003, *Configuration Management Program,* Department of Energy, Washington, D.C., 2003.

- DOE-STD-1090-2011, *Hoisting and Rigging (Formerly Hoisting and Rigging Manual),* Department of Energy, Washington, D.C., 2011.

- DOE-STD-1098-2008, *Radiological Control,* Department of Energy, Washington, D.C., 2008.

- DOE-STD-1128-2008, *Guide of Good Practices for Occupational Radiological Protection in Plutonium Facilities,* Department of Energy, Washington, D.C., 2008.

- DOE-STD-1134-1999, *Review Guide for Criticality Safety Evaluations,* Department of Energy, Washington, D.C., 1999.

- DOE-STD-1158-2010, *Self-Assessment Standard for DOE Contractor Criticality Safety Programs,* Department of Energy, Washington, D.C., 2010.

- DOE-STD-1186-2004, *Specific Administrative Controls,* Department of Energy, Washington, D.C., 2004.

- DOE-STD-1189-2008, *Integration of Safety into the Design Process,* Department of Energy, Washington, D.C., 2008.

- DOE-STD-1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities,* Department of Energy, Washington, D.C., 2011.

- DOE-STD-1212-2012, *Explosives Safety,* Department of Energy, Washington, D.C., 2012.

- DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities,* Department of Energy, Washington, D.C., 2007.

- DOE-STD-3009-1994, Chg 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports,* Department of Energy, Washington, D.C., 2006.

- DOE-STD-3020, *Specifications for HEPA Filters Used by DOE Contractors,* Department of Energy, Washington, D.C., 2005.

- DOE-STD-3024-2011, *Content of System Design Descriptions,* Department of Energy, Washington, D.C., 2011.

- DOE-HDBK-1132-1999, *Design Considerations,* Department of Energy, Washington, D.C., 1999.

- DOE-HDBK-1163-2003, Integration of Multiple *Hazard Analysis Requirements and Activities,* Department of Energy, Washington, D.C., 2003.

- DOE-HDBK-1169-2003, *Nuclear Air Cleaning Handbook,* Department of Energy, Washington, D.C., December, 2003.

Defense Nuclear Facilities Safety Board

- DNFSB Recommendation 2004-2, *Active Confinement Systems.*
- DNFSB TECH 34, *Confinement of Radioactive Materials at Defense Nuclear Facilities*, Technical Report, October 2004.

Hydraulic Institute Standards

- *Hydraulic Institute Standards*, standards as applicable.

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE Std. C37 Series, *Power Switchgears, Substations, and Relays,* (standards on switchgear as applicable), 2010.
- IEEE C2-2012, *National Electrical Safety Code*, 2012.
- IEEE Std N42.18-2004, *American National Standard Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents,* 2004.
- IEEE Std N323D-2002, *American National Standard to Installed Radiation Protection Instrumentation*, 2003.
- IEEE Std 7-4.3.2-2010, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,* 2010.
- IEEE Std 80-2000, *IEEE Guide for Safety in AC Substation Grounding,* 2000.
- IEEE Std. 141-1993, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants,* 1994.
- IEEE Std. 142-2007, *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems,* 2007.
- IEEE Std. 242-2001, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems (IEEE Buff Book),* 2001.
- IEEE Std. 279-1971, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations,* 1971.
- IEEE Std. 308-2001, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations,* 2001.
- IEEE Std. 323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,* 2003.

- IEEE Std. 334-2006, *IEEE Standard for Qualifying Continuous Duty Class 1E Motors for Nuclear Power Generating Stations,* 2006.

- IEEE Std. 336-2010, *IEEE Recommended Practice for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities,* 2010.

- IEEE Std. 338-2012, *IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems,* 2012.

- IEEE Std. 344-2004, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,* 2004.

- IEEE Std 352-1987, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems,* 1987.

- IEEE Std. 379-2000, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,* 2000.

- IEEE Std. 382-2006, *IEEE Standard for Qualification of Safety-Related Actuators for Nuclear Generating Stations,* 2006.

- IEEE Std. 383-2003, *IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations,* 2003.

- IEEE Std. 384-2008, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,* 2008.

- IEEE Std. 387-1995, *Standard Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generation Stations,* 1995.

- IEEE Std. 399-1997, *IEEE Recommended Practice for Industrial and Commercial Power Systems Analysis (IEEE Brown Book),* 1998.

- IEEE Std. 420-2001, *Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations,* 2002.

- IEEE Std. 446-1995, *Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications,* 1996.

- IEEE Std. 450-2010, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications,* 2010.

- IEEE Std. 484-2002, *IEEE Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications,* 2002.

- IEEE Std. 493-2007, *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems,* 2007.

- IEEE Std. 535-2006, *IEEE Standard for Qualification of Class 1E Lead Storage Batteries for Nuclear Power Generating Stations*, 2006.

- IEEE Std. 577-2012, *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities,* 2012.

- IEEE Std. 603-2009, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,* 2009.

- IEEE Std 627-2010, *IEEE Standard for Qualification of Equipment Used in Nuclear Facilities*, 2010.

- IEEE Std. 628-2011, *IEEE Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations,* 2011.

- IEEE Std. 649-2006, *IEEE Standard for Qualifying Class 1E Motor Control Centers for Nuclear Power Generating Stations*, 2006.

- IEEE Std. 650-2006, *IEEE Standard for Qualification of Class 1E Static Battery Chargers and Inverters for Nuclear Power Generating Stations,* 2006.

- IEEE Std. 749-1983 (withdrawn), *Standard for Periodic Testing of Diesel Generator Units Applied as Standby Power Supplies in Nuclear Power Generating Stations,* 1983.

- IEEE Std. 833-2005, *IEEE Recommended Practice for the Protection of Electric Equipment in Nuclear Power Generating Stations from Water Hazards*, 2005.

- IEEE Std. 946-2004, *IEEE Recommended Practice for the Design of DC Auxiliary Power Systems for Generating Systems*, 2004.

- IEEE Std. 1023-2004, *IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and other Nuclear Facilities*, 2004.

- IEEE Std. 1050-2004, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations,* 2004.

International Code Council

- International Code Council, *International Building Code.*

Illuminating Engineering Society

- IES HB-10-11, *IES Lighting Handbook,* 2011.

International Society of Automation

- ISA-TR84.00.06, *Safety Fieldbus Design Considerations for Process Industry Sector Applications,* 2009.

National Council on Radiation Protection and Measurements (NCRP)

- NCRP Report 49, *Structural Shielding Design and Evaluation for Medical Use of X Rays and Gamma Rays of Energies Up to 10 MeV,* 1976.

National Fire Protection Association (NFPA)

- NFPA 30, *Flammable and Combustible Liquids Code,* 2012.
- NFPA 70, *National Electric Code,* 2011.
- NFPA 72, *National Fire Alarm and Signaling Code,* 2013.
- NFPA 101, *Life Safety Code,* 2012.
- NFPA 110, *Standard for Emergency and Standby Power Systems, National Fire Protection Association,* 2013.
- NFPA 780, *Standard for the Installation of Lightning Protection Systems,* 2011.
- NFPA 1143, *Standard for Wildland Fire Management,* 2009.

Nuclear Regulatory Commission

- NUREG-0700, *Human-System Interface Design Review Guidelines,* Nuclear Regulatory Commission, 2002.

Tubular Exchanger Manufacturers Association (TEMA)

- TEMA, 9th Edition TEMA Standards, Tubular Exchanger Manufacturers Association, Inc., standards on heat exchangers Classes B, C, and R. Appendix F, Concluding Material.