National Nuclear Security Administration

Nuclear Safety Specialist

Qualification Standard

Reference Guide

AUGUST 2008

This page is intentionally blank.

Table of Contents

LIST OF FIGURES ..... **iv**
LIST OF TABLES ..... **v**
ACRONYMS ..... **vi**
PURPOSE **1**
SCOPE **1**
PREFACE **1**
ACKNOWLEDGEMENTS **2**
TECHNICAL COMPETENCIES **3**

1. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the fission process 3
2. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the principles and concepts for internal and external dosimetry, dose consequences, and the various methods to reduce exposure. 7
3. Nuclear safety specialists shall demonstrate a familiarity level knowledge of criticality control, safety parameters, alarm systems, and poisons. 12
4. Nuclear safety specialists shall demonstrate a working level knowledge of terminology used in nuclear safety analysis. 23
5. Nuclear safety specialists shall demonstrate a working level knowledge of the principal hazard and accident analysis methods. 36
6. Nuclear safety specialists shall demonstrate a familiarity level knowledge of terminology associated with PRA techniques. 59
7. Nuclear safety specialists shall demonstrate a familiarity level knowledge of basic Heating, Ventilation, Air Conditioning (HVAC) system and filtration system construction, operation, and application. 67
8. Nuclear safety specialists shall demonstrate a familiarity level knowledge of process instrumentation principles of operation as applied to nuclear safety-related systems. 79
9. Nuclear safety specialists shall demonstrate a familiarity level knowledge of P&ID. 86
10. Nuclear safety specialists shall demonstrate a familiarity level knowledge of electrical diagrams and schematics. 96
11. Nuclear safety specialists shall demonstrate a familiarity level knowledge of electrical logic diagrams. 103
12. Nuclear safety specialists shall demonstrate a working level knowledge of radioactivity and transformation mechanisms. 108
13. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the biological effects of radiation. 114
14. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the principles and use of radiological instrumentation and radiological monitoring/survey practices. 116

Table of Contents

REGULATORY 122

15. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.204, Documented Safety Analysis, and DOE Guide (G) 421.1-2, Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830, with respect to their impact on the Department's nuclear safety. 122
16. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.207, DOE Approval of Safety Basis, and DOE-STD-1104-96, Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements), with respect to their impact on the Department's nuclear safety. 133
17. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.206, Preliminary Documented Safety Analysis, with respect to its impact on the Department's nuclear safety. 138
18. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.202, Safety Basis, and DOE-STD-1027-92, Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports, with respect to their impact on the Department's nuclear safety. 141
19. Nuclear safety specialists shall demonstrate a familiarity level knowledge of DOE O 420.1B, Facility Safety; DOE G 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE O 420.1, Facility Safety; and DOE-STD-1020-2002, Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities; with respect to their impact on the Department's nuclear safety. 144
20. Nuclear safety specialists shall demonstrate a working level knowledge of the TSRs as described in 10 CFR 830.205, Technical Safety Requirements, and DOE G 423.1-1, Implementation Guide for Use in Developing Technical Safety Requirements, with respect to their impact on the Department's nuclear safety. 155
21. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.203, Unreviewed Safety Question Process, and DOE G 424.1-1A, Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements, with respect to their impact on the Department's nuclear safety..... 162
22. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the relationships between the problems being addressed by safety analysis and computer codes, the design requirements for the codes, and the components of the codes. 172
23. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the following criticality safety-related American National Standards Institute/American Nuclear Society (ANSI/ANS) standards:..... 177
24. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the following DOE Orders, technical standards, and Guides: 181

Table of Contents

25. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the Price-Anderson Amendments Act of 1988 and its relationship to Subparts A and B of 10 CFR 830 190

26. Nuclear safety specialists shall demonstrate a working level knowledge of the requirements in DOE technical standard DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis, and DOE-STD-3010-94**, Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities. 192

27. Nuclear safety specialists shall demonstrate a working level knowledge of DOE-STD-1186-2004, Specific Administrative Controls, with respect to its impact on the Department's nuclear safety. 215

MANAGEMENT, ASSESSMENT, AND OVERSIGHT 221

28. Nuclear safety specialists shall demonstrate a working level knowledge of assessment techniques (such as the planning and use of observations, interviews, and document reviews) to assess facility performance, report results of assessments, and follow up on actions taken as the result of assessments. 221

29. Nuclear safety specialists shall demonstrate a working level knowledge of the DOE facility contract provisions necessary to provide oversight of a contractor's operations. 226

30. Nuclear safety specialists shall demonstrate a familiarity level knowledge of problem analysis principles and the techniques necessary to identify problems, potential causes, and corrective action(s) associated with nuclear safety issues at DOE nuclear facilities..... 230

31. Nuclear safety specialists shall demonstrate a familiarity level knowledge of DOE Policy 450.4, Safety Management System Policy; Policy 226.1A, Department of Energy Oversight Policy; and DOE O 226.1, Implementation of Department of Energy Oversight Policy, as applied to nuclear safety. 234

SELECTED BIBLIOGRAPHY AND SUGGESTED READING 239

Figures

Figure 1. Binding energy per nucleon vs. mass number 4
Figure 2. Uranium-235 fission yield vs. mass number 6
Figure 3. MAGIC MERV 13
Figure 4. Flowchart for performing a hazard analysis 41
Figure 5. Atmospheric processes acting upon radiological/toxicological releases 52
Figure 6. Coordinate system of Gaussian plume 53
Figure 7. Time-dependent component availability 62
Figure 8. Typical process facility confinement zones 75
Figure 9. Limit switches 82
Figure 10. Potentiometer valve position indicator 83
Figure 11. Linear variable differential transformer 84
Figure 12. Example P&ID 85
Figure 13. Valve symbols 87
Figure 14. Valve actuator symbols 87
Figure 15. Fluid power pump and compressor symbols 88
Figure 16. Symbols for major components 89
Figure 17. Indicators and recorders 91
Figure 18. Controllers 92
Figure 19. Signal conditioners 92
Figure 20. Control valve designations 93
Figure 21. Remotely controlled valve 93
Figure 22. Level control valve 94
Figure 23. Control valve with valve positioners 94
Figure 24. Valve status symbols 95
Figure 25. Electrical symbols 97
Figure 26. Symbols for motors 97
Figure 27. Basic transformer symbols 98
Figure 28. Transformer polarity 98
Figure 29. Fuse and circuit breaker symbols 99
Figure 30. Three-phase and removable breaker symbols 100
Figure 31. Generator—electromagnetic induction 100
Figure 32. Basic chemical battery 101
Figure 33. One-line diagram 102
Figure 34. Basic logic symbols 103
Figure 35. Conventions for depicting multiple inputs 104
Figure 36. Coincidence gate 104
Figure 37. EXCLUSIVE OR and EXCLUSIVE NOR gates 105
Figure 38. Truth tables 106
Figure 39. Logic gate status notations 107
Figure 40. Example of a logic print 108
Figure 41. Nuclide chart for atomic numbers 1 to 6 109
Figure 42. Relative locations of the products of various nuclear processes 110
Figure 43. Wind speed and direction affect plume dispersion 211

Tables

Table 1. Surface areas for sphere, cylinder, and disk....14
Table 2. Example hazard identification....39
Table 3. Instrument identifiers....90
Table 4. Flood criteria summary....149
Table 5. Comparison of performance categories from various sources....154
Table 6. Insolation data....189
Table 7. Criteria for free drop test (weight/distance)....190
Table 8. Safe harbor methods....203

Acronyms	
°C	degree Celsius
°F	degree Fahrenheit
AC	administrative control
AEA	Atomic Energy Act
AED	aerodynamic equivalent diameter
AEGL	acute exposure guideline level
ALARA	as low as reasonably achievable
ALI	annual limit on intake
ALOHA	Areal Locations of Hazardous Atmospheres
ANS	American Nuclear Society
ANSI	American National Standards Institute
ARF	airborne release fraction
ARM	area radiation monitor
ARS	acute radiation syndrome
ASCE	American Society of Civil Engineers
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
ASME	American Society of Mechanical Engineers
BIO	basis of interim operation
Bq	becquerel
CAAS	criticality accident alarm system
cal	calorie
CAM	continuous air monitor
CFAST	Consolidated Model of Fire and Smoke Transport
CFR	*Code of Federal Regulations*
Ci	curie
cm	centimeter
CSDR	conceptual safety design report
CSE	criticality safety evaluation
CSO	Cognizant Secretarial Officer
CSP	criticality safety program
DAC	derived air concentration
DBA	design basis accident
DBFL	design basis flood
DCG	derived concentration guide
DEGADIS	Dense Gas Dispersion Model
DID	defense in depth

Acronyms	
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
DR	damage ratio
DSA	documented safety analysis
EG	evaluation guideline
EPA	U. S. Environmental Protection Agency
EPIcode	Emergency Prediction Information Code
ERPG	emergency response planning guide
ESD	event sequence diagram
ET	event tree
FAQS	functional area qualification standard
FEM	field element manager
FHA	fire hazard analysis
FMEA	failure modes and effects analysis
FRAM	Safety Management Functions, Responsibilities, and Authorities Manual
ft	foot or feet
g	gram
G	Guide
GENII	Generation II Environmental Dosimetry System
G-M	Geiger-Mueller
GOCO	government-owned, contractor-operated
Gy	gray
h	hour
HAR	hazard analysis report
HASP	health and safety plan
HAZOP	hazard and operability study
HAZWOPER	hazardous waste operations and emergency response
HEPA	high energy particulate air (filter)
HRA	human reliability assessment
HSS	U.S. DOE, Office of Health, Safety, and Security
HVAC	heating, ventilation, air conditioning
IBC	International Building Code
ICRP	International Commission on Radiological Protection
ICSSC	Interagency Committee on Seismic Safety in Construction
IE	initiating event
IEEE	Institute of Electrical and Electronics Engineers

Acronyms	
IMBA	Integrated Modules for Bioassay
in.	inch
INPO	Institute of Nuclear Power Operations
ISM	integrated safety management
ISMS	Integrated Safety Management System
JCO	justification for continuing operations
kg	kilogram
kPa	kiloPascal
L	liter
LANL	Los Alamos National Laboratory
lb	pound or pounds
lbf	pound-force
lbm	pound-mass
LCO	limiting conditions for operation
LCS	limiting condition statement
LD50	median lethal dose
LPF	leak path factor
LVDT	linear variable differential transformer
m	meter
M	Manual
M&O	management and operating
M&TE	measuring and test equipment
MACCS/ MACCS2	MELCOR Accident Consequence Code System (2 versions)
MAR	material at risk
MARPLOT	Mapping Applications for Response, Planning, and Local Operational Tasks
MCS	minimal cut set
MELCOR	Methods for Estimation of Leakages and Consequences of Releases
MeV	million electron volts
mg	milligram
MOI	maximally-exposed offsite individual
mR	milliroentgen
MW	megawatt
NASA	National Aeronautics and Space Administration
NCS	nuclear criticality safety
NEHRP	National Earthquake Hazards Reduction Program
NFPA	National Fire Protection Association

Acronyms	
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NPH	natural phenomena hazard
NQA	nuclear quality assurance
NRC	U. S. Nuclear Regulatory Commission
NSS	nuclear safety specialist
O	Order
OL	operating limit
ORR	operational readiness review
OSHA	Occupational Safety and Health Administration
P&ID	piping and instrumentation drawing
PAAA	Price-Anderson Amendments Act
PAC	protective action criteria
PC	performance category
PDSA	preliminary documented safety analysis
PEP	performance evaluation plan
PHA	preliminary hazard analysis
PI	performance indicator
PISA	potential inadequacy of the safety analysis
PM	particulate matter
ppm	parts per million
PRA	probabilistic risk assessment
PSDR	preliminary safety design report
psi	pounds per square inch
psig	pounds per square inch gauge
PSM	process safety management
PSO	Program Secretarial Officer
QA	quality assurance
QAP	quality assurance program
R	roentgen
rad	radiation absorbed dose
rem	roentgen equivalent man
RF	respirable fraction
RTD	resistance temperature detector
SA	specific activity
SAC	specific administrative control
SAR	safety analysis report

Acronyms	
SARP	safety analysis report for packaging
SC	safety class
SCRAM	Support Center for Regulatory Air Models
sec	second (time)
SEN	Secretary of Energy Notice
SER	safety evaluation report
SL	safety limit
SME	subject matter expert
SNM	special nuclear material
SQA	software quality assurance
SR	surveillance requirement
SS	safety significant
SSC	structure, system, component
TC	thermocouple
TEDE	total effective dose equivalent
TEEL	temporary emergency exposure limit
TLD	thermoluminescent dosimeters
TQ	threshold quantity
TSR	technical safety requirement
USQ	unreviewed safety question
USQD	unreviewed safety question determination
VAC	volts alternating current
VOC	volatile organic compound
Wt	weighting factor
yr	year

PURPOSE

The purpose of this reference guide is to provide a document that contains the information required for a Department of Energy (DOE)/National Nuclear Security Administration (NNSA) technical employee to successfully complete the Nuclear Safety Specialist Functional Area Qualification Standard (FAQS). Information essential to meeting the qualification requirements is provided; however, some competency statements require extensive knowledge or skill development. Reproducing all the required information for those statements in this document is not practical. In those instances, references are included to guide the candidate to additional resources.

SCOPE

This reference guide addresses the competency statements in the November 2007 edition of DOE-STD-1183-2007, *Nuclear Safety Specialist Functional Area Qualification Standard*. The qualification standard contains 31 competency statements.

Please direct your questions or comments related to this document to the NNSA Learning and Career Development Department.

PREFACE

Competency statements and supporting knowledge and/or skill statements from the qualification standard are shown in contrasting bold type, while the corresponding information associated with each statement is provided below it.

A comprehensive list of acronyms and abbreviations is found at the beginning of this document. It is recommended that the candidate review the list prior to proceeding with the competencies, as the acronyms and abbreviations may not be further defined within the text unless special emphasis is required.

The competencies and supporting knowledge, skill, and ability (KSA) statements are taken directly from the FAQS. Most corrections to spelling, punctuation, and grammar have been made without remark, and all document-related titles, which variously appear in roman or italic type or set within quotation marks, have been changed to plain text, also mostly without remark. Capitalized terms are found as such in the qualification standard and remain so in this reference guide. When they are needed for clarification, explanations are enclosed in brackets.

Every effort has been made to provide the most current information and references available as of August 2008. However, the candidate is advised to verify the applicability of the information provided. It is recognized that some personnel may oversee facilities that utilize predecessor documents to those identified. In those cases, such documents should be included in local qualification standards via the Technical Qualification Program.

In the cases where information about an FAQS topic in a competency or KSA statement is not available in the newest edition of a standard (consensus or industry), an older version is referenced. These references are noted in the text and in the bibliography.

Only significant corrections to errors in the technical content of the discussion text source material are identified. Editorial changes that do not affect the technical content (e.g., grammatical or spelling corrections, and changes to style) appear without remark. A horizontal line separates original discussion text from material taken from other sources.

ACKNOWLEDGEMENTS

Some of the references and responses to the knowledge, skill, and ability statements that are related to specific nuclear safety specialist responsibilities were provided by a team of subject matter experts in the NNSA Service Center.

TECHNICAL COMPETENCIES

1. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the fission process.

a. Define the following terms:
- **Excitation energy**
- **Critical energy**
- **Fissile material**
- **Fissionable material**
- **Fertile material**

The following definitions are taken from DOE-HDBK-1019/1-93.

Excitation Energy

The measure of how far the energy level of a nucleus is above its ground state is called the excitation energy (E_{exc}).

Critical Energy

The critical energy (E_{crit}) is the minimum excitation energy required for fission to occur.

Fissile Material

A fissile material is composed of nuclides for which fission is possible with neutrons of any energy level. What is especially significant about these nuclides is their ability to be fissioned with zero kinetic energy neutrons (thermal neutrons). Thermal neutrons have very low kinetic energy levels (essentially zero) because they are roughly in equilibrium with the thermal motion of surrounding materials. Therefore, in order to be classified as fissile, a material must be capable of fissioning after absorbing a thermal neutron. Consequently, fission products impart essentially no kinetic energy to the reaction. Fission is possible in these materials with thermal neutrons, since the change in binding energy supplied by the neutron addition alone is high enough to exceed the critical energy. Some examples of fissile nuclides are uranium-235, uranium-233, and plutonium-239.

Fissionable Material

A fissionable material is composed of nuclides for which fission with neutrons is possible. All fissile nuclides fall into this category. However, also included are those nuclides that can be fissioned only with high-energy neutrons. The change in binding energy that occurs as the result of neutron absorption results in a nuclear excitation energy level that is less than the required critical energy. Therefore, the additional excitation energy must be supplied by the kinetic energy of the incident neutron. The reason for this difference between fissile and fissionable materials is the so-called odd-even effect for nuclei. It has been observed that nuclei with even numbers of neutrons and/or protons are more stable than those with odd numbers. Therefore, adding a neutron to change a nucleus with an odd number of neutrons to a nucleus with an even number of neutrons produces an appreciably higher binding energy than adding a neutron to a nucleus already possessing an even number of neutrons. Some

examples of nuclides requiring high energy neutrons to cause fission are thorium-232, uranium-238, and plutonium-240.

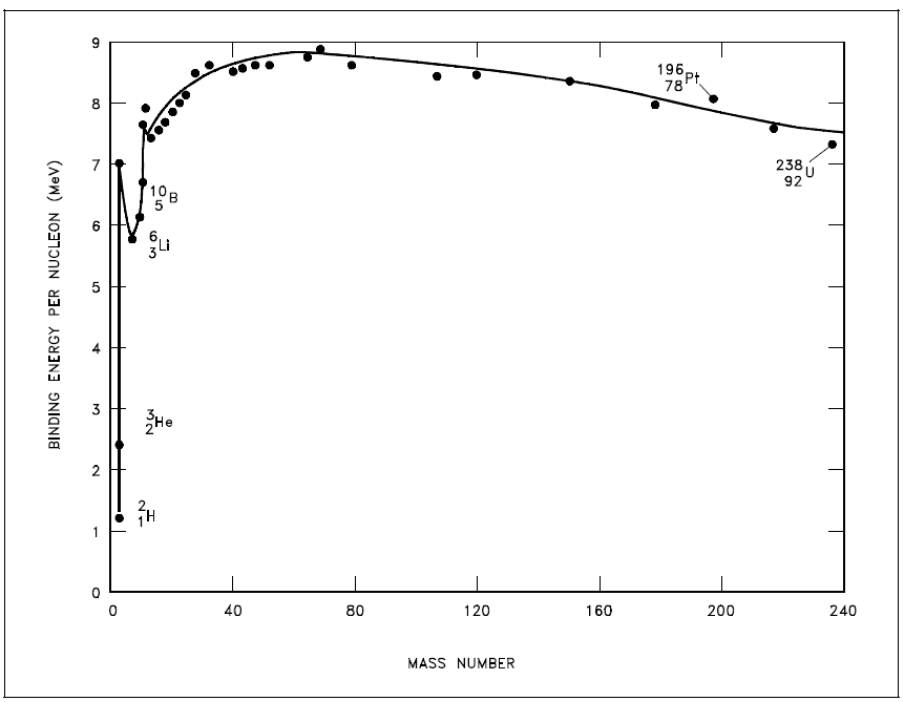
Fertile Material

All of the neutron absorption reactions that do not result in fission lead to the production of new nuclides through the process known as transmutation. These nuclides can, in turn, be transmuted again or may undergo radioactive decay to produce still different nuclides. The nuclides that are produced by this process are referred to as transmutation products. Because several of the fissile nuclides do not exist in nature, they can only be produced by nuclear reactions (transmutation). The target nuclei for such reactions are said to be fertile. Fertile materials are materials that can undergo transmutation to become fissile materials.

b. Describe the curve of binding energy per nucleon vs. mass number and qualitatively describe the reasons for its shape.

The following is taken from DOE-HDBK-1019/1-93.

As the number of particles in a nucleus increases, the total binding energy also increases. The rate of increase, however, is not uniform. This lack of uniformity results in a variation in the amount of binding energy associated with each nucleon within the nucleus. This variation in the binding energy per nucleon (BE/A) is easily seen when the average BE/A is plotted versus atomic mass number (A), as shown in figure 1.



Source: DOE-HDBK-1019/1-93

Figure 1. Binding energy per nucleon vs. mass number

Figure 1 illustrates that as the atomic mass number increases, the binding energy per nucleon decreases for A > 60. The BE/A curve reaches a maximum value of 8.79 million electron volts (MeV) at A = 56 and decreases to about 7.6 MeV for A = 238. The general shape of the BE/A curve can be explained using the general properties of nuclear forces. The nucleus is held together by very short-range attractive forces that exist between nucleons. On the other hand, the nucleus is being forced apart by long-range repulsive electrostatic (coulomb) forces that exist between all the protons in the nucleus.

As the atomic number and the atomic mass number increase, the repulsive electrostatic forces within the nucleus increase due to the greater number of protons in the heavy elements. To overcome this increased repulsion, the proportion of neutrons in the nucleus must increase to maintain stability. This increase in the neutron-to-proton ratio only partially compensates for the growing proton-proton repulsive force in the heavier, naturally occurring elements. Because the repulsive forces are increasing, less energy must be supplied, on the average, to remove a nucleon from the nucleus. The BE/A has decreased. The BE/A of a nucleus is an indication of its degree of stability. Generally, the more stable nuclides have higher BE/A than the less stable ones. The increase in the BE/A as the atomic mass number decreases from 260 to 60 is the primary reason for the energy liberation in the fission process. In addition, the increase in the BE/A as the atomic mass number increases from 1 to 60 is the reason for the energy liberation in the fusion process, which is the opposite reaction of fission.

c. Explain why only the heaviest nuclei are easily fissioned.

Per DOE-HDBK-1019/1-93, the heaviest nuclei require only a small distortion from a spherical shape (small energy addition) for the relatively large coulomb forces forcing the two halves of the nucleus apart to overcome the attractive nuclear forces holding the two halves together. Consequently, the heaviest nuclei are easily fissionable compared to lighter nuclei.

d. Explain why uranium-235 fissions with thermal neutrons and uranium-238 fissions only with fast neutrons.

Per DOE-HDBK-1019/1-93, uranium-235 fissions with thermal neutrons because the binding energy released by the absorption of a neutron is greater than the critical energy for fission. The binding energy released by uranium-238 absorbing a neutron is less than the critical energy, so additional kinetic energy must be possessed by the neutron for fission to be possible.

e. Characterize the fission products in terms of mass groupings and radioactivity.

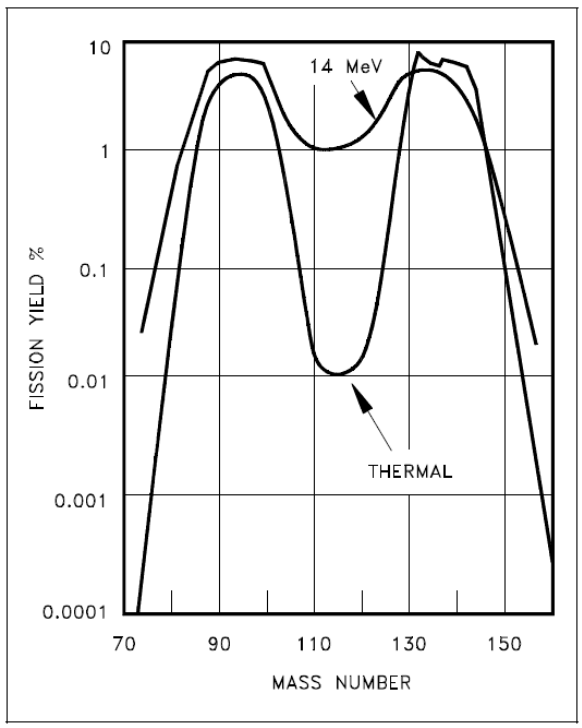
The following is taken from DOE-HDBK-1019/1-93.

Nuclear fission results in the release of enormous quantities of energy. It is necessary to be able to calculate the amount of energy that will be produced. The logical manner in which to pursue this is to first investigate a typical fission reaction such as the one listed below.

$$ {}^{1}_{0}n + {}^{235}_{92}U \rightarrow \left({}^{236}_{92}U\right)^{*} \rightarrow {}^{140}_{55}Cs + {}^{93}_{37}Rb + 3\left({}^{1}_{0}n\right) $$

It can be seen that when the compound nucleus splits, it breaks into two fission fragments, rubidium-93, cesium-140, and some neutrons. Both fission products then decay by multiple β^- emissions as a result of the high neutron-to-proton ratio possessed by these nuclides.

In most cases, the resultant fission fragments have masses that vary widely. Figure 2 gives the percent yield for atomic mass numbers. The most probable pair of fission fragments for the thermal fission of the fuel uranium-235 have masses of about 95 and 140. Note that the vertical axis of the fission yield curve is on a logarithmic scale. Therefore, the formation of fission fragments of mass numbers of about 95 and 140 is highly likely.



Source: DOE-HDBK-1019/1-93

Figure 2. Uranium-235 fission yield vs. mass number

2. **Nuclear safety specialists shall demonstrate a familiarity level knowledge of the principles and concepts for internal and external dosimetry, dose consequences, and the various methods to reduce exposure.**

   a. **Define the following terms:**
      - **Committed effective dose equivalent**
      - **Total effective dose equivalent**
      - **Whole body**
      - **Derived Air Concentration (DAC)**
      - **Annual Limit on Intake (ALI)**
      - **Tissue**
      - **Weighting factors**
      - **Stochastic effects**
      - **Non-stochastic (deterministic) effects**

The following definitions are taken from DOE-HDBK-1122-99, module 2.04.

Committed Effective Dose Equivalent

Committed effective dose equivalent is the sum of the committed dose equivalents to various tissues, excluding the skin and lens of the eye, in the body, each multiplied by the appropriate weighting factor (Wt). A committed dose equivalent for a tissue or organ is the dose equivalent calculated to be received by the tissue or organ over a 50-year period after the intake of a radionuclide into the body. Committed effective dose equivalent is expressed in units of rem (or sievert).

Total Effective Dose Equivalent

Total effective dose equivalent is the sum of the effective dose equivalent (for external exposures) and the committed effective dose equivalent (for internal exposures). Deep dose equivalent to the whole body may be used as effective dose equivalent for external exposures.

Whole Body

For the purposes of external exposure, the whole body is the head, the trunk (including male gonads), the arms above and including the elbow, or the legs above and including the knee.

Derived Air Concentration (DAC)

For the radionuclides listed in appendix A of 10 CFR 835, DAC is the airborne concentration that equals the ALI divided by the volume breathed by an average worker for a working year of 2,000 hours (assuming a breathing volume of 2,400 m^3).

Annual Limit on Intake (ALI)

The ALI is the limit for the amount of radioactive material taken into the body of an adult worker by inhalation or ingestion in a year. ALI is the smaller value of intake of a given radionuclide in a year by the reference man that would result in a committed effective dose equivalent of 5 rem (0.05 sievert) or a committed dose equivalent of 50 rem (0.5 sievert) to any individual organ or tissue.

Tissue

Radiosensitive tissues include the following:

- Germinal (reproductive) cells of the ovary and testis, e.g., spermatogonia
- Hematopoietic (bloodforming) tissues: red bone marrow, spleen, lymph nodes, thymus
- Basal cells of the skin
- Epithelium of the gastrointestinal tract (interstitial crypt cells)

Radioresistant tissues include the following:

- Bone
- Liver
- Kidney
- Cartilage
- Muscle
- Nervous tissue

Radiosensitivity not only differs from one cell or tissue to another but also between individuals and genders.

Weighting Factors

Weighting factors are the fraction of the overall health risk, resulting from uniform, whole-body irradiation, attributable to specific tissue. The dose equivalent to the affected tissue is multiplied by the appropriate weighting factor to obtain the effective dose equivalent contribution from that tissue.

Stochastic Effects

Stochastic effects include the following:

- An effect in which the probability of the effect occurring increases with the dose
- The effects have no established threshold; they can occur from the irradiation of only one cell; any exposure, however low, has some chance of causing the effect
- Two examples of stochastic effects: cancer and genetic mutations

Non-stochastic (Deterministic) Effects

Non-stochastic effects include the following:

- Effects in which the severity of the effect increases as the dose increases.
- It is generally assumed that a threshold exists, and if doses received are below the threshold dose, no effects will occur.
- Effects typically result from the collective injury of many cells.
- Effects include cataracts, skin burns, and lowering of blood cell counts.

b. Discuss International Commission on Radiological Protection (ICRP) publications 26, 30, 60, 68, 71 and 72 as they relate to dose conversion factors and consequence analysis in hazard categorization and accident analysis.

ICRP Publication 26

The ICRP published its initially general recommendation for radiological protection in 1928. Further recommendations adapted to the latest information followed in 1959 and 1966. Since 1977, when the ICRP published its fundamental recommendations as ICRP publication 26, the ICRP has checked these recommendations annually and published supplementary comments from time to time in the annals of the ICRP.

ICRP Publication 30

This addendum is concerned with the numerical value of the secondary limits, the ALI, and the DAC for certain radionuclides. It takes into account data from the 1986 review of publication 19, which was published as publication 48. Publication 48 paid specific attention to information regarding absorption from the gastrointestinal tract and distribution between, and retention within, the skeleton and liver. Dosimetric data for the radionuclides are given in an appendix.

ICRP Publication 60

The ICRP issued its last basic recommendations in 1977. The recommendations have been used widely throughout the world to limit exposure of both radiation workers and members of the public to ionizing radiations. In publishing these recommendations, the Commission has had three aims in mind: to take account of new biological information and of trends in the setting of safety standards; to improve the presentation of the recommendations; and to maintain as much stability in the recommendations as is consistent with the new information. The recommendations are set out in the form of a main text supported by annexes. The main text contains all the recommendations, together with sufficient explanatory material to make clear the underlying reasoning for policy makers. The supporting annexes contain more detailed scientific information on specific points for specialists.

ICRP 68

The Commission's 1990 recommendations on radiation protection standards in ICRP publication 60 were developed to take into account new biological information related to the detriment associated with radiation exposures and supersede the earlier recommendations in ICRP publication 26. In order to permit immediate application of these new recommendations, revised values of the ALIs based on the methodology and biokinetic information and incorporating the new dose limits and tissue weighting factors, were issued as ICRP publication 61. Since issuing ICRP publication 61, the ICRP has published a revised kinetic and dosimetric model of the respiratory tract. The main aim of ICRP 68 is to give values of dose coefficients for workers using this new model.

ICRP 71

An ongoing objective of the ICRP is to evaluate dose coefficients (doses per unit intake) for members of the public. The purpose of ICRP publication 71 is to provide updated inhalation

dose coefficients for selected radioisotopes of hydrogen, carbon, sulfur, calcium, iron, cobalt, nickel, zinc, selenium, strontium, zirconium, niobium, molybdenum, technetium, ruthenium, silver, antimony, tellurium, iodine, cesium, barium, cerium, lead, polonium, radium, thorium, uranium, neptunium, plutonium, americium, and curium. Age-dependent biokinetic models for calcium, curium, and for decay products formed following the intake of lead, radium, tellurium, thorium, and uranium are provided in annexes.

ICRP 72

The purpose of ICRP 72 is to summarize data on age-dependent committed effective dose coefficients for members of the public from intakes by ingestion and inhalation of radioisotopes of the 91 elements described in ICRP publications 56, 67 through 69, and 71. These dose coefficients have been adopted in the International Atomic Energy Agency in their publication "International Basic Safety Standards for Protection against Ionizing Radiation," and in the Council Directive 97/43 Euratom, of June 30, 1997. ICRP 72 does not give committed equivalent dose coefficients to tissues and organs. ICRP will be useful to operational health physicists and to regulatory and advisory bodies responsible for radiation protection.

On February 22, 2008, the NNSA Central Technical Authority issued a memorandum directing the use of dose conversion factors in ICRP 68 and 72 for safety basis radiological dose consequence analyses because they provide more accuracy and are consistent with methodology use in 10 CFR 835.

c. Describe the following aspects of dose reduction:

- **Time**
- **Distance**
- **Shielding**
- **Inverse square law**
- **As Low As Reasonably Achievable (ALARA)**

The following definitions are taken from DOE-HDBK-1130-2007.

Time

Dose received is proportional to the time spent in proximity to a radiation source; therefore, dose can be reduced by minimizing the time of exposure. Methods for minimizing time include the following:

- Plan and discuss the task thoroughly prior to entering the area. Use only the number of workers actually required to do the job.
- Have all necessary tools present before entering the area.
- Use mock-ups and practice runs that duplicate work conditions.
- Take the most direct route to the job site if possible and practical.
- Never loiter in an area controlled for radiological purposes.
- Work efficiently and swiftly.
- Perform as much work outside the area as possible. When practical, remove parts or components to areas with lower dose rates to perform work.

- Do not exceed stay times. In some cases, the radiological control organization may limit the amount of time a worker may stay in an area due to various reasons. This is known as "stay time." If you have been assigned a stay time, do not exceed this time.

Distance

Dose received is inversely proportional to the distance (see "Inverse Square Law," below) from a radiation source; therefore, dose can be reduced by increasing the distance from the source. Methods for increasing distance from sources of radiation are as follows:

- Be familiar with radiological conditions in the area.
- Stay as far away from radiation sources as practical given the task assignment.
- During work delays, move to lower dose rate areas.
- Use remote handling devices when possible.

Shielding

Shielding reduces the amount of radiation dose to the worker by attenuation. Different materials shield a worker from the different types of radiation. Permanent shielding is installed as part of facility construction in accordance with the facility design, which should have as a goal dose minimization. Temporary shielding (e.g., lead or concrete blocks) can be installed for temporary conditions such as maintenance activities. Temporary shielding should be installed and used only in accordance with procedures of the Radiation Protection Program.

Inverse Square Law

Inverse square law is the principle that a physical quantity (in this case, radiation dose) is inversely proportional to the square of the distance from the source of the quantity. For example, the dose rate at a given distance from a point source (such as a hot spot), will decrease to one-fourth the value at twice the distance.

As Low As Reasonably Achievable (ALARA)

ALARA is an approach to radiation safety that strives to manage and control doses (both individual and collective) to the work force and the general public to as low as is reasonable, taking into account social, technical, economic, practical, and public policy considerations.

d. Describe the hierarchy of controls; engineered, administrative, and personnel protective equipment objectives of 10 CFR 835; for controlling personnel exposure from external sources of radiation in areas of continuous occupational occupancy.

The following is taken from DOE-HDBK-1141-2001.

The minimization and control of internal dose should be conducted in accordance with the following hierarchy of controls:

1. Engineered controls, including containment of radioactive material at the source wherever applicable, should be the primary method of minimizing airborne radioactivity and internal dose to workers. Engineered controls are devices such as glove boxes, glove bags, portable filtration units, and containment tents. They should

be used to prevent worker inhalation of radionuclides. Portable and fixed/permanent shielding using dense materials (lead) or portable plastic interlocking fluid filled containers are also engineered features, used to minimize external radiation dose. The use of these devices reduces the spread of contamination, cleanup time, and decontamination costs. These measures help maintain doses ALARA. In addition, they can reduce the need for respirators and the impact on work in nearby areas. Engineered controls should be used in accordance with technical instructions, proper training, and effective administrative controls. Site-specific manuals should contain generic instructions on the design, controls, training, and use of engineered controls.

2. Administrative controls, including access restrictions and the use of specific work practices designed to minimize airborne contamination, should be used as the secondary method to minimize worker internal dose.

3. Only when engineered and administrative controls have been applied and the potential for airborne radioactivity still exists, should personnel protective equipment, including use of respiratory protection, be considered.

Chapter 3 of DOE-STD-1098-99 discusses access controls for contamination areas, controlling the spread of contamination, and monitoring for contamination. Appendix 3C, "Contamination Control Practices," includes recommended selection of protective clothing, and a recommended sequence for donning and doffing.

3. Nuclear safety specialists shall demonstrate a familiarity level knowledge of criticality control, safety parameters, alarm systems, and poisons.

a. Discuss the effects and applications of the following factors relevant to criticality safety of operations:
- **Mass**
- **Shape**
- **Interaction and separation**
- **Moderation**
- **Reflection**
- **Concentration**
- **Volume**
- **Density**
- **Neutron absorbers**
- **Heterogeneity**
- **Enrichment**

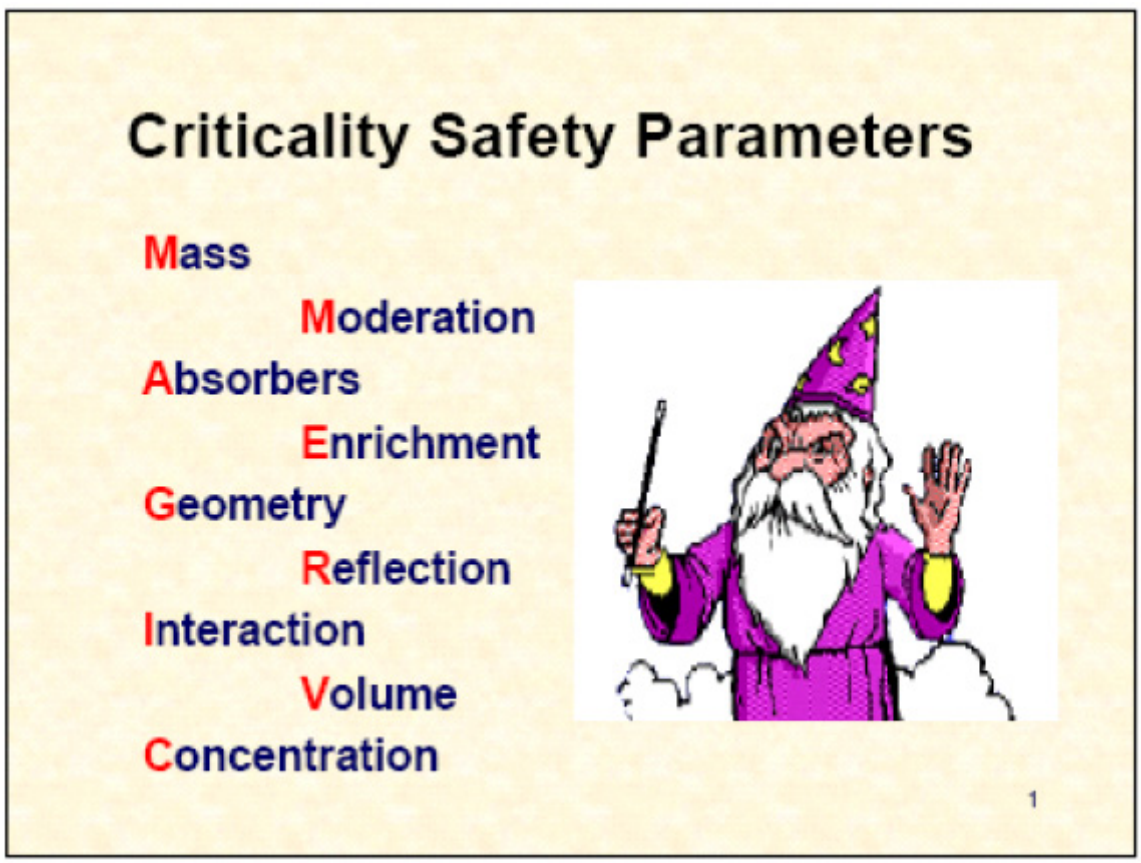
The following definitions are taken from the Los Alamos National Laboratory (LANL) Nuclear Science Self-Study Guide.

Mass

As an extensive property of matter, mass is the most commonly used measure of how much fissile material is available to contribute to a potentially critical system. Mass is frequently

one of the easiest parameters to control. Mass refers to the quantity of fissile material allowed. Mass is a convenient quantity to control because it can be measured fairly accurately. The potential for fission to occur increases as the mass increases because the number of fissionable target atoms increases. A critical mass is the minimum amount of fissionable material that will support a chain reaction (i.e., $k_{eff} \geq 1$) under a given set of conditions. A sustained nuclear reaction is only possible if enough material is brought together at one time. A large mass of fissile material gives neutrons more opportunity to strike fissile atoms and less opportunity to leak out of the material. The larger the mass of fissile material, the more fissions and the higher the neutron population.

Note that k_{eff} is called the "effective multiplication factor" which is defined as the ratio of neutrons produced by fission in one generation to the number of neutrons lost through absorption and leakage in the preceding generation. So, the value of k_{eff} for a self-sustaining chain reaction of fissions, where the neutron population is neither increasing nor decreasing, is one. The condition where the neutron chain reaction is self-sustaining and the neutron population is neither increasing nor decreasing is referred to as the critical condition and can be expressed by the simple equation $k_{eff} = 1.0000$.



Source: NNSA Service Center Safety Department, local training document mnemonic

Figure 3. MAGIC MERV

If the neutron production is greater than the absorption and leakage of neutrons, the reaction is called supercritical. In a supercritical condition, k_{eff} is greater than one, and the neutron population increases each generation. If, on the other hand, the neutron production is less than the absorption and leakage, the reaction is called subcritical. In a subcritical condition, k_{eff} is less than one, and the neutron population decreases each generation.

For criticality control, k_{eff} must be less than one (i.e., $k_{eff} < 1$).

Shape

Shape and geometry refer to the same controlled parameter. Recall that nuclear criticality occurs if the neutron production rate is equal to or exceeds the neutron loss rate. Therefore, unplanned criticality can be prevented by making the loss rate large when compared to the production rate. One way to avoid accidental criticality is to select an appropriate container. Table 1 illustrates how surface area can vary in different shapes while volume remains constant. For example, a long, thin cylinder has 1.43 times more surface area than a sphere of the same volume, and a disk has 1.56 times more surface area than the same sphere.

Table 1. Surface areas for sphere, cylinder, and disk

Shape	Volume (liters)	Surface Area (cm^2) [b]	Surface Area Compared to Sphere
Sphere	1.0	484	1.00
Cylinder (H/D[a] = 1/1)	1.0	554	1.14
Long, thin cylinder (H/D = 5/1)	1.0	694	1.43
Disk (H/D = 1/5)	1.0	755	1.56

Notes:

[a] H/D: height/diameter ratio.

[b] cm: centimeters.

Source: LANL, Nuclear Science Self-Study Guide

Geometric shape can either increase or decrease the number of neutrons that escape the material. The smallest leakage occurs from a sphere. Since fewer neutrons leak out, more are absorbed in fissile material producing more fissions, more neutrons, and so on. A circular cylinder with its height about equal to its diameter has somewhat more leakage than a sphere. The most leakage occurs from a thin cylinder. These shapes may be ranked from best to worst, where best means safest (very leaky) and not likely to form a critical mass. For a constant volume, then, the best shape is a long thin cylinder. The worst shape is the sphere. An elongated container has more surface area than a sphere.

Taking this concept one step further, look at a 1-liter cylinder and the changes in its surface area as the H/D (height to diameter) ratio is changed. If H/D is equal to 1 (H/D = l, or H = D), the cylinder is as wide as it is high; if R/D is greater than 1, the cylinder is long and thin, like a pencil; and if H/D is less than 1, the cylinder is disk-shaped.

The aforementioned table shows that long, thin cylinders and disks have more surface area, and thus have a greater neutron leakage rate than the cylinders where H = D. These shapes are preferred at the Savannah River Site.

A fissile solution of a certain concentration and volume may be safely stored in a long, thin cylindrical container. However, when the solution is transferred to a spherical container, an accidental criticality may occur. The solution has not changed in concentration or volume; the only change is in the shape of the container. The solution, safe in the first container, became critical in the second container because of the reduction in the neutron leakage rate caused by the reduction in surface area. The increased number of neutrons available for the fission reaction, as a result of the change in shape, was sufficient to permit a chain reaction.

Interaction and Separation

This parameter is also known as spacing. It is also related to concentration and fissile atom density. This interaction between two or more masses (or containers) of fissile material reduces the leakage of neutrons. This results in more neutrons being available to cause fission; therefore, criticality is more likely.

For example, consider two containers of fissile material, A and B. If the containers are close enough to each other, a certain number of neutrons leak out of container A and enter container B and cause fission. Likewise, neutrons leaking out of container B can enter container A and cause fission. This process is called interaction. Interaction decreases the neutron loss rate and increases the neutron production rate.

If container A is left by itself without a reflector, all of the neutrons leaking from the container are lost and cause no further fission. The two containers form a more reactive system together than when they are separated. The amount of interaction between the two containers depends upon the distance between them. The farther apart the two containers are spaced, the less they will interact. As the containers come closer together, interaction increases and so does the reactivity of the system.

Extreme care must be taken when working with containers containing fissile solutions. Maximizing the physical separation of containers of fissile material is an important method of criticality control.

Moderation

The energy (speed) of a neutron affects its ability to cause fission. In most fissile materials, a slow neutron is much more likely to cause fission than a fast neutron. All neutrons produced by fission are fast neutrons, with a speed of about 30,000,000 miles per hour when first produced, but neutrons can be slowed down (i.e., reduced in kinetic energy) by colliding with

other nuclei within the material. This process of slowing down neutrons is called moderation, and any substance, wet or dry, used for this purpose is called a moderator.

Moderation results from the scattering reactions mentioned previously. When a neutron collides with the nucleus of an atom, the nucleus recoils, taking with it some of the neutron's energy. The neutron then bounces away in a new direction, but with less speed than it had before the collision. Thus, the neutron is moderated or slowed down. Just how much of the neutron's speed is lost in a collision depends on the mass of the nucleus with which it collides.

The presence of an effective moderator can substantially reduce the amount of fissile material needed to achieve critical mass. For example, the critical mass for a solution of plutonium containing 1,000 grams plutonium per liter is approximately 4,500 grams of plutonium. If a sufficient amount of moderator (water) were added to the 1,000 gram/liter solution to create a solution with a concentration of 100 grams/liter, the critical mass would be reduced to approximately 850 grams.

A vessel that contains fissile material may be either over moderated or under moderated. An example of an over-moderated condition is the waste tanks that contain large amounts of water. If additional moderator is added to a condition of overmoderation (e.g., the addition of water to the waste tanks), the additional moderation will have no effect on the k_{eff} of the fissile material.

In a condition of under moderation (e.g., pure, dry plutonium metal bars), any condition that increases moderation or reflection increases the k_{eff} of the fissile material.

Reflection

Because critical mass depends on the neutron leakage rate, the characteristics of the substance surrounding the fissile material must also be considered. If the surroundings deflect escaping neutrons back into the fissile material, then less fissile material is necessary to reach a critical mass.

Consider, again, a bare sphere of Pu-239 metal. Neutrons will escape from the surface of the bare sphere, be lost from the system, and cause no further fissions. If the sphere is surrounded by water, some of the neutrons that leaked out will hit atoms in the water and bounce back into the sphere. These neutrons can then cause fissions.

This process is called reflection, and the substance used is called a reflector. Reflection is caused by the same elastic scattering reaction mentioned for moderators and moderation. A certain number of neutrons leak out of the fissile material, are scattered by atoms in the reflector, and consequently bounce back into the fissile material.

All effective moderators are also effective reflectors, but the reverse is not true. Water, oil, polyethylene, concrete, paraffin, and any other hydrogenous material can make an effective reflector. The human body contains a large amount of water and is also an effective reflector. However, some reflectors are not effective moderators. Lead and U-238 make effective

reflectors, yet they do not slow down neutrons as effectively as water or hydrogenous material. Carbon (graphite) and beryllium, both light metals, are effective neutron moderators and reflectors.

The goal is to avoid accidentally placing a reflector near fissile material. It is also necessary to avoid accidentally immersing a fissile material in a reflector. Placing a sealed container of fissile material into a pool of water will decrease the neutron leakage, because the water reflects some of the leakage neutrons back into the container.

Concentration

The terms "density" and "concentration" belong together when discussing criticality safety of operations (i.e., criticality control). Density refers to the number of fissile atoms within a unit volume of a solid mass. Concentration refers to the number of fissile atoms within a unit volume of a liquid solution. As the density increases, the atoms are packed closer together. Higher densities increase the chance of a neutron causing a fission reaction, because more fissile material is in the same space.

For example, consider different densities of dry homogeneous plutonium oxide (PuO_2), which is a powder. At a density of 2 grams of PuO_2 per cubic centimeter, the critical mass is about 800 kilograms (kg). When the density is increased to 5 grams of PuO_2 per cubic centimeter, the critical mass decreases to about 128 kg. Clearly, changes in density affect critical mass.

As another example, consider a fully reflected plutonium solution in a spherical container (reflection is discussed above.). A sphere containing 20 grams per liter of plutonium solution would require a volume of approximately 30 liters to achieve criticality. If the concentration of the solution were increased to 200 grams per liter, the critical volume would be decreased to approximately 7 liters.

A 9.8 kilogram mass of Pu-239 may be a critical mass if it is a solid sphere of pure Pu-239 metal. However, 9.8 kg of Pu-239 dissolved in a large tank of water may not be a critical mass. Similarly, 1,000 lbm (pound-mass) of natural UO_2 is not a critical mass if the moderator is light water. Natural uranium contains only about 0.7 percent U-235. If the uranium is enriched, however, the concentration of U-235 is increased. A fairly low enrichment will allow 1,000 lbm of UO_2 to achieve criticality.

Simply specifying the mass without also specifying the density or concentration provides only part of the information needed to prevent inadvertent criticality. Materials with low fissile nuclide atomic density (atoms/centimeter^3) are less likely to become critical because the fissile atoms are not packed as closely together.

Increasing the atomic density, or packing the atoms closer together, decreases the amount of material needed to reach critical mass. The higher the concentration or atomic density of fissile material, the greater the chance of a criticality accident. If the concentration or density is high, other parameters must be adjusted to prevent self-sustaining chain reaction.

When a solution boils, the concentration increases as the liquid vaporizes, leaving the solids behind. Increasing the concentration of a dissolved fissile material could cause a criticality accident.

The following is taken from LANL, Nuclear Science Self-Study Guide and R. Knief, *Nuclear Criticality Safety: Theory and Practice.*

Volume

The volume of fissile material is controlled in much the same way as mass. Because fissile material is frequently stored in solution, a certain volume of fissile material may correspond to an equivalent critical mass. Containers of limited volume are used to ensure that the accumulation of fissile material solutions does not approach a condition of criticality. In areas such as gloveboxes where an accumulation of fissile solutions presents a potential criticality hazard, criticality drains are typically used. Criticality drains allow solutions produced by process equipment malfunction to accumulate to a predetermined depth. Once maximum allowed depth is reached, solutions will flow out of the criticality drain and onto the process area floor or, in some cases, an engineered collection system.

Volume is usually controlled in conjunction with other criticality control parameters, such as concentration and geometry. Batch processing limits, for example, often employ mass or volume limits that depend upon the fissile composition, enrichment, and physical form of the material. Thus, control of fissile material in terms of mass or volume depends on robust administrative practices that are augmented by non-favorable (to fission) geometry in container designs. This is especially important to concerns over having solutions in non-favorable geometry containers that lead to leak collection as described above.

Density

Refer to the discussion under “Concentration” for information related to density.

The following definitions are taken from LANL, Nuclear Science Self-Study Guide.

Neutron Absorbers

Neutron absorbers are also known as absorption. Certain isotopes readily absorb neutrons. Once absorbed, these neutrons cannot cause further fissions. Such materials, called neutron poisons, are used to decrease the neutron population. A neutron poison is a material that absorbs neutrons without causing fission. Although all materials absorb neutrons to some extent, the word “poison” is used for materials that strongly absorb neutrons. Water, for example, is not considered a poison. Poisons remove neutrons from the chain reaction. One example of a poison is boron. About 20 percent of natural boron is the isotope B-10. Boron-10 is the isotope of boron that is a poison. The neutron absorption reaction for B-10 is

$$^{10}_{5}\mathrm{B} + {}^{1}_{0}\mathrm{n} \rightarrow {}^{7}_{3}\mathrm{Li} + {}^{4}_{2}\mathrm{He}$$

This reaction has a very high probability of occurring, and if B-10 is placed in fissile material, it is an effective poison. The more neutrons absorbed in a poison, the fewer

neutrons are available for absorption in fissile atoms. When sufficient neutron poison material is added to fissile material, enough neutrons are captured (absorbed) to prevent a criticality accident.

For example, poisons in waste tanks effectively allow a larger amount of fissile solution to be stored safely without becoming critical. Poisons that are found in the waste tanks are primarily iron (Fe), manganese (Mn), nickel (Ni), chromium (Cr), and sodium (Na).

The following examples illustrate neutron absorption reactions for Fe-56, Mn-55, and Ni-58:

$$^{56}_{26}\mathrm{Fe} + {}^{1}_{0}\mathrm{n} \rightarrow {}^{57}_{26}\mathrm{Fe}\ \text{(stable)}$$

$$^{55}_{25}\mathrm{Mn} + {}^{1}_{0}\mathrm{n} \rightarrow {}^{56}_{25}\mathrm{Mn} \xrightarrow[\text{2.578 hrs.}]{\beta^-} {}^{56}_{26}\mathrm{Fe}\ \text{(stable)}$$

$$^{58}_{28}\mathrm{Ni} + {}^{1}_{0}\mathrm{n} \rightarrow {}^{59}_{28}\mathrm{Ni} \xrightarrow[\text{7.6E4 yrs.}]{\varepsilon} {}^{59}_{27}\mathrm{Co}\ \text{(stable)}$$

The second reaction proceeds to stability by beta minus decay (β^-). The third reaction proceeds to stability by electron capture (Є).

Heterogeneity

Heterogeneity is also known as intermixing. When working with uranium or plutonium suspended in a chemical solution, it is common for the chemicals to separate, similar to the way oil and water do. This can prove (and has proved) to be dangerous if there is enough fissile material in the suspension that could concentrate and reach critical mass. It is important to be aware that some chemicals separate from solution, unless the mixture is kept well stirred. This information is vital because accidents can and have happened due to separation of solution.

Heterogeneity and enrichment are discussed together due to the resonance capture effect. Heterogeneous systems can be made critical with lower masses than similar homogeneous systems.

The following is taken from LANL, Nuclear Science Self-Study Guide and the Bureau of Radiological Health and the Training Institute, *Radiological Health Handbook.*

Enrichment

This is the process by which material in which the relative amount of one or more isotopes of a constituent has been increased. For example, uranium that has been processed to raise the concentration of uranium-235 is referred to as enriched uranium. All other things being equal, increasing the relative amount of a fissile isotope such as uranium-235 above its normal abundance in a material such as naturally occurring uranium, will lower the mass necessary to achieve criticality compared with uranium with a natural abundance of

uranium-235. Enrichment as a criticality control parameter must be managed with respect to other parameters such as concentration and density

b. Discuss the influence of the presence of non-fissionable materials mixed with, or in contact with, fissionable material on nuclear criticality safety.

[Note: This KSA should have used the term "fissile" in place of "fissionable."]

In general, nuclear criticality safety is concerned with fissile material, i.e., isotopes that can be fissioned by neutrons of any energy including thermal neutrons. Fissionable isotopes can be fissioned only by high energy neutrons.

Refer to the discussion on moderation, heterogeneity, and reflection for more information.

c. Discuss the concept of contingencies for checking the validity of criticality Safety Limits (SL).

The following is taken from DOE-STD-1134-99.

Appendix A of ANSI/ANS-8.1 (American National Standards Institute/American Nuclear Society) contains a list of typical scenarios to consider when reviewing the contingency analysis for a particular evaluation. The reviewer must be familiar with the operation being evaluated to perform an adequate review. Without such knowledge, no decision can be made relative to whether postulated abnormal events are anticipated, unlikely, or incredible, or if any credible contingencies have been omitted.

Each contingency that could lead to criticality should be shown to be unlikely, independent, and non-concurrent with other contingencies that could lead to criticality. If this can not be done, then the contingency under evaluation becomes part of the normal operating conditions, i.e., an anticipated event.

Two simplifications are possible here. Criticality scenarios that are deemed incredible and those that are not physically possible need no contingency analysis. The reviewer's task in each of these two cases is to decide whether the arguments against criticality occurring are sound. The reviewer should take care to note the definition of contingency and credible in DOE-STD-3007-2007. If a quantitative probabilistic risk assessment is utilized in the critical safety evaluation despite the qualitative definition of "credible," the reviewer should rigorously scrutinize any calculations and assumptions leading to extremely small probabilities. In the more likely situation, the experienced, professional judgment of engineering and operational personnel will be the basis for this argument. The bases for these judgments should be carefully documented in the nuclear criticality safety (NCS) evaluation. The reviewer's task is to verify that the bases (assumptions and conditions) for the experts' judgment are reflected, as appropriate, in the NCS limits and requirements for NCS controls.

In other cases, where criticality is possible, the reviewer's task is to assure that no credible single failure can result in the potential for a criticality accident. To accomplish this, all credible failure modes known to the reviewer that are applicable to the process should be

bounded by the analysis, or adequate barriers to its occurrence must be in place. The reviewer should ask, "How bad can the situation credibly get? If it gets that bad, will it remain subcritical?" and ensure that the documented contingency analysis considers the scenario. This contingency discussion must contain a clear description of the process upsets (i.e., contingencies) considered by the NCS analyst. The contingencies should be specific enough to provide a definitive boundary to the process upset. For example, rather than stating a mass contingency as "overbatch," state "double batching" if this has been determined to be the maximum credible overbatch. The former means any overbatch no matter how small would have to be an "unlikely" event. The latter concludes that while a small overbatch would be an "anticipated" event, double-batching would be an "unlikely" event. The reviewer need not document all conceivable abnormal pathways or scenarios, only those deemed reasonable and credible.

d. Define the following terms:
- **Criticality accident**
- **Minimum accident of concern**
- **Process area**

The following definitions are taken from DOE G 421.1-1 and ANS 8.3.

Criticality Accident

A criticality accident is the release of energy as the result of accidentally producing a self-sustaining or divergent fission chain reaction.

Minimum Accident of Concern

The term "minimum accident of concern" refers to the smallest accident a criticality alarm system is required to detect. A criticality accident such as this would produce approximately 10^{12} fissions in its first minute and provide an absorbed dose in free air of 20 rad at 2 meters if no significant shielding were present.

Process Area

A process area is any area involved in the chemical processing, mechanical processing, handling, or storage of fissionable materials.

e. Discuss the general principles associated with the use of criticality alarm systems, including the following:
- **Installation**
- **Coverage**
- **Detection**
- **Alarms**
- **Dependability**

The following is taken from DOE G 421.1-1 and ANS 8.3.

Installation and Coverage

The number of detectors must be adequate enough to detect the minimum accident of concern anywhere in the fissionable material handling area of concern or under consideration and to alarm. The design must be robust enough to survive up to the design basis accident (DBA).

Detection

The system must detect and respond to the minimum accident of concern within ½ second (sec).

Alarms

The alarm signal must be unique to a criticality accident, uniform for the site, and for immediate evacuation only.

Dependability

The alarm system must be adequately reliable and sensitive to detect the minimum accident of concern, but only minimally subject to false alarms. Protection against component failure, power failure, or other common challenges to operability should be factored into the design.

f. Describe the use of neutron poisons.

According to DOE G 421.1-1, neutron poisons, such as cadmium, boron, and gadolinium, may be used to maintain equipment and processes subcritical, provided measured data or validated computational results confirm the effectiveness of the neutron poison and ensure its presence and reliability.

g. Define the following terms:

- **Burnable poison**
- **Non-burnable poison**
- **Chemical shim**

The following definitions are taken from DOE-HDBK-1019/2-93.

Burnable Poison

A burnable neutron poison is a material that has a high neutron absorption cross section that is converted into a material of relatively low absorption cross section as the result of neutron absorption.

Non-burnable Poison

A non-burnable neutron poison is a material that has relatively constant neutron absorption characteristics over core life. The absorption of a neutron by one isotope in the material produces another isotope that also has a high absorption cross section.

Chemical Shim

Chemical shim is a soluble neutron poison that is circulated in the coolant during normal operation.

h. Explain the purpose and use of Raschig Rings as a neutron poison.

According to DOE G 421.1-1, Raschig rings may be used to render otherwise geometrically unsafe vessels favorable depending on fissionable material concentration and packing density of the rings. Typical applications of Raschig rings include sumps, evaporator de-entrainment separator heads, large tanks, and scale pits. Packing density of the rings should not be overestimated when calculating the nuclear criticality safety of a vessel. Ring settling and boron leaching may also present problems. The detailed requirements for the use of borosilicate-glass Raschig rings are found in ANSI/ANS-8.5-1986.

4. Nuclear safety specialists shall demonstrate a working level knowledge of terminology used in nuclear safety analysis.

a. Define the following accident related terms:

- **Accident**
- **Authorization basis**
- **Beyond design basis accident**
- **Design basis**
- **Design basis accidents**
- **Evaluation guideline**
- **Safety basis**
- **Safety analysis**
- **Consequence**
- **Frequency**
- **Risk**
- **External event**
- **Internal event**

Accident

According to DOE-STD-3009-94, an accident is an unplanned sequence of events that results in undesirable consequences.

Authorization Basis

According to DOE G 450.4-1B, the authorization basis consists of safety documentation that supports the decision to allow a process or facility to operate. Included are corporate operational and environmental requirements as found in regulations and specific permits, and, for specific activities, work packages, or job safety analyses.

Beyond Design Basis Accident

Beyond design basis accident is an accident of the same type as a design basis accident (e.g., fire, earthquake, spill, explosion, etc.), but that is defined by parameters that exceed in

severity the parameters defined for the design basis accident. The same correlation applies to beyond derivative design basis accidents with regard to derivative design basis accidents.

Design Basis

According to DOE-STD-3009-94, the design basis is the set of requirements that bound the design of systems, structures, and components within the facility. These design requirements include consideration of safety, plant availability, efficiency, reliability, and maintainability. Some aspects of the design basis are important to safety, others are not.

Design Basis Accident

According to DOE G 420.1-1, a design basis accident is an accident postulated for the purpose of establishing functional and performance requirements for safety structures, systems, and components (SSCs).

Evaluation Guideline

DOE-STD-3009-94 states that the evaluation guideline (EG) is the radiation dose value against which the safety analysis is evaluated. Offsite EGs are established for the purpose of identifying and evaluating safety-class (SC) SSCs.

Safety Basis

According to 10 CFR 830, safety basis is the documented safety analysis (DSA) and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely in a manner that adequately protects workers, the public, and the environment.

Safety Analysis

According to DOE-STD-3009-94, a safety analysis is a documented process to provide systematic identification of hazards within a given DOE operation; to describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and to analyze and evaluate potential accidents and their associated risks.

The following definitions are taken from DOE-STD-3009-94.

Consequence

Consequence is the effect on a member of the public, a worker, or the environment, resulting from exposure to a hazard.

Frequency

Frequency is the expected number of occurrences of a hazardous scenario, generally expressed as an annual likelihood of occurrence. Frequency is typically determined by considering a combination of applicable factors such as the initiating event likelihood per year, failure probabilities of enabling events, number of repetitive operations over time, and percentage of time the hazardous material is present.

Risk

Risk is the quantitative or qualitative expression of possible loss; the expression considers both the probability that an event will occur and the consequences of that event.

External Event

An external event is an accident-initiating event outside the facility and not associated with facility operations. In a DSA, the term "external event" normally refers only to a human-initiated event, such as a traffic accident, an accident at an adjacent facility, a utility accident, an airplane crash, or wildfire (whether initiated by humans or not). Events caused by natural phenomena hazards (NPHs,) such as earthquakes, tornados, high winds, lightning, and flooding, are external events but are generally classified as "natural events" or "NPH events" in a DSA.

Internal Event

An internal event is an accident-initiating event associated with facility operations. Examples include operator error and equipment failure. In a DSA, internal events generally lead to operational accidents such as spills/chemical releases, fires, explosions, and criticality events.

b. Define the following hazard-related terms:

- **Hazard**
- **Hazard categorization**
- **Hazard Category 1**
- **Hazard Category 2**
- **Hazard Category 3**
- **Hazardous material**

Hazard

According to 10 CFR 830.3, a hazard is a source of danger (e.g., 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).

Hazard Categorization

According to DOE-STD-3009-94, hazard categorization is the evaluation of the consequences of unmitigated releases in order to categorize facilities or operations into one of three hazard categories. DOE-STD-1027-92 provides guidance and radiological threshold values for determining the hazard category of a facility.

Hazard Categories 1, 2, and 3

According to DOE-STD-3009-94, evaluation of the consequences of unmitigated releases to categorize facilities or operations fall into the following hazard categories:

- Hazard category 1—The hazard analysis shows the potential for significant offsite consequences.
- Hazard category 2—The hazard analysis shows the potential for significant onsite consequences.

- Hazard category 3—The hazard analysis shows the potential for only significant localized consequences.

Hazardous Material

According to DOE-STD-3009-94, hazardous material is any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health.

Candidate hazards include radioactive materials, hazardous chemicals as defined by the Occupational Health and Safety Administration (OSHA) in 29 CFR 1910.1200 and 29 CFR 1910.1450; any material assigned a reportable quantity value in 40 CFR 302, table 302.4; threshold planning quantities in 40 CFR 355, appendix A; threshold planning quantities in 29 CFR 1910.119; level of concern quantities in the U. S. Environmental Protection Agency's (EPA's) *Technical Guidance for Hazards Analysis: Emergency Planning for Extremely Hazardous Substances*; or materials rated as 3 or 4 in National Fire Protection Association (NFPA) 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response*.

c. Define the following safety control related terms:
- **Limiting Conditions for Operations (LCO)**
- **Limiting control settings**
- **SL**
- **Specific Administrative Control (SAC)**
- **Administrative Control (AC)**

The following definitions are taken from 10 CFR 830 and DOE G 423.1-1.

Limiting Conditions for Operations (LCOs)

LCOs define the limits that represent the lowest functional capability or performance level of safety SSCs required to perform an activity safely.

LCOs should include the initial conditions for those DBA or transient analyses that involve the assumed failure of, or present a challenge to, the integrity of the primary radioactive material barrier. Identification of these variables should come from a search of each transient and accident analysis documented in the DSA. The LCO should be established at a level that will ensure the process variable is not less conservative during actual operation than was assumed in the safety analyses.

LCOs should also include those SSCs that are part of the primary success path of a safety sequence analysis, and those support and actuation systems necessary for them to function successfully. Support equipment for these SSCs would normally be considered to be part of the LCO if relied upon to support the SSCs' function.

Limiting Control Settings

Limiting control settings define the settings on safety systems that control process variables to prevent exceeding an SL.

Limiting control settings for reactors should include reactor trip system instrumentation set points. The reactor trip set-point limits are the nominal values at which the reactor trips are set and should be selected to provide sufficient allowances between the trip set point and the SL. This allowance will ensure the core and the reactor coolant systems are prevented from exceeding SLs during normal operation and anticipated operational occurrences.

Limiting control settings of instruments that monitor process variables at nonreactor nuclear facilities are the settings that either initiate protective devices themselves or sound an alarm to alert facility personnel to take action to protect barriers that prevent the uncontrolled release of radioactive materials. A limiting control setting is only specified for a variable that also protects an SL. Limiting control settings should be chosen so that there is adequate time after exceeding the setting to correct the abnormal situation, automatically or manually, before an SL is exceeded.

SL

SLs are the limits on process variables associated with those SC physical barriers, generally passive, that are necessary for the intended facility function and that are required to guard against the uncontrolled release of radioactive materials.

Specific Administrative Control (SAC)

According to DOE-STD-3009-94, an SAC is an AC identified in the DSA as a control needed to prevent or mitigate an accident scenario and having a safety function that would be safety-significant (SS) or SC if the function were provided by an SSC.

Administrative Control (ACs)

According to DOE G 423.1-1, ACs are the provisions relating to organization and management, procedures, record keeping, reviews, and audits necessary to ensure safe operation of the facility. ACs may include reporting deviations from technical safety requirements (TSRs) (i.e., exceeding LCOs, limiting control settings , or surveillance requirements [SRs], or violation of a TSR), staffing requirements for facility positions important to safe operation of the facility, ACs of the criticality safety program, and commitments to safety management programs important to worker safety.

d. Differentiate between the following categories of individuals who may be affected by an accident at a Department nuclear facility:
- **Off-site individual**
- **On-site individual**
- **Public**
- **Worker (including collocated worker)**

Off-Site Individual

An offsite individual is any member of the public or any other individual who may not be normally assigned to or located within the subject site boundaries, and therefore unlikely to be trained on site-specific hazards. The offsite area comprises the area beyond the site boundaries.

On-Site Individual

An onsite individual is any member of the public or any other individual who may be normally or temporarily located within the subject site boundaries. This individual may not be trained on the presence of site-specific hazards. The onsite area includes any area that has been established as a National Defense Area or National Security Area.

Public

Title 10 CFR 835 defines a member of the public as an individual who is not a general employee. An individual is not a "member of the public" during any period in which the individual receives an occupational dose.

Worker (Including Collocated Worker)

Title 10 CFR 835 defines a radiological worker as a general employee whose job assignment involves operation of radiation producing devices or working with radioactive materials, or who is likely to be routinely occupationally exposed above 0.1 rem (0.001 Sv) per year total effective dose.

e. Differentiate between the function of SSCs in the following classifications:

- **Safety-Class Structures, Systems, and Components (SC-SSC)**
- **Safety-Significant Structures, Systems, and Components (SS-SSC)**
- **Defense-in-Depth (DID)/important to safety**

The following definitions are taken from DOE-STD-3009-94.

Safety-Class Structures, Systems, and Components (SC-SSC)

Safety-class structures, systems, and components are related to public protection and are defined by comparison with the numerical EG.

Safety-Significant Structures, Systems, and Components (SS-SSC)

Safety-significant structures, systems, and components are identified for specific aspects of defense in depth and worker safety as determined by the hazard analysis.

Defense-in-Depth (DID)/Important to Safety

Defense-in-depth/important to safety refers to equipment and administrative features providing preventive or mitigative functions so that multiple features are relied on for prevention or mitigation to a degree proportional to the hazard potential, and to integrated safety management (ISM) programs that control and discipline operation.

f. Differentiate between the function and contents of the following documents:

- **DSA**
- **Preliminary Documented Safety Analysis (PDSA)**
- **Safety Analysis Report (SAR)**
- **Basis for Interim Operation (BIO)**
- **TSR**
- **Preliminary Hazards Analysis (PHA)**

DSA

The following is taken from DOE G 421.1-2.

The DSA for hazard category 1, 2, or 3 nuclear facilities must, as appropriate for the complexities and hazards associated with the facility or activity

- describe the facility, activities, and operations, including the design of safety SSCs and the work to be performed;
- provide a systematic identification of natural and man-made hazards associated with the facility;
- evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility;
- derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining them current at all times and controlling their use;
- define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) quality assurance (QA), procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection; and
- with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a criticality safety program (CSP) that—
  (a) ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions,
  (b) identifies applicable nuclear criticality safety standards, and describes how the program meets applicable nuclear criticality safety standards.

The preparation of DSAs must conform to one of the methodologies set forth in table 2 of appendix A of 10 CFR 830 or an alternate methodology approved by DOE. These methodologies are called “safe harbors” in 10 CFR 830.

Preliminary Documented Safety Analysis (PDSA)

The following is taken from DOE G 421.1-2.

Development of a PDSA is the process whereby facility hazards are identified, controls to prevent and mitigate potential accidents involving those hazards are proposed, and commitments are made for design, construction, operation, and disposition so as to assure adequate safety at DOE nuclear facilities. DOE, in its review and approval role, may require modification or addition to these commitments by the responsible contractor. Throughout the life of the facility, from design and construction to mission-oriented operations, through deactivation, long-term surveillance and maintenance, to decontamination and

decommissioning, there must be a safety basis in place that is appropriate to the activities (operations) occurring during each of those phases.

During design and construction, the governing safety basis document is the PDSA. It is updated as the design matures and is approved prior to procurement and construction activities. Until approval, the PDSA and its updates serve to keep DOE informed as to how DOE nuclear safety design criteria are being addressed in the design. Project design reviews provide the vehicle by which safety-related changes are reviewed and DOE can provide guidance to the contractor. Prior to operations, the PDSA evolves to a final DSA that reflects the facility as actually constructed.

Safety Analysis Report (SAR)

According to DOE G 420.1-1, a SAR is 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.

Basis for Interim Operation (BIO)

According to DOE G 421.1-2, there are primarily two cases where 10 CFR 830 allows BIOs to be used as the appropriate safety basis documentation: (1) for short-lived activities and (2) during transition phases, including transition surveillance and maintenance, deactivation, and decontamination and decommissioning. A BIO is applicable to a nuclear facility in transition as the facility moves through the appropriate life-cycle states, providing accurate safety documentation for rapidly changing activities. A BIO can also be linked to a series of tasks or activities.

TSR

According to DOE G 423.1-1, TSRs define the performance requirements of SSCs and identify the safety management programs used by personnel to ensure safety. TSRs are aimed at confirming that SSCs and personnel can perform their intended safety functions under normal, abnormal, and accident conditions. These requirements are identified through hazard analysis of the activities to be performed and identification of the potential sources of safety issues. Safety analyses to identify and analyze a set of bounding accidents that take into account all potential causes of releases of radioactivity also contribute to development of TSRs.

Preliminary Hazards Analysis (PHA)

The following is taken from DOE G 440.1-8.

"Preliminary hazard analysis" has a specific meaning in DOE O 413.3A and DOE-STD-1189-2008, which provides implementation guidance for nuclear facility safety requirements for facilities rated at certain hazard categories. "Preliminary hazard analysis" also has a more general meaning when it is used for non-nuclear worker safety and health hazard analysis. The various uses of this term all follow the same basic principles and are therefore compatible.

PHAs provide a broad hazard-screening tool that includes a review of the types of operations that will be performed in the proposed facility and identifies the hazards associated with these types of operations and facilities. The results of the PHA are used to determine the need for additional, more detailed analysis, serve as a precursor documenting that further analysis is deemed necessary, and serve as a baseline hazard analysis where further analysis is not indicated. The PHA is most applicable in the conceptual design stage, but it is also useful for existing facilities and equipment that have not had an adequate baseline hazard analysis.

PHAs are detailed studies to identify and analyze potential hazards associated with each aspect of the facility and related equipment and operations. The analysis should include a systematic review of each facility component and task and should consider

- facility design characteristics such as electrical installations, platform heights, egress concerns, etc.;
- proposed equipment, including types of equipment, location of equipment relative to the other operations and workers, required equipment interfaces, etc.;
- proposed operations, including related hazardous substances and potential exposures, potential energy sources, locations of operations and required interfaces, resulting material and personnel traffic patterns, etc.; and
- facility and equipment maintenance requirements, including confined space concerns, electrical hazards, and inadvertent equipment startup or operations hazards.

g. Differentiate between the controls which have the following designations:

- **Mitigating controls**
- **Preventive controls**
- **AC**
- **SAC**
- **Design features**
- **Passive controls**
- **Active controls**
- **Safety SSCs**
- **Controls that provide confinement**
- **Controls that provide containment**

The following definitions are taken from DOE-STD-3009-94.

Mitigating Controls

Mitigating controls are any SSCs that serve to mitigate the consequences of a release of hazardous materials in an accident scenario; they can be a passive or active features or controls.

Preventive Controls

Preventive controls are any SSCs that serve to prevent the release of hazardous material in an accident scenario; they can be passive or active features or controls.

AC

According to DOE G 423.1-1, ACs are the provisions relating to organization and management, procedures, record keeping, reviews, and audits necessary to ensure safe operation of the facility. ACs may include reporting deviations from TSRs (i.e., exceeding LCOs, limiting control settings , or SRs, or violation of a TSR), staffing requirements for facility positions important to safe operation of the facility, ACs of the criticality safety program, and commitments to safety management programs important to worker safety.

SAC

According to DOE-STD-1186-2004, SACs are ACs that are selected to provide preventive and/or mitigative functions for specific potential accident scenarios, and that also have safety importance equivalent to engineered controls that would be classified as SC or SS if the engineered controls were available and selected.

Design Features

According to 10 CFR 830, design features are the features of a nuclear facility specified in the TSRs that if altered or modified would have a significant effect on safe operation.

The following definitions are taken from DOE G 423.1-1.

Passive Controls

Passive controls are normally passive characteristics of the facility that are not subject to change by operations personnel, e.g., shielding, structural walls, relative locations of major components, installed poisons, or special materials.

Active Controls

Active controls are normally described in the DSA and are the subject of the various TSRs; they are not normally described in the design features section. All changes or modifications that impact the safety basis of the facility are subject to the unreviewed safety question (USQ) process. The design features section captures those permanently built-in features critical to safety that do not require, or infrequently require, maintenance or surveillance.

The following definitions are taken from DOE G 420.1-1.

Safety SSCs

A computational construct using the concepts of an unmitigated accident release and an EG has been developed to aid in the designation of SC SSCs. The process uses the same initiating events as identified in the hazard and accident analyses discussed in section 2.1 of DOE G 420.1-1, but for the purposes of showing which SSCs are sufficiently important to classify as SC, 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 EG, 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 SC.

These analyses and evaluations should be retained as backup information to support the designations of SC SSCs.

Controls That Provide Confinement

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 SC 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 a DBA and to retain collected radioactive and hazardous materials after the accident.

Controls That Provide Containment

In some cases safety SSCs rely on supporting SSCs to perform their intended safety function.

These support SSCs may be classified as SC or SS SSCs. For example, a safety-class designation may be appropriate for an instrumentation and control system that supports a tritium containment system if it can be demonstrated that failure of the instrumentation and control support system can lead to either failure or reduced availability of the SC containment barrier. In general, the following classification criteria apply:

- Support SSCs to safety-class SSCs must be classified as SC 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 SS 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 SS.

Priority of Controls

Prioritization of items for a facility safety strategy is as follows:

- Minimization of hazardous materials (material at risk [MAR]) is the first priority.
- Safety SSCs are preferred over ACs.
- 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 workers and the public.
- Controls that are effective for multiple hazards can be resource effective.

h. Differentiate between the following types of facilities:

- **Nuclear facility**
- **Category A nuclear reactor**

- **Category B nuclear reactor**
- **Non-reactor nuclear facility**
- **Radiological (below Hazard Category 3 nuclear facility)**

The following definitions are taken from DOE Order 5480.30.

Nuclear Facility

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

Category A Nuclear Reactor

Category A reactor facilities are those production, test, and research reactors designated by DOE based on power level (e.g., design thermal power rating of 20 megawatts steady state and higher), potential fission product inventory, and experimental capability.

Category B Nuclear Reactor

Category B reactor facilities are those test and research reactors designated by DOE based on power level (e.g., design thermal power rating of less than 20 megawatts steady state), potential fission product inventory, and experimental capability.

Non-reactor Nuclear Facility

10 CFR 830 defines non-reactor nuclear facilities as 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 to workers, the public, or the environment potentially exists. This definition does not include accelerators and their operations. It does not include activities involving only incidental use and generation of radioactive materials or radiation such as check and calibration sources in research, experimental, and analytical laboratory activities, electron microscopes, and x-ray machines.

Radiological (below Hazard Category 3 Nuclear Facility)

Title 10 CFR 830 defines radiological facilities as those facilities that cannot have a significant radiological impact outside the facility. Radiological facilities are therefore exempt from the preparation of a SAR/DSA pursuant to 10 CFR 830.

i. Differentiate between the following chemical terms:

- **Acute Exposure Guideline Level (AEGL)-1**
- **AEGL-2**
- **AEGL-3**
- **Emergency Response Planning Guide (ERPG)-1**
- **ERPG-2**
- **ERPG-3**
- **Temporary Emergency Exposure Limit (TEEL)-1**
- **TEEL-2**
- **TEEL-3**

The following definitions are taken from EPA, *Acute Exposure Guideline Levels*.

Acute Exposure Guideline Level (AEGL)-1

AEGL-1 is the airborne concentration (expressed as parts per million or milligrams per cubic meter [ppm or mg/m^3]) of a substance above which it is predicted that the general population, including susceptible individuals, could experience notable discomfort, irritation, or certain asymptomatic nonsensory effects. However, the effects are not disabling and are transient and reversible upon cessation of exposure.

AEGL-2

AEGL-2 is the airborne concentration (expressed as ppm or mg/m^3) of a substance above which it is predicted that the general population, including susceptible individuals, could experience irreversible or other serious, long-lasting adverse health effects or an impaired ability to escape.

AEGL-3

AEGL-3 is the airborne concentration (expressed as ppm or mg/m^3) of a substance above which it is predicted that the general population, including susceptible individuals, could experience life-threatening health effects or death.

The following definitions are taken from American Industrial Hygiene Association, *Emergency Response Planning Guidelines*.

Emergency Response Planning Guide (ERPG)-1

The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hour without experiencing other than mild, transient, adverse health effects or without perceiving a clearly defined objectionable odor.

ERGP-2

The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hour without experiencing or developing irreversible or other serious health effects or symptoms which could impair an individuals ability to take protective action.

ERGP-3

The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 hour without experiencing or developing life-threatening health effects.

The following definitions are taken from DOE Office of Health, Safety, and Security (HSS), Protective Action Criteria (PAC) with AEGLs, ERPGs, & TEELs: Rev. 23 for Chemicals of Concern Web site.

Temporary Emergency Exposure Limit (TEEL)-1

TEEL-0 is the threshold concentration below which most people will experience no adverse health effects.

TEEL-1 is the same as ERPG-1 (with the exception of the recommended averaging time).

TEEL-2

TEEL-2 is the same as ERPG-2 (with the exception of the recommended averaging time).

TEEL-3

TEEL-3 is the same as ERPG-3 (with the exception of the recommended averaging time).

TEELs are intended for use until AEGLs or ERPGs are adopted for chemicals.

j. Identify the types of chemical or toxicological hazards that may be found in nuclear facilities.

Any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health is considered a hazard. Such materials, including radioactive materials, are defined in 29 CFR 1910.1200 and 29 CFR 1910.1450; reportable quantities pursuant to 40 CFR 302; threshold planning quantities pursuant to 40 CFR 355, appendix A; threshold planning quantities per 29 CFR 1910.119; level of concern quantities in the EPA's *Technical Guidance for Hazards Analysis: Emergency Planning for Extremely Hazardous Substances*; and materials rated as 3 or 4 in NFPA 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response*.

5. Nuclear safety specialists shall demonstrate a working level knowledge of the principal hazard and accident analysis methods.

a. Identify and discuss the use of different methods for qualitative hazard analysis. Identify specific strengths and weaknesses with the various methods.

DOE-STD-3009-94 references *Guidelines for Hazard Evaluation Procedures* (1992) published by the American Institute of Chemical Engineers. This text is a generally accepted industrial standard for hazard analysis methods. DOE has also published some specific references of its own, such as DOE/EH-0340, September 1993, *Example Process Hazard Analysis of a Department of Energy Water Chlorination Process;* DOE-HDBK-1100-2004, *Chemical Process Hazards Analysis*; and DOE-HDBK-1101-2004, *Process Safety Management for Highly Hazardous Chemicals*. It is important to remember that there is no one correct way to perform a hazard analysis, and some DOE sites may have their own methodologies that are simply adaptations of standard techniques.

Hazard evaluation methods differ in appropriateness depending on the types and complexity of operations being examined. Checklists, process hazard analyses, or "what if" approaches

are generally used on simpler or well-understood systems and operations. Where operations are routine and familiar, hazard analysis team members can identify issues of concern from their own first-hand experience and knowledge. When a specific subject assumes sufficient complexity that a number of distinct subcomponent failures need to be characterized, a failure modes and effects analysis (FMEA) is often used to ensure completeness. The FMEA is particularly appropriate for systems when hardware failure modes are of more interest than human error. The hazard and operability study (HAZOP) method is designed for the systematic examination of a facility or operation of such complexity as to cast doubt on the effectiveness of simple inspection or general knowledge to expose all potential issues of concern. This method requires the team to go through a predefined set of detailed considerations based on guide words such as "more, less, and the same as" for parameters such as "flow, temperature, and pressure."

The preceding paragraph's brief discussion is general. Selection of an appropriate method, or a combination of methods, for hazard analysis is not a decision made in isolation; many factors bear on that decision, not the least of which is the previous experience of the team leader and the team itself. Judgments of appropriateness are often less a question of actual technique than of the attitude and effort put into use of that technique. For example, a well structured "What-If" that covers an operation systematically, with thorough identification of preventive and mitigative features, is preferable to a shallow HAZOP undertaken merely as an exercise to satisfy requirements. The former would likely be acceptable, whereas the latter would not.

A DSA hazard evaluation must be performed by a team that meets as a group to examine facilities and operations. The team should include an experienced leader; a scribe to record team discussions; one or more persons with safety knowledge and experience relevant to the operations being examined; one or more persons familiar with the facility design and the types of operations being examined; and operations staff. The hazard evaluation should not be performed entirely by subcontractors with no first-hand experience in the facility's operation. If facility operations' personnel are not included on the team, the hazard analysis will typically be generic at best.

b. Discuss methods used to categorize and bin hazardous conditions associated with nuclear safety analysis.

DOE Order 5480.23, *Nuclear Safety Analysis Reports,* established a requirement to categorize nuclear facilities and their operations based on whether or not potential consequences were deemed significant offsite (category 1 hazard), significant only onsite (category 2 hazard), or significant only in the immediate locality (category 3 hazard). When implementation across sites throughout the United States produced multiple interpretations of "significant," DOE issued DOE-STD-1027-92 to provide for uniform categorization.

DOE-STD-1027-92 restricts the category 1 hazard definition to class A reactors or any facility/operation with a similar consequence profile as determined by DOE Headquarters. It also contains two tables of radionuclide mass limits generated to serve as category 2 and category 3 threshold values. The category 2 thresholds are based on applying an overall

building release fraction to the entire operational inventory to determine what amount of material would produce a 1 rem exposure at a specified distance. The dispersion parameter assigned in this calculation is a Chi/Q value of 1.0×10^{-4} sec/m^3. That translates into a distance of roughly 300 meters for average meteorology (condition D with a wind speed of 4.5 m/sec, per DOE-STD-1027-92). Exceeding minimum critical mass quantities for any radionuclide also results in category 2 designation, regardless of what quantity threshold the aforementioned calculation derives for the given radionuclide. A similar calculation, based on 10 rem at 30 m, is used to determine the category 3 thresholds.

The intent of DOE-STD-1027-92 was to remove hazard categorization as an issue of contention. At most sites, the determination is now a simple formality, although DOE does allow operations management to present rationales for lowering the assigned categorization. These are typically based on arguments as to why a given inventory is not vulnerable, or, in cases such as environmental restoration sites, that the inventory is so dispersed as to render it inconceivable that any accident could affect more than a small fraction of the total material present.

Hazard Identification

The following is taken from DOE-HDBK-3010-94 and DOE G 421.1-X (draft).

Any hazard analysis should begin with a basic review of the quantities of hazardous materials and energy sources involved in the activity being assessed. A DSA must include a summary table of the hazards for the facility. This summary contains an identification of each hazard (e.g., plutonium-239, chlorine gas, thermal energy), its form (e.g., powder, liquid, solid), the type of hazard (e.g., radiological, toxicological, explosive), location, quantity, and any unusual storage conditions (e.g., refrigerated to 25 ºF) or hazardous interaction potentials, most commonly between chemicals used or stored in proximity to a given process.

The hazard identification should cover all the activities discussed in the facility description. In the same sense, the hazard and accident analyses and their associated text make assumptions about material quantities that are expected to correlate with the hazard identification. A basic logic must be employed to systematically identify quantities of hazardous material or energy sources. For example, assessments of specific operations will typically use flow sheet parameters or administrative limits to assign quantities. In some cases, nuclear criticality limits are used, although these may be excessively conservative depending on how the calculated limits correlate to actual operating practice. It would be inappropriate, however, to randomly mix and match flow sheet and criticality limit parameters.

The following table provides an example hazard identification table from DOE-HDBK-3010-94. As can be seen from this example, clarity of presentation and comprehensiveness are the main goals. While tools such as chemical interaction matrixes and generic hazard-type checklists may be used to guide generation of such a table, the methodologies involved in hazard identification are typically minimal, as it is largely a fact-collecting exercise.

Table 2. Example hazard identification

Location	Hazard	Quantity
Ion exchange glovebox	1. Plutonium 2. 35 percent nitric acid 3. Chemical energy 4. Thermal energy 5. Potential energy 6. Kinetic energy	1. Procedural limit is 6,500 g Pu in nitrate feed solution into the box (5–6 g/L) or sorbed on resin. Normal run is ≈5,800 g. 2. 1,330 L flow through the glovebox during the course of a load/wash/elute/reconditioning cycle. ≈920 L of that are plutonium feed solution. 3. ≈45 kg of Dowel 21-K anion resin (strong base) in 3 columns. Resin decomposition reactions can be explosive under certain circumstances. Relevant factors include drying resin, exposing to temperatures in excess of 60 ^{o}C, excess radiation, stagnation, and confinement. 4. Steam supplied to heat exchanger at 280 ^{o}F. 5. Forced ventilation; 115 VAC; 30 and 65 psig source air lines. 6. Small gear pump (12 psi).
Peroxide precipitation glovebox	1. Plutonium nitrate solution 2. Plutonium peroxide cake 3. Plutonium filtrate solution 4. 35 percent hydrogen peroxide 5. Chemical energy 6. Potential energy 7. Kinetic energy	1. ≈23,300 g of Pu in solution fed into the box in a complete production run at inlet feed concentration of 90 g/L. Based on precipitation vessel sizes, ≈2,000 g cumulative total of Pu can be in vessels during normal operation (i.e., vessels ½ full of feed and ½ full of 35 percent H_2O_2). 2. ≈2,900 g of peroxide cake (2,300 g Pu) are collected in a load cell before its contents are sent to the calcining line. 3. ≈100 g of Pu in solution are collected in the filtrate slab tank for transfer to the evaporation line for recycle. ≈500 to 600 g of Pu will pass through the filtrate slab tank in a complete production run. 4. ≈180 L of H_2O_2 fed in a complete production run. 5. 35 percent H_2O_2 can decompose explosively from pressure buildup (i.e., not propagating detonation) under certain conditions such as excessive temperature or mixture with organic or ferrous contaminants. 52 percent or greater solutions pose the greatest hazard and can require special handling.

Source: DOE G 421.1-X (draft)

For large nuclear facilities with many hazardous materials in small quantities (e.g., facilities with numerous gloveboxes and storage vaults), it can often be impractical to identify every possible material location by individual stations. In such cases, locations and quantities of materials should be specified by room and operation, generically for low-quantity operations and specifically for major operations. Lists should provide enough detail that an independent reviewer can understand the approximate material quantities foreseen in each major operation, can estimate the distribution of the materials within the building, and can judge the validity of the MAR quantities or energy estimations used in any accident analysis.

c. Identify and discuss the methods used to determine and analyze failure modes of SSCs, ACs, and control programs.

A methodology for evaluation of the risk is through the use of an FMEA. This methodology is less rigorous than the fault tree/event tree methodology and generally is used when a simplified, lower cost, scoping analysis is desirable.

The FMEA process is an inductive logic approach to the identification of all possible failure modes and their effects for all equipment on a component-by-component basis. This process identifies single-failure modes only in accordance with the requirements of Institute of Electrical and Electronics Engineers (IEEE) 603-1991, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*; 10 CFR 50.120, appendix K; and Nuclear Regulatory Commission (NRC) Regulatory Guide 1.7, *Control of Combustible Gas Concentrations in Containment*. An FMEA is generally much more detailed than a fault tree analysis since all failure modes are considered rather than only considering dominant ones, as is typical in a fault tree analysis.

As a consequence of the analysis, a qualitative, systematic list of equipment, failure modes, and associated effects is developed. The worst case consequences of a single failure are also given with recommendations for improving safety for individual failures. The end result is the generation of recommendations for increasing equipment reliability and thus improving safety.

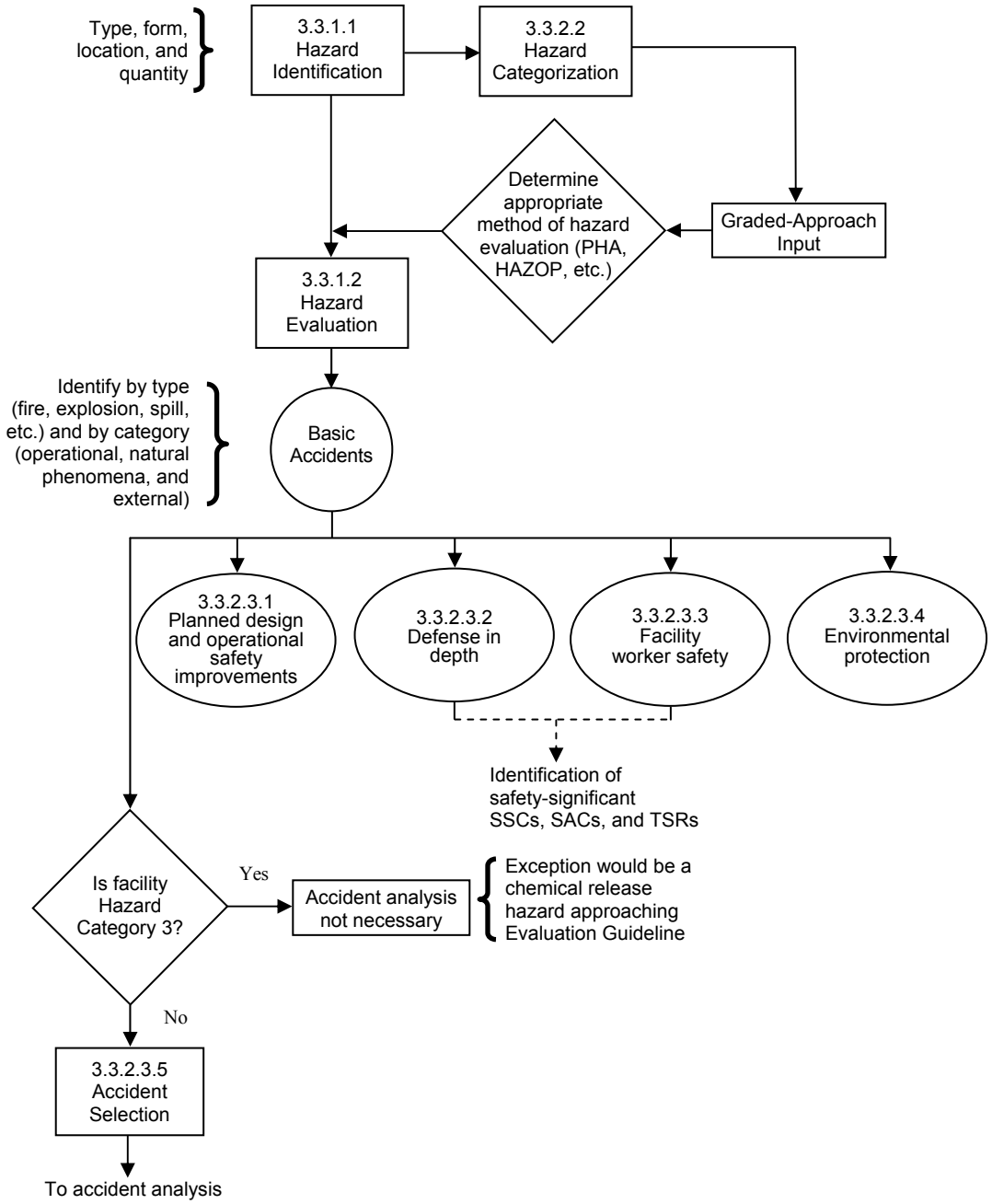
FMEA is the study of the potential failures that might occur in any part of a system to determine the probable effect of each on all other parts of the system and on probable operational success.

d. Identify and discuss methods available to reviewers to determine if a hazard analysis has omitted important accident vulnerabilities.

A basic flowchart for hazard/accident analysis is provided in figure 4, which is taken from DOE-STD-3009-94. The major features of hazard analysis and the graded approach are captured in this figure. Hazard identification provides the basis for the final hazard categorization of the facility. That categorization is input for the graded approach for hazard evaluation. Hazard category 3 facilities are not required to perform formal, quantitative accident analysis.

Figure 4 identifies the specific point where the analyst must move beyond the general outline of DOE-STD-3009-94 and use the graded approach to determine specifically appropriate hazard analysis methodology. Application of a graded approach is based on the judgment and experience of the analysts and results in the selection of a hazard evaluation technique such as process hazards analysis, HAZOP, etc. More elaborate techniques will generally be associated with more complex processes. The experience and capabilities of analysts are also major considerations in efficient performance of a comprehensive hazard evaluation.

Systematic application of the chosen techniques to the operations in a facility generates a number of basic accidents based on types of events and system performance in response to the events. These accidents can be binned in accordance with predefined consequence and frequency ranking thresholds.



Source: DOE-STD-3009-94

Figure 4. Flowchart for performing a hazard analysis

Products of the hazard evaluation include

- identification of planned design and operational safety improvements;
- summary of defense in depth including identification of SS SSCs and other items needing TSR coverage, including relevant programs covered under TSR ACs;

- summary of significant worker protection features including identification of SS SSCs and relevant programs covered under TSR administrative controls;
- summary of design and operational features that reduce the potential for large material releases to the environment.

e. Identify and discuss the relationship between hazard analysis and the postulation of accidents for quantitative consequence analysis in DSA for DOE nuclear facilities. Describe what factors govern the choice of an accident warranting further consequence analysis.

The following is taken from DOE-STD-3009-94.

The hazard analysis identifies DBAs that will be used in the accident analysis. These accidents represent a complete set of bounding conditions. The identification of DBAs results from the hazard evaluation ranking of the complete spectrum of facility accidents. The approach used at any specific facility is based on the detail needed for a given facility and the experience of the analysts. Hazard analysis involves ranking risk for accidents by consequence and frequency. The ranking schemes are designed to separate the lower risk accidents that are adequately assessed by hazard evaluation from higher risk accidents that may warrant additional quantitative analysis if the phenomena involved are not simplistic. Rankings use a bin system. For example, frequency bins should typically cover two orders of magnitude. Although the exercise of binning is essentially qualitative, analysts often use a simple numerical basis for judgments to provide consistency.

Another methodology would be to use a summary of historical data. Before beginning the evaluation, a conservative Gaussian plume estimation of the amount of material needed outside the building to cause a certain dose might be performed to aid in defining thresholds of significance. However, the ranking of frequency and consequence into thresholds of significance is more of a qualitative than a quantitative exercise. An important factor in estimating binning thresholds for consequences is to tie the thresholds to the EG so that accidents that could challenge the guideline are correctly identified for formal accident analysis..

This accident selection activity identifies the process and criteria used to select the unique and representative potential accidents to be included in accident analysis. Unique accidents are those with sufficiently high-risk estimates that individual examination is needed. Representative accidents bound a number of similar accidents of lesser risk. Representative accidents are examined to the extent they are not bounded by unique accidents. In any case, at least one bounding accident from each of the major types determined from the hazard analysis should be selected unless the bounding consequences are “low.” Accidents are identified and listed by accident category and type.

f. Identify and discuss essential elements of deterministic and Probabilistic Risk Assessment (PRA) techniques.

The following is taken from DOE G 421.1-X (draft).

Accident Scenarios in General

The hazards analysis described in chapter 3 of DOE G 421.1-X (draft) yields, as one of its products, a limited set of bounding accidents selected for subsequent accident analysis. The accident analysis then defines these scenarios in a formally rigorous manner. Each scenario must be developed and described in a clear, step-by-step manner, starting with an initiator and detailing every significant event in the scenario progression. For example, consider a metal dissolution process that generates hydrogen as a by-product. For an explosion accident, the initiator is not excess hydrogen in the vessel air space or offgas. The true initiator is not even excess acid concentration, or solution temperature being too high. There is a reason either condition occurred, and that is the accident initiator. The failure of each indicator, alarm, or shutdown interlock that allows the hydrogen concentration to build without intervention is a significant event in the progression; so are the failures of any SSCs intended to mitigate the explosion's consequences. The function of each preventive and mitigative feature in this hypothetical scenario progression must be apparent. Only in that way can the complete set of controls associated with an event be understood, the complete spectrum of functional failures postulated, and their significance systematically assessed.

The extent of physical damage to the process from the initiating event and its progression is the single most critical aspect of understanding the overall scenario. It must be estimated using standard engineering principles such as those discussed in chapter 6 of DOE G 421.1-X (draft), or from specialized damage assessments using first-order principles or more sophisticated computer modeling as appropriate. The level of engineering analysis in this regard must be complete enough to allow independent confirmation at the level of a peer review process.

Scenarios are typically evaluated in either a deterministic or a probabilistic manner. While there is a clear distinction between these two approaches, they can easily blend. It is not uncommon for deterministic scenario definitions to use some of the tools associated with probabilistic analysis (e.g., event and fault trees), and the selection of any one probabilistic progression path generates a deterministic scenario.

Deterministic Scenarios

The deterministic approach is centered on a complete narrative description of the postulated accident scenario, identifying all key assumptions such as whether a safety SSC is assumed to provide its safety function or is assumed to fail. The key distinction is that assumptions about such progression are made and stated as part of the scenario definition.

The classic DBAs used in nuclear reactor regulation by the NRC are deterministic scenarios. The assumptions made should not, however, be superficial or frivolous. The reactor DBAs allowed assumptions about SSC functionality because those assumptions were tied to a set of functional requirements that guaranteed performance. For example, if an electrical circuit could be exposed to given levels of temperature, humidity, or radiation, its design basis was to survive those conditions. Definition of the extent of physical damage from accident phenomena is absolutely vital to deterministic analysis, as that definition virtually is the scenario. In probabilistic analysis, one can identify a wide range of damage possibilities, so

that the worst case potential is recorded even if the frequencies associated with it are suspect. In a deterministic scenario, if the estimate of physical damage is wrong, there is no other estimate available, and this error can become deeply embedded in the safety basis.

Probabilistic Scenarios

The probabilistic approach identifies a variety of possible outcomes in order to characterize the key progression and decision points. The most common tools associated with this approach are event trees and fault trees.

Event tree analysis is a simple approach to delineating sequences of events that could lead to an undesired event. Unlike the deterministic approach discussed above, the event tree models both success and failure of SSCs, resulting in different accident sequences. Success and failure of preventive and mitigative SSCs are graphically depicted from left to right either in the time sequence in which they occur, or in some other logical order reflecting operational interdependence. A path through the event tree is defined as an accident sequence. The end result of an accident sequence is either a safe termination of the initiating event (i.e., the success of preventive or mitigative SSCs results in minimal consequence), or increasing levels of consequence severity depending on how many SSCs fail.

If desired, the event tree can also be used to quantitatively estimate frequencies of occurrence of accident sequences. This is accomplished by estimating the frequency of occurrence of the initiating event, the conditional success and failure probabilities for each SSC, and multiplying them for each path through the event tree. For those sequences that result in the same level of consequence severity, their frequencies of occurrence can be summed to represent the frequency of occurrence for that level of consequences (e.g., a major fire). When doing so, however, attention to the dependence of SSCs upon one another or to the initiating event is important to prevent error. For example, a common cause loss of power could fail two SSCs such that the conditional failure probability is greater than the product of the two SSCs' independent failure probabilities.

Where needed, initiating event frequencies and failure probabilities can be established from historical accident experience, generalized rules of failure probabilities, or reliability data. These characterizations can be made in either a top-level manner or derived from the bottom up using fault trees.

Fault tree analysis is a deductive reasoning process used to systematically identify how an undesired event can occur. The fault tree should reflect all possible failure modes, whether associated with equipment or human error, that allow the undesired event to occur.

The basic idea is to select a particular failure mode for analysis. This failure mode becomes the top event of the fault tree and determines the immediate, necessary, and sufficient causes for the occurrence of the top event, one step at a time. The analysis of the top event produces a linkage of fault events connected by "and" and "or" logic gates. For example, the hypothetical hydrogen explosion discussed earlier would require either excessive solution temperature *or* excess acid concentration to generate a significant amount of hydrogen. To progress to the next level up toward the failure mode of an explosion, however, would

require both improper solution chemistry *and* failure of the hydrogen detection and shutdown interlock.

If the fault tree model developed to assess the accident is large, computer codes are commercially available for either qualitative analysis (e.g., determination of minimal cut sets that identify the combination of component failures leading to the failure defined by the top event) or quantitative assessments of failure rates or failure probabilities. Specialized training is necessary for such applications and is available from commercial sources.

Quantitative fault tree and event tree analyses have been used for probabilistic risk assessments of nuclear reactor accidents for over 2 decades (along with the deterministic accident analysis precedents for nuclear power that date back 40 years). They are used to lesser degrees in almost every industry with significant accident potentials related to equipment failures. Probabilistic methods are of real value when dealing with a complex electro-mechanical system because they can break down potentially very complex interaction issues.

g. Given an accident source term of radionuclide/hazardous chemical release, discuss the factors that should be considered in selection of an appropriate computer code for off-site transport and deposition.

The following is taken from DOE-EH-4.2.1.2-Criteria.

Safety analysis software for the DOE "toolbox" was designated by DOE/EH in March 2003 (DOE/EH, 2003). The supporting basis for this designation was provided by a DOE-chartered Safety Analysis Software Group in the technical report *Selection of Computer Codes for DOE Safety Analysis Applications*. The codes for toolbox status, their version, and area of applicability are listed in table 1-1 of DOE-EH-4.2.1.2-Criteria. Later versions of the codes may be selected based on recommendations by the software developers and information obtained in the course of the SQA Implementation Program.

Eventually, each of these six codes and their respective development programs will undergo evaluation of their SQA attributes relative to established requirements identified in Task 4.2.1.2 and is termed an SQA evaluation. The SQA evaluation will assess those measures requiring action before the individual codes meet current SQA-compliant standards, and will be documented in a series of reports.

Appendix A of DOE-STD-3009-94 provides detailed guidance on evaluating dispersion and consequences. This appendix states

- the EG is 25 rem total effective dose equivalent (TEDE) to the maximally-exposed offsite individual (MOI) at the site boundary;
- the 95th percentile of the distribution of the doses to the MOI is used;
- the method for dispersion and transport should be consistent with Nuclear Regulatory Guide 1.145, *Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants,* using hourly averaged meteorological data, straight-line Gaussian dispersion (exposure duration <8 hours);

- exposure starts when the plume reaches the MOI; and
- for elevated releases, the plume touchdown can occur beyond the site boundary.

Phenomena or variables that impact dispersion and transport are meteorological conditions, building wake effects, source depletion and transformation, site characteristics, boundary layer phenomena, and resuspension potential.

h. Discuss the physics of fires and explosions as the means of generating airborne plumes of hazardous materials and damaging barriers to releases. Also describe how the physics affects the quantities of or rates at which hazardous materials may become airborne as a result of spills, evaporation, entrainment, fires, and other accidents.

The following is taken from DOE G 421.1-X (draft).

Physics of Fires

A fire involves highly exothermic chemical reactions that heat the surroundings. The heated air and combustion products (smoke and gases) are less dense than the surrounding air and therefore rise. The rising plume draws in fresh air, which sustains the combustion process. This incoming air can entrain radioactive particles that would otherwise not be involved in the fire.

The aspect of a fire that may influence the airborne release of radiological materials directly is the suspension of particulate material from surfaces and entrainment of the particles in the buoyant plume generated by the gaseous fire products. Indirect influences convert material into particulate matter and entrain them in the buoyant plume generated by the gaseous fire products.

Physics of Explosions

After detonation, heating of all material enclosed within the explosive occurs quickly, vaporizing the material into small droplets. The near instantaneous injection of energy into a small volume causes expansion of the air so quickly that a local density deficit results in what can be termed a cloud or bubble. The density deficit in the cloud relative to the surrounding air density, combined with the cloud initial momentum, causes the cloud to rise.

Aerodynamic drag, as well as the gradually increasing mass of the cloud resulting from the entrainment of surrounding air caused by the density deficit, slows the cloud during the rise. Cooling of the cloud due to radiation transport and internal mixing of entrained air with the air in the cloud reduces the density deficit until the cloud's density approximates that of the atmosphere. At that time the upward motion of the cloud stops because the effects of buoyancy are abated. The rate of entrainment is generally assumed to be proportional to the product of the average translational speed of the cloud and its surface area.

It has been experimentally noted that in a stably stratified atmosphere, the cloud first overshoots the maximum final cloud height. This is due to the fact that while the cloud density may have equilibrated with the atmospheric density (causing neutral buoyancy), the

momentum of the cloud does not vanish when the buoyancy difference does. This results in a drag friction damped oscillation of the cloud about a buoyancy equilibrium height.

i. Discuss the phenomena and modeling of airborne dispersion of toxic materials, addressing weather effects, turbulent mixing, mixing heights, plume temperature, evolution and potential settling or plate out of particulates and aerosols, precipitation, building wake, and surface roughness effects.

The following is taken from DOE G 421.1-X (draft).

Radiological and/or chemically hazardous pollutants, once released into the atmosphere, are transported in the direction of the mean wind, diluted by the mean wind speed as it stretches out the plume, and diffused by atmospheric turbulence. This atmospheric turbulence consists of random, chaotic air motion in the form of countless whirling eddies. These eddies have a great range of size, from millimeters to tens or even hundreds of meters in diameter, with the smaller eddies being embedded within the larger ones. When a plume of material is released into the atmosphere, the smaller eddies cause the material to diffuse within the plume, while the larger ones cause the plume to meander. These turbulent eddies are formed by horizontal and vertical gradients in both the velocity and the temperature of the air (i.e., mechanical turbulence and buoyancy).

If pollutants are neutrally buoyant, as in the release of trace amounts of very fine particulates or gases, plume dispersion approximates a Gaussian distribution in both the crosswind (lateral) and vertical directions. As the plume moves downwind, it gets progressively larger and less concentrated.

For continuous releases, the magnitude of the downwind diffusion (i.e., σ_x) is negligible in comparison with the speed of the wind. If the release is of short duration (i.e., a puff), the mean wind speed only acts as a transport agent, and the turbulent diffusion in the downwind direction becomes meaningful. Accordingly, a puff is described by Gaussian equations in all three dimensions, whereas a continuous release is described by Gaussian equations in two dimensions and a length (determined by wind speed and duration) in the third dimension.

If the released material is an undiluted gas (i.e., not mixed with air) and is more dense than air, it will slump to the ground and slowly spread as it moves downwind. The material's density restricts the vertical turbulence spread, resulting in a pancake-like plume. Over time, it mixes with the air through lateral and restricted vertical turbulence and becomes increasingly less concentrated. Similarly, a lighter-than-air gas (e.g., hydrogen) that is initially undiluted will rise as a bubble due to buoyancy. It, too, mixes with the air and becomes increasingly less concentrated. Once a gas is thoroughly mixed with the air, it may be treated as neutrally buoyant, although its molecular weight may be significantly different from that of air. Several meteorological parameters affect the shape and size of a neutrally buoyant plume. These are discussed in the following sections.

Wind Variations

Wind velocity is a vector quantity, having both magnitude and direction. Its magnitude is the wind speed. Variations in magnitude and direction are important in dispersion.

The wind speed at the height of the release determines the travel time to reach a given downwind receptor, and it determines the amount of initial dilution from the point of release. The greater the wind speed, the more "stretched out" the plume will be. It is also a factor in determining the magnitude of atmospheric stability. Mechanical turbulence is generated in the air when adjacent parcels of air move at different velocities, either at different speeds or in different directions; this is known as wind shear. Thus, a change in wind speed with height above the ground, or a variation in wind direction at a given height, causes mechanical turbulence. Mechanical turbulence is also generated when air interacts with some fixed object, such as the ground, described by roughness length, or with a building, described by aerodynamic effects such as wake and cavity.

The horizontal wind direction at the height of the release determines the initial direction of transport. The horizontal wind direction used in modeling is the average, or first moment, of a series of "instantaneous" wind direction measurements. By convention, the horizontal wind direction is 180° out of phase with the downwind or transport direction. For example, a wind blowing from the southeast will transport the plume to the northwest. For a steady-state straight line Gaussian model, discussed below, the direction of transport always remains the same in time and space, by definition.

Atmospheric turbulence is directly related to the variability of wind direction. This variability is normally expressed in terms of the standard deviation of a series of instantaneous wind direction measurements over a selected observation period, normally 15 minutes. The standard deviation, or second moment, of the horizontal wind direction, σ_θ, is commonly used to type atmospheric turbulence into stability classes. Some sites also include the standard deviation of the vertical wind component, σ_φ, to type atmospheric turbulence.

Atmospheric turbulence can also be produced by temperature gradients, especially vertical temperature gradients. When a parcel of air is displaced vertically, it will expand (if rising) or contract (if sinking) to adjust its pressure to that of its surroundings. The expansion or contraction is accompanied by an adiabatic temperature change. As a parcel rises, it cools. If the surrounding air is warmer, the parcel will be heavier than its surroundings and sink back toward its original position; its motion ceases. On the other hand, if the surrounding air is cooler, the parcel will be lighter and continue to move upward; its motion is enhanced. Similarly, if the air parcel sinks, it warms up as it contracts. If the surrounding air is cooler, the parcel will be lighter and rise back toward its original position; its motion ceases. However, if the surrounding air is warmer, the parcel will be heavier and continue to sink. Thus, turbulence is suppressed if the temperature profile of the air (the so-called lapse rate) is less than adiabatic (i.e., subadiabatic), and enhanced if greater than adiabatic (i.e., superadiabatic). The adiabatic lapse rate near ground is about -9.8 °C/km (or -5.4 °F/1,000 ft).

The atmospheric layer near the ground is called the mixed layer, as this is where atmospheric turbulence is the most common. During daylight, the ground heats up, warming the air near the surface. The lapse rate near the surface thus becomes superadiabatic and buoyancy forces enhance any existing mechanical turbulence caused by ground roughness or wind shear. At night, the ground cools, causing the air near the surface to cool, and the lapse rate becomes subadiabatic (and frequently inverted), suppressing any existing mechanical turbulence. At greater heights, a few hundred to a few thousand meters in altitude, the lapse rate may change. It is common for a turbulent lower atmosphere to be capped by a lapse rate that is subadiabatic so that turbulent eddies rising from below are suppressed.

The atmospheric variables of temperature and moisture (e.g., relative humidity, absolute humidity, dew point temperature, wet-bulb temperature) do not directly affect the magnitudes of the atmospheric dilution and dispersion. However, for releases of hazardous chemicals, these variables play a significant role in determining the thermodynamics in establishing rates of flashing, aerosolization, and puddle evaporation. For example, for releases of anhydrous ammonia, knowledge of the relative humidity is crucial in determining its ultimate equilibrium state after release. On very humid days, the anhydrous ammonia will absorb water vapor from the atmosphere since it is deliquescent, become ammonium hydroxide, and act as a dense gas. During low humidity days, the ammonia will absorb little to no water vapor, and remain lighter than air and become buoyant. Other releases, such as uranium hexafluoride, are also very sensitive to atmospheric water vapor.

With regard to precipitation scavenging (i.e., rainout or snowout), the rate of precipitation is needed as an input to models that address this atmospheric phenomenon.

A comprehensive treatment of atmospheric dispersion is so complex that many approximations are needed to make it tractable. Since the atmosphere has an infinite number of degrees of freedom, and since turbulence is random and chaotic, it can not be parameterized and one must resort to empirical formulations. One early attempt to simplify the treatment of turbulence was to define atmospheric stability classes and associate a rate of lateral and vertical diffusion with each class as a function of downwind distance only. Although computations based on these stability classes provide only a rough approximation to reality, they have proven extremely useful and are still in use, although treatments that are more accurate are available. The most common measurements employed in typing stability class are wind direction variability and vertical temperature gradients. The wind direction variability provides the best approximation of mechanical turbulence, and the vertical temperature gradient provides an approximation of the buoyancy component. The following paragraphs provide some definitions associated with stability class and the methods to type it in order to approximate the turbulence intensities that drive atmospheric dispersion.

Definitions of Stability Classes

The rate at which turbulence diffuses material depends upon the stability of the atmosphere. Seven stability classes have been defined. These classes, their relation to temperature gradient, and the conditions of occurrence are as follows:

1. A—Extremely unstable (strong superadiabatic). Normally occurs during bright sunshine with relatively low wind speed (<3 m/sec).
2. B—Moderately unstable (moderate superadiabatic). Normally occurs during conditions that range from bright sunshine with wind speeds in the 3 to 5 m/sec range, to dim sunshine with wind speeds <2 m/sec.
3. C—Slightly unstable (slight superadiabatic). Normally occurs during conditions that range from bright sunshine with wind speeds in the 5 to 6 m/sec range, to dim sunshine with wind speed in the 2 to 3 m/sec range.
4. D—Neutral (adiabatic). Normally occurs with moderate to dim sunshine, cloudy conditions, and at night, with wind speeds >3 m/sec. It also occurs with very strong wind speeds on either sunny or cloudy days.
5. E—Slightly stable (slight subadiabatic with or without inversion). Normally occurs at night or in the early morning with some cloud cover and with wind speeds in the 2 to 5 m/sec range.
6. F—Moderately stable (moderate subadiabatic with inversion). Normally occurs at night or in the early morning with little cloud cover and with relatively low wind speeds (<3 m/sec).
7. G—Extremely stable (strong subadiabatic with inversion). Normally occurs at night or in the early morning with very light to nearly zero wind speed (i.e., calm wind conditions). This class, as well as the F stability class, is associated with inversion breakup fumigation conditions in which an elevated plume is rapidly forced to the ground. Due to the stable conditions (i.e., slow lateral and vertical diffusion) and the low wind speed (i.e., slow dilution), the plume concentrations can be high. Fumigation represents the worst case scenario for near-field immersion doses associated with elevated releases.

Unstable conditions result in rapid lateral and vertical diffusion of pollutants (i.e., wide plumes), whereas stable conditions result in slow lateral and vertical diffusion (i.e., narrow plumes).

Although class A is not rare, it is not as common as classes B through F. Class D is the most common stability class because of the large number of combinations of meteorological conditions that can result in class D stability. For example, high-wind conditions and/or cloudy conditions during the day or at night are normally class D. During periods of extended rainfall and overcast conditions, as many as 100 consecutive hours of class D stability have been recorded. Classes E and F are the most common stability classes at night. Class G is less common and because it is difficult to model accurately, it is often ignored in computer models of the Gaussian equations. Inversion breakup fumigation (i.e., class G) occurs when a very stable atmosphere becomes a very unstable atmosphere in response to early morning heating. An elevated plume can be quickly brought down to the surface through the fumigation depth.

In calculating plume concentrations, or consequences to the receptor, “typical” and “unfavorable” dispersion conditions are of special interest in accident analyses.

Typical

The median (i.e., 50th percentile), the mean (i.e., average), or the mode (i.e., peak) of a distribution could all be considered as representative of typical conditions. However, the median is the most meaningful for plume dispersion, for several reasons. It is not heavily influenced by outliers (abnormally small or large values), as is the mean. For a bimodal distribution (which can happen for dispersion), the mean may fall between the peaks (i.e., modes) of the distribution and thus be comparatively infrequent, which could not be considered typical. (The median could also be atypical in this sense but it, at least, has a relevant meaning.) In addition, if the mode were chosen as typical, a bimodal distribution could give two valid choices if the peaks are nearly as large.

Unfavorable

Unfavorable is normally taken to be 95th percentile dispersion, for which the consequences are smaller 95 percent of the time and larger 5 percent of the time. Other dispersion conditions are sometimes used for unfavorable conditions, such as worst case, near worst case, or specific constant-weather conditions, such as class F stability and 1.0 or 2.0 m/sec wind speed. Near-worst-case conditions (most likely G stability class and nearly calm winds), however, are extremely rare and would be overly conservative for most applications.

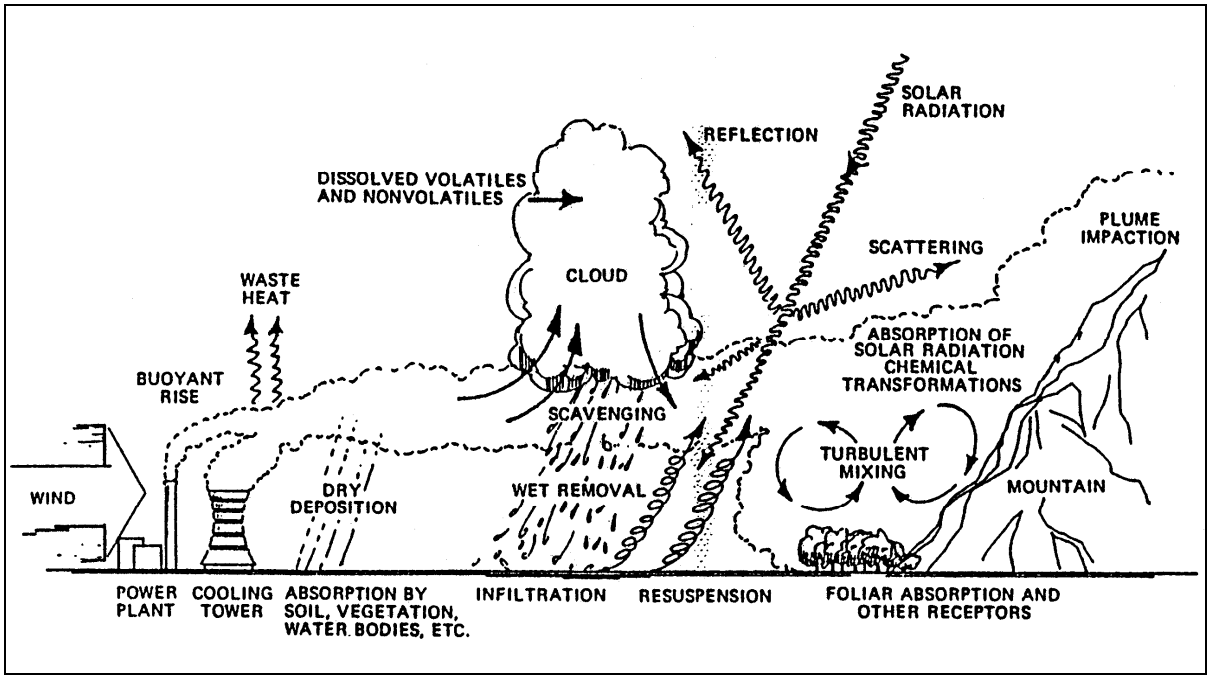
The amount of atmospheric dispersion corresponding to 50th or 95th percentile weather depends upon the nature of the pollutant. If the pollutant is a trace constituent, it can be treated with a Gaussian plume or puff model, depending upon the duration of the release. If it is a heavy gas, it must be treated with a heavy-gas model that both limits vertical dispersion due to slumping, while simultaneously entraining ambient air through the sides of the plume. The amount of dispersion for the 50th or 95th percentile conditions would likely be different for these different models.

All releases of radioactive plumes should be considered as trace-amount releases. They can be handled with the Gaussian plume model. Likewise, if a small quantity of chemical is spilled or released in a fire or explosion, the resultant plume can be approximated with the Gaussian plume model, as long as the additional plume buoyancy and explosion overpressures are addressed. For chemicals, however, other complicating factors must be considered, such as chemical reactions within the plume, and source term determinants such as evaporation rate, aerosolization rate, subcooling, superheating, etc.

Gaussian Plume Model for Neutrally Buoyant Plumes

Figure 5 provides an overview of which atmospheric and terrestrial processes are involved in determining the ultimate fate of a radionuclide or chemical pollutant after it is released to the environment. These highly complex interactions of physical phenomena with underlying topography and foliar populations are extremely difficult to describe mathematically. In order to approximate the effects of such phenomena, a Gaussian plume model has found wide

application. The following sections describe modeling techniques that are used to simulate the effects of these phenomena.



Source: DOE G 421.1-X (draft)

Figure 5. Atmospheric processes acting upon radiological/toxicological releases

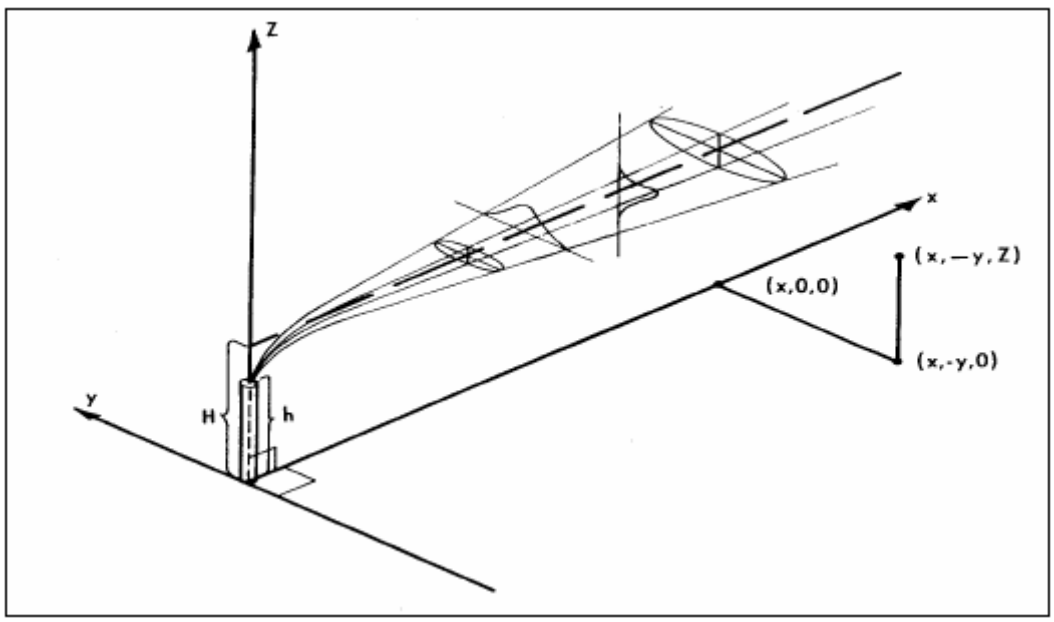
Basic Gaussian Equations

Intrinsic to the assumptions underlying the Gaussian approximation of atmospheric dispersion is that as a plume is transported downwind, its horizontal expansion is essentially unlimited. Vertical expansion is limited by the earth's surface and aloft under inversion conditions. The downward expansion of the plume stops at the ground, while upward expansion may be stopped if there is a stable layer (i.e., a "cap") at the top of the mixed layer. This cap acts as a lid to rising "thermals" of air, thus restricting the range and magnitude of vertical turbulence. The plume is often considered to "reflect" off both the ground and the top of the mixed layer, causing the vertical profile to become increasingly uniform as the plume proceeds downwind. For low level mixing heights, multiple reflections can occur from the ground and the lid, especially for far-field receptors.

Figure 6 illustrates the general shape of a Gaussian plume as released from a stack. The coordinate system typically used in Gaussian equations is shown, in which x is defined as the downwind direction, y then follows as the horizontal cross-wind direction, and z is vertical direction.

The amount of atmospheric dispersion is usually expressed in terms of χ/Q, where χ is the concentration of the pollutant in air at some downwind (x, y, z) location, either the

instantaneous concentration (e.g., becquerel [Bq]/m^3 or g/m^3) or the time-integrated concentration (e.g., Bq-s/m^3 or g-sec/m^3), and Q is the constant rate of release (e.g., Bq/sec or g/sec) of the pollutant, or total source strength (e.g., becquerel or grams) of the pollutant. The units of χ/Q are sec/m^3 whether the instantaneous or time-integrated releases are considered or whether radioactive or chemical pollutants are being evaluated. Thus, χ/Q is the concentration of the pollutant in air at the receptor per unit source rate, or time-integrated concentration per unit source. The actual concentration of the pollutant in air (χ) at the receptor is thus the product of χ/Q and the rate of release of the pollutant (Q).



Source: DOE G 421.1-X (draft)

Figure 6. Coordinate system of Gaussian plume

The Gaussian plume model, when not constrained in the vertical by the ground or the top of the mixed layer, is expressed as

$$\frac{\chi(x,y,z,h)}{Q}=\frac{1}{2\pi u\sigma_y\sigma_z}e^{-y^2/2\sigma_y^2}\left[e^{-(z-h)^2/2\sigma_z^2}\right]$$

where
x = the downwind distance of the receptor from the point of release
y = the horizontal cross-wind distance of the receptor from the centerline of the plume
z = the distance of the receptor above the ground
h = the height of the plume centerline above the ground (same as H in figure 6)
σ_y = the standard deviation of the horizontal Gaussian distribution (i.e., the “half width”)
σ_z = the standard deviation of the vertical Gaussian distribution (i.e., the “half thickness”)
u = the wind speed at a reference height.

The standard measurement height is usually taken to be 10°m since that is the measurement level of winds at First Order National Weather Service stations and the lowest level of measurement at Federal and commercial nuclear facilities. The constant 2π is implicit in a Gaussian distribution, in which the lateral and vertical components each contribute $(2\pi)^{1/2}$. The wind speed u enters mathematically from a time integration of the time-dependent form of the Gaussian equation; physically, it represents the initial dilution of the plume caused by the "stretching out" of the plume when it is initially released. Note that the downwind distance x does not appear explicitly in this equation. The x dependence is implicit, as the σ_y and σ_z are functions of x only, for a given stability class.

The bracketed term in the above equation defines the vertical distribution. If the pollutants are reflected from the ground and from the top of the mixed layer, this term must be modified. This is done mathematically by adding multiple mirror source terms. The bracketed term in the above equation thus is replaced with

$$\left[e^{-(z-h)^2/2\sigma_z^2} + e^{-(z+h)^2/2\sigma_z^2} + \sum_{n=1}^{N} \left(e^{-(z-h-2nL)^2/2\sigma_z^2} + e^{-(z+h-2nL)^2/2\sigma_z^2} + e^{-(z-h+2nL)^2/2\sigma_z^2} + e^{-(z+h+2nL)^2/2\sigma_z^2} \right) \right]$$

The term before the summation in the above equation is the ground reflection component, since perfect reflection is assumed. The series of terms after the summation represent multiple reflections from the top of the mixed layer and the ground. L represents the height of the top of the mixed layer and the summation is over the number (N) of reflections to be considered. The contribution of the summation term is minor, especially for distances close to the source and for larger values of L. The higher order terms contribute progressively less, and the series is normally terminated after only a few terms. For example, in the MACCS code, the series is terminated at 5.

For a ground-level release (i.e., h = 0), the first two exponential terms become equivalent. Each of these terms is 1 when the receptor is at ground level (i.e., z = 0). In these cases, the "2" in the denominator of the first equation cancels out with the "2" in the numerator, if the summation term is ignored, as is often done. The maximum concentration occurs at plume centerline (i.e., y = 0). Thus, if the summation term is ignored, the Gaussian equation simplifies to

$$\frac{\chi(x, y=0, z=0, h=0)}{Q} = \frac{1}{\pi u \sigma_y \sigma_z}$$

Strictly speaking, the numerator in the above expression is slightly greater than one because of the contribution of the summation term. The above equation, which is now only a function of downwind distance of the receptor, is often used for the collocated worker and MOI, as plume centerline represents a conservative value.

Mixing Layer Height

For an evaluation of χ/Q that includes reflections from the ground and the top of the mixing layer, the height of the top of the mixing layer at the site must be known. This height varies throughout the day and throughout the seasons. During clear nights, when inversions are present, the mixing layer is relatively low, while during sunny days, the mixing layer is much higher. The magnitude of these heights can be obtained from balloon soundings or from remote sensing techniques, such as acoustic or radar soundings.

Building Wakes

For distances less than about 100 m, these coefficients do not provide a good fit to the observations, and the models are generally not considered valid. This arises from the underlying assumption of steady state in the Gaussian models, and they are not accurate in the near-field. Also, building wake effects are important for these smaller distances, but the above coefficients ignore the enhancement of vertical turbulence from wake effects, the increased lateral turbulence, and the down-washing into the cavity behind the building.

Surface Roughness

Surface roughness primarily affects the magnitude of vertical turbulence, and hence, the vertical atmospheric dispersion. The rougher the surface over which the plume passes, the larger the turbulent eddies formed by plume interaction with the earth's surface. If the terrain is not smooth, which is frequently the case, a linear scaling factor needs to be introduced to increase the effective value of σ_z.

For additional information regarding airborne dispersions refer to chapter 9 of DOE G 421.1-X, currently in draft.

j. Discuss the mechanisms involved in the damage caused by extreme natural phenomena including hurricanes, tornadoes, ice storms, wind, flood, earthquakes and wild fires.

The main natural phenomena hazards of interest at all DOE sites are earthquakes and winds/tornadoes. Individual sites may also have to consider range fires, floods, lightning, etc. These phenomena can represent, however, a special case, in that they can inevitably damage even the sturdiest of facilities or systems at some level of severity. The severity of such events is, in turn, related to the initiator frequency of the event. Consequently, DOE has expended a great deal of effort in attempting to define an appropriate probabilistic methodology for assessing safety issues related to natural phenomena.

DOE O 420.1B, *Facility Safety,* and DOE G 420.1-2, *Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Nonnuclear Facilities,* establish the policy and requirements for NPH mitigation for DOE sites and facilities. Specific technical details for addressing NPH events are also provided in several other DOE NPH standards: 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; and DOE-STD-1023-95, *Natural Phenomena Hazards Assessment Criteria*.

The design and evaluation criteria developed in these standards are intended to ensure NPH issues are evaluated both consistently and with a consensus standard of conservatism. The basic approach begins with site-specific probabilistic severity data developed in accordance with DOE standards. Performance categories (PC) are then assigned to structures, systems, and components based on their safety function. Each performance category has a target performance goal, specified in terms of mean annual probabilities of exceedance. Consequently, the combination of performance category and site-specific severity data yields natural phenomena events of specified strength against which safety issues are evaluated.

Five performance categories are currently defined. They are, in order of decreasing importance:

- Performance category 4—Associated with SSCs whose failure during an NPH event could result in offsite consequences greater than or equal to the unmitigated release from a large (>200 megawatt [MW]) category A reactor severe accident. This definition is comparable to that for a hazard category 1 nuclear facility as used in 10 CFR 830.
- Performance category 3—Associated with SSCs whose failure during an NPH event could result in offsite consequences greater than the SC SSC EG of 25 rem.
- Performance category 2—Associated with SS SSCs, buildings in which more than 300 people assemble, or related to emergency functions to preserve the health and safety of workers.
- Performance category 1—Associated with human occupancy, SSC failure resulting in worker fatality or injury, or cost-effective improvements possible.
- Performance category 0—All other SSCs.

k. Define and discuss the following terms:

- **Chi/Q**
- **Dose conversion factor**
- **Breathing rate**
- **Aerodynamic equivalent diameter**
- **Solubility class**
- **Population dose**

Chi/Q

According to DOE/EIS-0120, Chi/Q is the relative calculated air concentration due to a specific air release; units are (sec/m^3). For example, (curies [Ci]/m^3)/(Ci/sec) = (sec/m^3) or (g/m^3)/(g/sec) = (sec/m^3).

Dose Conversion Factor

Dose conversion factors can be obtained from tabulated data in Federal Guidance Report No. 11; in ICRP 30, part 4; in the supplement to part 1 of ICRP 30; or calculated directly using computer programs.

Breathing Rate

According to DOE-HDBK-1122-99, the breathing rate of a worker performing light activity is approximately 2 liters per minute.

Aerodynamic Equivalent Diameter

According to DOE-HDBK-3010-94, the aerodynamic equivalent diameter (AED) is the diameter of a sphere of density 1 g/cm^3 that exhibits the same terminal velocity as the particle in question.

The following definitions are taken from DOE-HDBK-1122-99.

Solubility Class

DOE regulations are currently based on the use of the ICRP 30 dosimetric model for the respiratory system. Under this model, materials are classified as D, W, or Y to describe the clearance of inhaled radioactive materials from the lung. These designations refer to the length of time particles from inhaled aerosols are retained in the pulmonary region: D representing days, W representing weeks, and Y representing years.

Population Dose

ALARA dictates that the facility be aware of changes in radiation exposure to the general population that results from nuclear operations. Issuing thermoluminescent dosimeters (TLDs) to the population is not practical. In addition the TLDs are not sensitive enough to detect changes in environmental radiation levels. The only practical way to determine population exposure is by measurement of environmental radiation levels:

- External radiation level
- Radioactivity present in air
- Radioactivity present in food
- Radioactivity present in water

Population exposure can then be determined by using these values combined with knowledge of the drinking water sources and the types of food consumed in the region.

l. Given a source term, determine dose consequences applying Chi/Q, dose conversion factor, breathing rate, and specific activity as applicable.

Element l is performance based. The Qualifying Official will evaluate its completion.

m. Given a simple accident scenario, demonstrate knowledge by constructing a simple neutral gas dispersion and heavy gas dispersion. Estimate consequences using an accident modeling code including hand calculations, and explain the assumptions, inputs, and results.

Element m is performance based. The Qualifying Official will evaluate its completion. The following information from DOE G 421.1-1 may be helpful.

Version 1 of the Dense Gas Dispersion Model (DEGADIS) was developed by the University of Arkansas for the United States Coast Guard and the Gas Research Institute in 1985. The present version, version 2.1, was established in 1989. EPA lists DEGADIS as an "Appendix B" refined air quality model that may be considered for individual regulatory applications on a case-by-case basis. Although the model is relatively easy to run, the analyst must take special care to fully understand the user options and the data input requirements (e.g., distinctions between isothermal and non-isothermal simulations). The EPA presently manages the maintenance of the model and it can be accessed through the SCRAM (Support Center for Regulatory Air Models) bulletin board.

DEGADIS can address the transport and diffusion of many types of dense gas releases and account for a variety of surface roughness elements. DEGADIS can also simulate atmospheric transport and diffusion of pure chemical releases in passive-dispersion flow regimes. DEGADIS does not have a front-end chemical library that the ALOHA and EPIcode models have. Correspondingly, the analyst needs to couple the DEGADIS dispersion results with chemical source terms generated from other models. DEGADIS can not address buoyant plumes, although it is usually chosen for application for cases where the plume slumps due to its own density.

n. Discuss the processes for evaluating assumptions made for scenarios being modeled.

The following is taken from DOE-STD-3009-94.

All assumptions made in the accident analysis (i.e., the defining points in scenario progression) are to be validated as part of the accident analysis activity. For example, if an operator is supposed to push button Z to stop an accident progression, the accident analysis needs to make it clear that the operator can actually do so. Making it clear may simply involve noting there are no physical phenomena associated with the accident that would preclude the operator from doing so. Likewise, basic assurance must be provided that equipment relied upon in unusual or severe environments will function. This assurance does not constitute the need for or expectation of full, formal environmental qualification.

The above guidance is not meant to imply that the DSA must contain detailed validations for all assumptions. The DSA needs to present information at a level that is considered sufficient for review and approval of the DSA. Referencing an auditable trail of information as part of the controlled supporting documentation is acceptable.

o. Discuss the methods used in the calculation of criticality accidents.

The following is taken from DOE-STD-1135-99.

Various calculation methods are used depending on the complexity of the problem being evaluated. The most commonly used method is to compare the system to experiments in which the size of the accident pulse is known and to previous accidents in similar systems. Other empirical methods are available. The estimation of consequence can be done by

estimating the nuclide release and the dose at distance once the number of fissions is estimated. For metal and contained solids, the nuclide releases are low due to inability of fission products to transport out of the system. The total fission product yield is typically not high (1,017 fissions is 2×10^{-5} moles). Fission products can migrate out of liquids or be expelled from powders. Mass transport is a chemical engineering problem.

Mandatory Performance Activities:

a. Demonstrate by participation on at least five (5) safety basis document or amendment reviews whose major focus deals with hazard or accident analysis for the determination of adequacy of the analyses.

Mandatory performance activities are performance based. The Qualifying Official will evaluate the completion of this activity.

6. Nuclear safety specialists shall demonstrate a familiarity level knowledge of terminology associated with PRA techniques.

a. Identify the strengths and weaknesses of PRA for safety design and regulatory decision-making.

The following is taken from DOE G 421.1-1.

Probabilistic risk assessment has limitations. It may sometimes exclude or not adequately quantify potentially important risk factors, such as very-low-frequency accident initiators, various failures derived from a common event, physical processes resulting from several low-frequency failures, or long-term health effects from potentially toxic materials. Furthermore, because a risk assessment often deals with low-frequency but high-consequence accident risks, there is considerable potential for its results to be misunderstood.

The most useful aspects of the probabilistic risk assessment are not exclusively the risk numbers that are generated; they are also the insight gained by a systematic and methodical consideration of what can go wrong with a system. A procedural analysis leads to the understanding of the likely vulnerabilities of the system, the threats they pose, and the measures that could be applied to mitigate or prevent them. Risk assessment is a particularly powerful tool when there is only a limited set of alternatives for risk evaluation. Thus, meaningful insights can be obtained by a risk assessment without depending on the accuracy of an “actual risk” value; such values are notoriously difficult to ascertain.

The probabilistic approach identifies a variety of possible outcomes in order to characterize the key progression and decision points. The most common tools associated with this approach are event trees and fault trees.

Event tree analysis is a simple approach to delineating sequences of events that could lead to an undesired event. Unlike the deterministic approach the event tree models both success and failure of SSCs, resulting in different accident sequences.

Success and failure of preventive and mitigative SSCs are graphically depicted from left to right either in the time sequence in which they occur, or in some other logical order reflecting operational interdependence. A path through the event tree is defined as an accident sequence. The end result of an accident sequence is either a safe termination of the initiating event (i.e., success of preventive or mitigative SSCs results in minimal consequence), or increasing levels of consequence severity depending on how many SSCs fail.

If desired, the event tree can also be used to quantitatively estimate frequencies of occurrence of accident sequences. This is accomplished by estimating the frequency of occurrence of the initiating event, the conditional success and failure probabilities for each SSC, and multiplying them for each path through the event tree. For those sequences that result in the same level of consequence severity, their frequencies of occurrence can be summed to represent the frequency of occurrence for that level of consequences. For example, a common cause loss of power could fail two SSCs such that the conditional failure probability is greater than the product of the two SSCs' independent failure probabilities.

Where needed, initiating event frequencies and failure probabilities can be established from historical accident experience, generalized rules of failure probabilities, or reliability data. These characterizations can be made in either a top-level manner or derived from the bottom up using fault trees.

Fault tree analysis is a deductive reasoning process used to systematically identify how an undesired event can occur. The fault tree should reflect all possible failure modes, whether associated with equipment or human error, that allow the undesired event to occur. The basic idea is to select a particular failure mode for analysis. This failure mode becomes the top event of the fault tree and determines the immediate, necessary, and sufficient causes for the occurrence of the top event, one step at a time. The analysis of the top event produces a linkage of fault events connected by "and" and "or" logic gates.

If the fault tree model developed to assess the accident is large, computer codes are commercially available for either qualitative analysis (e.g., determination of minimal cut sets that identify the combination of component failures leading to the failure defined by the top event) or quantitative assessments of failure rates or failure probabilities.

Probabilistic methods are of real value when dealing with a complex electro-mechanical system because they can break down potentially very complex interaction issues.

b. Define the following terms with respect to reliability engineering and PRAs:

- **Probability**
- **Reliability**
- **Availability**
- **Unavailability**
- **Uncertainty**
- **Risk**
- **Safety**
- **Accident sequence**

- **Dominant contributors**
- **Minimal cut set**

The following is taken from DOE-HDBK-1014/2-92.

Probability

If E1 is the number of heads, and E2 is the number of tails, E1/(E1 + E2) is an experimental determination of the probability of heads resulting when a coin is flipped.

$$P(El) = n/N$$

By definition, the probability of an event must be greater than or equal to 0, and less than or equal to l. In addition, the sum of the probabilities of all outcomes over the entire "event" must add to equal l. For example, the probability of heads in a flip of a coin is 50 percent, the probability of tails is 50 percent. If we assume these are the only two possible outcomes, 50 percent + 50 percent, the two outcomes, equals 100 percent, or 1.

The concept of probability is used in statistics when considering the reliability of the data or the measuring device, or in the correctness of a decision. To have confidence in the values measured or decisions made, one must have an assurance that the probability is high of the measurement being true, or the decision being correct.

To calculate the probability of an event, the number of successes (s) and failures (f), must be determined. Once this is determined, the probability of the success can be calculated by

$$P = \frac{s}{s+f}$$

where (s + f) = number of tries (n).

The information related to the following terms is extracted from the *Probabilistic Risk Assessment Procedures Guide for NASA [National Aeronautics and Space Administration] Managers and Practitioners*.

Reliability

Reliability is the probability that an item (component or system) would not fail during a specified time (or mission).

Availability

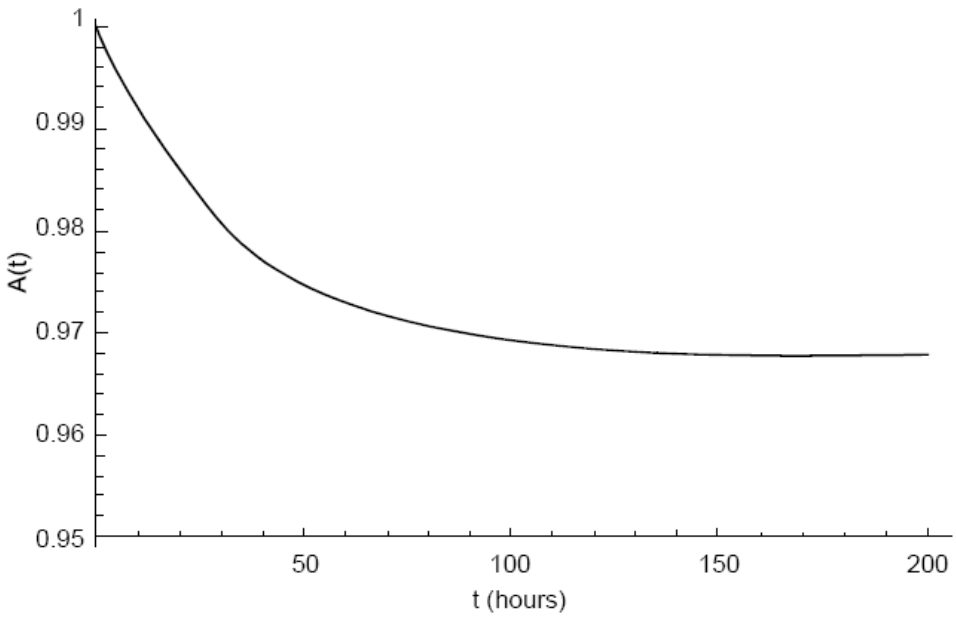
Consider first a single component. Given that the component is initially available, its time-dependent availability A(t) is

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

where
λ = the component failure rate
μ = the repair rate.

Notice that the equation asymptotically approaches a steady state value. This is illustrated in figure 7 for a component with a

- 10^{-3} per hour failure rate; and
- 3×10^{-2} per hour repair rate.



Source: NASA*, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*

Figure 7. Time-dependent component availability

In figure 7 the steady state availability is 0.968. This steady state availability is achieved because repair is possible, which necessitates the presence of a crew or maintenance staff to restore components that fail.

Unavailability

The unavailable state includes two distinct sub-states: failed and functionally unavailable, depending on whether the cause of the unavailability is damage to the component or lack of necessary support such as motive power. The state classification also recognizes that even when a component may be capable of performing its function (i.e., it is available), an incipient or degraded condition could exist in that component or in a supporting component. These failure situations are termed "potentially failed" and "potentially functionally unavailable," respectively. These concepts have proven useful in many PRA data applications.

Uncertainty

Estimation of model parameters involves uncertainties that need to be identified and quantified. A broad classification of the types and sources of uncertainty and potential variabilities in the parameter estimates is as follows:

- Uncertainty in statistical inference based on limited sample size.
- Uncertainty due to estimation model assumptions. Some of the most important assumptions are
  - assumption about applicable testing scheme (i.e., staggered vs. nonstaggered testing methods);
  - assumption of homogeneity of the data generated through specializing generic data to a specific system.

- Uncertainty in data gathering and database development. These include
  - uncertainty because of lack of sufficient information in the event reports, including incompleteness of data sources with respect to number of failure events, number of system demands, and operating hours;
  - uncertainty in translating event characteristics to numerical parameters for impact vector assessment (creation of generic database);
  - uncertainty in determining the applicability of an event to a specific system design and operational characteristics (specializing a generic database for system-specific application).

The role of uncertainty analysis is to produce an epistemic probability distribution of the common cause failure frequency of interest in a particular application, covering all relevant sources of uncertainty from the above list. Clearly, some of the sources or types of uncertainty may be inapplicable, depending on the intended use of the common cause failure parameter and the form and content of the available database. Also, methods for handling various types of uncertainty vary in complexity and accuracy.

The uncertainty associated with the risk model assumptions is handled with sensitivity analysis.

The following techniques have been used for propagation of uncertainties:

- Simulation—The distributions for input parameters are mapped using crude Monte Carlo or Latin Hypercube sampling technique to obtain an empirical distribution for the output function.
- Moment propagation—First and second moments of the input parameters are mapped to obtain mean and variance of the output function using variance/covariance propagation.
- Discrete probability distribution—The distributions for input parameters are converted to discrete probability distribution before mapping. The resulting distribution for the output function is empirical.

Risk

A very common definition of risk is that of a "set of triplets." Determining risk generally amounts to answering the following questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

The answer to the first question is a set of accident scenarios. The second question requires the evaluation of the probabilities of these scenarios, and the third estimates their consequences.

In addition to probabilities and consequences, the triplet definition emphasizes the development of accident scenarios and makes them part of the definition of risk. These scenarios are indeed one of the most important results of a risk assessment.

Safety

In safety applications, PRA helps managers and engineers find design and operation weaknesses in complex systems and then helps them systematically and efficiently uncover and prioritize safety improvements. There must be a small but robust group of in-house technical experts that can understand and appreciate the value of the PRA study, explain its meaning and usefulness to the management, and serve as in-house technical advisers to the management decision process for safety improvement.

Accident Sequence

Accident progression can be modeled using an event sequence diagram (ESD) or its derivative, an event tree (ET). Both are inductive logic models used in PRAs to provide organized displays of sequences of system failures or successes, and human errors or successes, that can lead to specific end states. An ESD is inductive because it starts with the premise that some initiating event (IE) has occurred and then maps out what could occur in the future if systems (or humans) fail or succeed. The ESD identifies accident sequences (or pathways) leading to different end states. The accident sequences form part of the Boolean logic, which allows the systematic quantification of risk.

A traditional accident progression analysis begins with an ESD, refines it, and then transforms it into an ET format. The advantage of this process is that the morphology of an ESD is less rigidly structured than an ET. Hence, ESDs permit the complex relationships among IEs and subsequent responses to be displayed more readily.

One ESD is developed for each IE. The objective is to illustrate all possible paths from the IE to the end states. An ESD is a success-oriented graphic in that it is developed by considering how human actions and system responses (including software) can prevent an accident or mitigate its severity.

Dominant Contributors

The description of each dominant risk scenario along with its likelihood should be provided. The narrative should discuss the nature of initiator and system failures involved in the scenario. The dominant contributors to each system end state should be presented. A consistent presentation scheme needs to be adapted to systematically delineate the progression of the accident, starting from the initiator, and all system failures and interactions that are captured in the definition of the accident scenario. The method of presentation should permit detailed technical review, including recalculation.

Minimal Cut Set

A collection of basic events whose simultaneous occurrence engenders the top event is called a cut set. Minimal cut sets (MCSs) are cut sets containing the minimum subset of basic events whose simultaneous occurrence causes the top event to transpire. Boolean reduction of a fault tree has the objective of reducing the fault tree to an equivalent form that contains only MCSs. This is accomplished by sequential application of the basic laws of Boolean algebra to the original logic embodied in the fault tree until the simplest logical expression emerges. Quantification of the fault tree is the evaluation of the probability of the top event in terms of the probabilities of the basic events, using the reduced Boolean expression of MCSs.

c. Define the following terms and differentiate between the associated processes:

- **Event tree**
- **Fault tree**
- **Failure Modes and Effects Analysis (FMEA)**

The information related to the following terms is extracted from DOE G 421.1-1.

Event Tree

Event tree analysis is an inductive logic technique that sequentially models the progression of events, both successes and failures, leading from some initiator to a series of logical outcomes. An event tree begins with some initiating failure, usually on a component or misoperation level, and maps out a sequence of events to form a set of branches, each of which represents a specific accident sequence leading to a particular final consequence such as a nuclear criticality accident. Like fault trees, event trees are normally used to model events having total success or failure.

Each accident sequence identified by the event tree is somewhat analogous to a branch of a fault tree. However, while a fault tree branch represents a combination of failures leading to the undesired consequence, an event tree branch represents a combination of sequential events (both failures and successes) leading to the undesired consequence. While complete event tree analysis requires identification of all possible and distinct initiating events and development of an event tree for each, fault trees are often useful in examining the consequences of failure of a particular piece of equipment. A detailed understanding of the overall system may be necessary in order to understand how the failure of a particular component affects the success or failure of other components.

Fault Tree

Fault tree analysis is a deductive logic technique that diagrammatically models the various combinations of basic failure events that contribute to some overall failure event. A fault tree begins with the definition of this ultimate failure event or consequence, such as a critical excursion in a specific piece of equipment, and is expanded downward through subsequent levels of contributing failures until an appropriate level of basic failure events has been reached. The contributing failures may be combined as necessary by logical AND and OR gates at the appropriate levels, if necessary. Fault trees are normally used to model events having binary operational states (total failure vs. total success), as opposed to those having partial failures. The deductive nature of the tree is an advantage in that no assumption of accident initiating events is necessary. However, a detailed understanding of the system being examined is necessary so that important system failure modes are not missed. Even so, this technique can be successfully employed throughout the various design and review stages.

As mentioned above, fault trees can be used to model accident sequences, where the top event becomes some consequence of failure sequences. This may result in combining several system logic trees that contribute to the overall consequence thereby providing several independent paths that can lead to the final consequence of a critical excursion.

Failure Modes and Effects Analysis (FMEA)

A failure modes and effects analysis, used with PRAs, is an inductive analysis that systematically analyzes component failure modes and identifies the resulting effects on the system. An FMEA can be relatively detailed, if needed, and quantitative if data exist. Emphasis is placed on identifying the problems that result from hardware failure. Typically, a columnar format is employed in an FMEA. Specific entries include

- component identification
- failure rate
- failure mode
- effect on the system
- severity class
- compensating provisions

An FMEA provides a systematic examination of failures of a system and is relatively simple to apply, but it has the disadvantage of considering only one failure at a time rather than multiple failures.

d. Discuss how PRA methods can help in understanding accident scenarios.

The following is taken from DOE G 421.1-1.

A set of accidents may be postulated based on the designer's/analyst's knowledge of previous operating experience, incident data, previously conducted safety assessments, and engineering judgment. This technique often involves the generation of a series of "what if" questions. These postulated accidents may also be quantified if accident frequency data are available. In many cases, accident frequencies are estimated using engineering judgment.

This approach offers the advantage of simplicity, but its success is highly dependent on the experience of the designer/analyst. The results of such analyses are difficult to reproduce and defend.

The maximum credible accident approach and the DBA approach are two related techniques that may be useful in identifying scenarios and in distinguishing between those that are credible and those that are incredible. The maximum credible accident approach uses engineering judgment to identify accidents. Based on an intuitive estimate of their probabilities, the accident scenarios are divided into credible and incredible accident scenarios. The incredible accidents are not analyzed in detail. Accidents having a probability of occurrence greater than the maximum credible accident can then be analyzed in detail. This approach is typically used only to estimate the upper bound of the accident consequence potential of the particular operation and to design specific protective systems only for the maximum credible accident. It is important to identify as many accident scenarios as possible that potentially could lead to a criticality accident. Designers/analysts should not subjectively dismiss potential criticality scenarios as incredible when it may be possible through a design change to eliminate the scenario completely. The advantage of the maximum credible accident approach is its simplicity, while its weakness is the subjective nature of the division between credible and incredible accident scenarios and the typical treatment of only the maximum credible accident.

The design-basis accident approach is an extension of the maximum credible accident approach. A series of accidents, including low-probability accidents with major consequences, are postulated based on various accident initiators and used as the explicit basis for design or analysis. Accidents having a lower probability of occurrence than the design-basis accident in each accident initiator area are generally not analyzed. The design-basis accident approach is more comprehensive than the maximum credible accident approach but the weakness remains—the subjective nature of the selection of accidents.

As applied to nuclear criticality safety, the terms “maximum credible accident” and “design-basis accident” are not particularly useful except as a means to aid in distinguishing between credible and incredible accidents. Any potential criticality event, regardless of the magnitude of the initial fission burst, should be carefully analyzed and appropriate design changes made if necessary.

7. Nuclear safety specialists shall demonstrate a familiarity level knowledge of basic Heating, Ventilation, Air Conditioning (HVAC) system and filtration system construction, operation, and application.

a. Given engineering diagrams of an HVAC system, identify the following components and discuss their purposes:
- **Blowers**
- **Fans**
- **Dampers**
- **Chillers**
- **Filters**

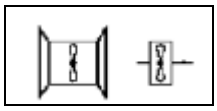
- **HEPA filters**
- **Heat exchangers**
- **Scrubbers**
- **Hoods**
- **Glove boxes**
- **Flow, pressure, temperature, current, level, voltage and position indicators, recorders, and controllers**

Element a is performance based. The Qualifying Official will evaluate its completion. The following information from DOE-HDBK-1016/1-93 and DOE-HDBK-1013/1-92 may be helpful.

Blowers

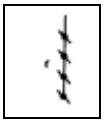
Blowers and fans circulate air through ventilation systems.

Fans



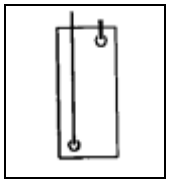
Blowers and fans circulate air through ventilation systems.

Dampers



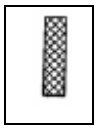
Dampers direct and restrict flow through a ventilation system.

Chillers



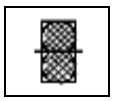
Chillers remove heat from air allowing it to enter a space at a lower temperature.

Filters



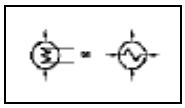
Filters are used to remove any particulates in the air.

HEPA Filters



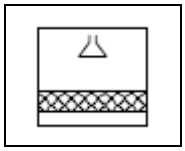
High energy particulate air (HEPA) filters work with efficiency greater than 99 percent.

Heat Exchangers



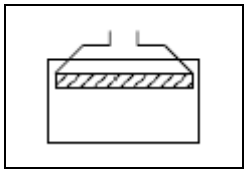
Heat exchangers transfer heat from steam or combustion to breathable air.

Scrubbers



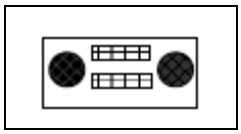
Scrubbers remove particulates in air systems in a localized area.

Hoods



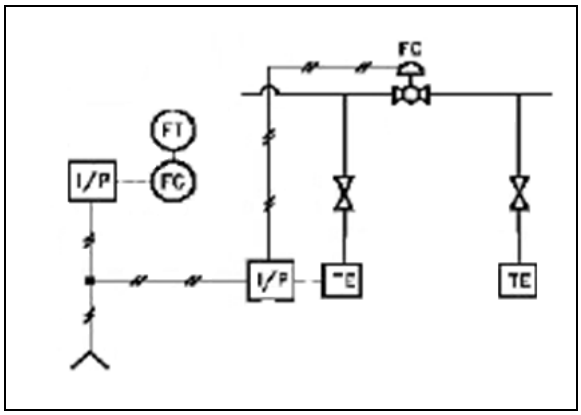
Hoods contain contaminates within a given boundary by using high-velocity air to flow and remove any airborne hazards prior to leaving hood space.

Glove Boxes



Gloveboxes isolate contaminates from the spaces in which they are located.

Flow, Pressure, Temperature, Current, Level, Voltage and Position Indicators, Recorders, and Controllers



Various indicators present a positive indication of system parameters and allow for warnings of unstable conditions.

b. Discuss the relationships between the following in HVAC systems:
- **Supply ventilation**
- **Flow**
- **Exhaust ventilation**

The following is taken from DOE Energy Efficiency and Renewable Energy.

Supply Ventilation

Supply ventilation systems work by pressurizing the building. They use a fan to force outside air into the building while air leaks out of the building through holes in the shell, bath and range fan ducts, and intentional vents (if any exist).

Supply ventilation systems are relatively simple and inexpensive to install. A typical supply ventilation system has a fan and duct system that introduces fresh air into usually one—but preferably several—rooms. This system may include an adjustable window or wall vents in other rooms.

Flow

Air flow to the conditioned space may be controlled, as in the case of a variable air volume system, with a terminal box containing a valve for modulating air flow. The air is finally delivered to the space through a diffuser, whose purpose is to mix the supply air and the

room air. The terminal box may or may not have a reheat coil, which provides additional heat when the space does not need to be cooled or needs less cooling than would be delivered by supply air at the terminal box's minimum air quantity setting. It also may have a fan. Constant air volume systems that are not allowed by energy codes in many applications do not reduce air delivery rates and are dependent on reheat coils to control the delivered cooling. Air leaves the conditioned space either through the return system, or through the exhaust system. In many installations, the ceiling plenum space is used as part of the return ducting in order to save the cost of return ductwork.

Exhaust Ventilation

Exhaust ventilation systems work by depressurizing the building. By reducing the inside air pressure below the outdoor air pressure, they extract indoor air from a house while make-up air infiltrates through leaks in the building shell and through intentional, passive vents.

Exhaust ventilation systems are most applicable in cold climates. In climates with warm, humid summers, depressurization can draw moist air into building wall cavities, where it may condense and cause moisture damage.

Exhaust ventilation systems are relatively simple and inexpensive to install. Typically, an exhaust ventilation system is composed of a single fan connected to a centrally located, single exhaust point in the house. A preferable design option is to connect the fan to ducts from several rooms (preferably rooms where pollutants tend to be generated, such as bathrooms). Adjustable, passive vents through windows or walls can be installed in other rooms to introduce fresh air rather than rely on leaks in the building envelope. However, passive vents may be ineffective because larger pressure differences than those induced by the ventilation fan may be needed for them to work properly.

c. Describe the purpose of the HVAC system in the following applications:

- **Hoods**
- **Glove boxes**
- **Hot cells**
- **Confinement systems**
- **HEPA filtration**

Hoods

According to D. J. Burton's *Industrial Ventilation Workbook,* the HVAC system reduces the pressure in the work area of the hood, which causes air from the room to enter the hood through the open face. Adjusting airflow and the size of the hood opening (typically with a vertically adjustable door) ensures the velocity of air across the face is sufficient to prevent contaminates such as vapors, mists, or smoke from escaping into the room.

Glove Boxes

According to LANL Master Specification sections 23 3816 and 11 5311.10, a glovebox is a controlled environment enclosure providing primary confinement from the work area. Operations inside gloveboxes are performed through sealed glove openings for the protection of the worker, the environment, and/or the process.

Hot Cells

The following definitions are taken from DOE-HDBK-1132-99.

Hot cell exhaust system considerations are as follows:

- Exhaust pre-filters and HEPA filters should be installed to facilitate filter replacement and repair. Use of a bag-in/out type of filter house can lessen personnel exposures.
- Standby filters should be considered to provide backup protection and facilitate primary filter replacement without shutting down the exhaust fans. Standby filters should be installed outside the cell and sealed in an acceptable enclosure for direct maintenance. Note: Air leakage through isolation valves/dampers should be evaluated to avoid the bypassing of filtration devices; the reduction of exhaust flow from recirculation through the standby filters; the exposure of personnel changing the isolated filter elements; and the premature loading of the standby filters.
- Exhaust systems should have monitors that provide an alarm if the concentration of radioactive material in the exhaust exceeds specified limits.
- If radioiodine may be present, consideration should be given to the installation of radioiodine-absorber units.

In facilities where plutonium or enriched uranium is processed, the following are additional considerations:

- Wherever possible, the designer should provide enclosures for confining process work on plutonium and enriched uranium. When these confinement enclosures are specified and designed, consideration should be given to whether room ventilation air for either a secondary or tertiary confinement can be recirculated. If a recirculation ventilation system is provided, the design should provide a suitable means for switching from recirculation to once-through ventilation.

- If advantageous to operations, maintenance, or emergency personnel, the ventilation system should provide for independent shutdown. Such a shutdown should be considered in light of its effect on the airflow in other interfacing ventilation systems. When a system is shut down, positive means of controlling backflow of air to uncontaminated spaces should be provided by positive shutoff dampers, blind flanges, or other devices.

- Equipment to continuously monitor oxygen levels should be provided for occupied working areas of facilities equipped with significant quantities of inert or oxygen-deficient process glovebox lines. Allowable leakage rates for ductwork systems should be taken into consideration.

- The supply of air to primary confinement, such as enclosures that confine the processing of plutonium and enriched uranium, should be filtered by HEPA filters at the ventilation inlets to the enclosures and area confinement barriers to prevent the transport of radioactive contamination in the event of a flow reversal.

- If room air is recirculated, the recirculation circuit should provide at least one stage of HEPA filtration. The design should include redundant filter banks and fans. If recirculation systems are used, contaminated process enclosure air should be prevented from exhausting into the working area rooms. Process enclosure air (from hoods, gloveboxes, etc.) should be treated and exhausted without any potential for recirculation to occupied areas.

- The designer should specify and locate components in the exhaust systems to remove radioactive materials and noxious chemicals before the air is discharged to the environment. These components should be capable of handling combustion products safely. Exhaust system design should safely direct effluents through the appropriate ventilation ducts and prevent spread beyond the physical boundary of the ventilation system until treated.

- HEPA filters should be installed at the interface between the enclosures that confine the process and the exhaust ventilation system to minimize the contamination of exhaust ductwork. Prefilters should be installed ahead of HEPA filters to reduce HEPA filter loading. The filtration system should be designed to allow reliable in-place testing of the HEPA filter and to simplify filter replacement.

- Separate exhaust ventilation system ductwork and the initial two stages of filtration should be designed for exhaust air from enclosures that confine the process (e.g., gloveboxes). These systems should maintain a negative pressure inside the enclosure with respect to the operating area. These systems should be designed to remove moisture, heat, explosive and corrosive gases, and other contaminates. These systems should also be designed to automatically provide adequate inflow of air through a credible breach in the enclosure confinement.

- Enclosures that confine the process and are supplied with gases at positive pressure should have positive-acting pressure-relief valves that relieve the exhaust system to prevent over-pressurization of the process confinement system.

Confinement Systems

Primary confinement consists of barriers, enclosures, gloveboxes, piping, vessels, tanks, and the like that contain radioactive or other hazardous material. Its primary function is to prevent release of radioactive or hazardous material to areas other than those in which processing operations are normally conducted.

Primary confinement of processes that involve readily dispersible forms of material (e.g., solutions, powder or small fragments, gases) is provided by gloveboxes or other confining enclosures. Hoods are used when hazards are acceptably low, as indicated by the quantity of the material involved, the specific operation to be performed, and the hazardous nature and chemical form of material involved. The confinement philosophy described below should be applied to any component that serves a primary confinement function, such as conveyor systems, material transfer stations, and ventilation/off-gas systems.

Breaches in the primary confinement barrier that cannot be totally avoided or ruled out (e.g., due to glove or seal failure) should be compensated for by providing adequate inflow of air or safe collection of spilled liquid. Occasional breaches required for anticipated maintenance should be made only under carefully controlled conditions. Primary confinement should provide for storage of in-process material elsewhere, temporary alternative barriers, and adequate inflow of air to provide contamination control.

The supply and exhaust ventilation system should be sized to maintain in-facility radiation doses at levels ALARA in the event of the largest credible breach. Process equipment and the process itself should be designed to minimize the probability of fire, explosion, or corrosion that might breach the confinement barrier. When handling pyrophoric forms (e.g., chips, filings, dust) of materials in the confinement enclosure, the guidance of DOE-HDBK-1081-94, *Primer on Spontaneous Heating and Pyrophoricity*, should be considered. Halon systems should not be used with pyrophoric metals due to the oxidizing reaction between halon and hot metal.

HEPA Filtration

DOE-STD-3020-2005 defines HEPA filtration as a throwaway, extended-media, dry-type filter with a rigid casing enclosing the full depth of the pleats. The filter shall exhibit a minimum efficiency of 99.97 percent at a test aerosol diameter of 0.3 micrometer.

d. Discuss the reason for, and safety significance of, the following system parameters:
- **Positive versus negative system pressure**
- **Differential pressure across filters**
- **Differential pressure across components**
- **Adequacy of flow across filters versus differential pressure**

Positive Versus Negative System Pressure

According to EPA, *Basic Concepts in Environmental Sciences*, when fans used in industrial systems create gas static pressures above the prevailing atmospheric pressure, the condition is termed positive pressure. When the fans create a gas static pressure below the prevailing atmospheric pressure, negative pressure exists. Both positive and negative pressures are considered relative terms because the static pressure is being described in a form that is compared to the atmospheric pressure.

The static pressure exerted by ambient air is termed either atmospheric or barometric pressure. The atmospheric pressure is an absolute pressure because it is directly related to the number of molecules and their kinetic energy. A barometer measures atmospheric pressure by comparing the pressure of the air against a chamber that approximates a vacuum.

Differential Pressure across Filters or Components

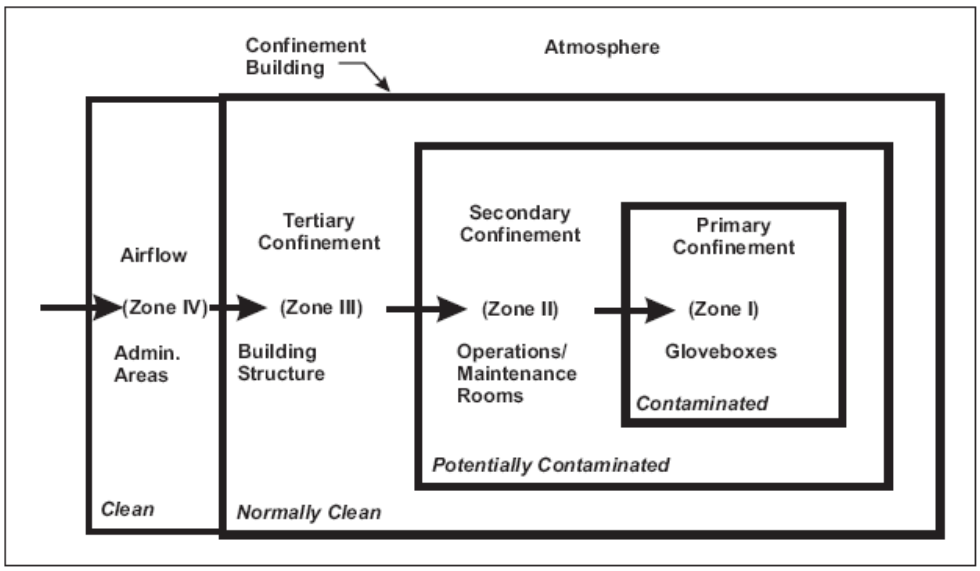
According to the National Institute for Occupational Safety and Health, *A Comparative Evaluation of the Differential-Pressure-Based Respirable Dust Dosimeter with the Personal Gravimetric Respirable Dust Sampler in Underground Coal Mines,* as differential pressure across a filter or a component increases, it indicates an increase in the amount of material

contained in the filters or that settles on the component. For radioactive systems, this may lead to increased radiation levels above what is prescribed in the DSA.

Adequacy of Flow across Filters Versus Differential Pressure

The following is taken from DOE-HDBK-1169-2003.

As shown in figure 8, the general approach to ventilation is a three-tiered relationship. Multi-zoned buildings are usually ventilated to achieve airflows from a relatively less contaminated zone to a relatively more contaminated zone. Thus, airflow must be sufficient to provide the necessary degree of contaminant dilution and cooling, and to maintain sufficient pressure differentials between zones such that there is no backflow of air spaces of lower contamination, even under abnormal conditions.



Source: DOE-HDBK-1169-2003

Figure 8. Typical process facility confinement zones

In the primary confinement zone, i.e., those areas of higher levels of airborne contamination anticipated during normal operations, unavoidable breaches in the primary confinement barrier must be compensated for by an adequate inflow of air or safe collection of any spilled materials. The exhaust system must be sized to ensure an adequate inflow of air in the event of a credible confinement breach.

The secondary confinement zone comprises those areas where airborne contamination could be generated during normal operations or as a result of a breach of a primary confinement barrier. This zone consists of the walls, floors, ceilings, and associated ventilation systems that confine any potential release of hazardous materials from primary confinement. Related areas include glovebox operating areas, hot cell service or maintenance areas, and the ventilation system servicing the operating areas. Pressure differentials must be available to

produce inward airflow into the primary confinement should a breach occur. Penetrations of the secondary confinement barrier typically require positive seals to prevent migration of contamination out of the secondary confinement zone. Air locks or a personnel clothing-change facility are recommended at the entrance to the zone. Restricted access areas are generally included in the secondary confinement zone.

The tertiary confinement zone comprises those areas where airborne contamination is not expected during normal facility operations. This zone consists of the walls, floors, ceilings, and associated exhaust system of the process facility. It is the final barrier against release of hazardous material to the environment. This level of confinement should never become contaminated under normal operating conditions. The secondary and tertiary boundaries may exist in common, as in a single-structure envelope.

The HVAC SSCs must be designed and sized to ensure rated and required airflows that maintain the differential pressures through the zones of a facility. This guarantees the direction of airflow from less contaminated zones to more contaminated zones in normal and abnormal conditions.

e. Discuss the failure modes and potential hazards (to equipment and personnel) associated with the use of HVAC systems and components within nuclear safety-related systems.

The following is taken from American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)/ANSI 62-2001 and DOE-HDBK-1169-2003.

There are several hazards that may be associated with HVAC systems:

- Chemicals used to treat water used in the HVAC system. This is especially true of water treatment additives in the water that is made into steam in a boiler. The chemicals in this steam get into the supply air. ASHRAE/ANSI 62-2001, *Ventilation for Acceptable Indoor Air Quality*, says that steam is the preferred method of humidifying indoor air; therefore, steam is replacing water humidification systems in newer buildings. These systems can be sites for the growth of mold and bacteria.
- Chemicals in the ductwork. There may be volatile organic compounds (VOCs) found in the duct liner, duct sealing caulk, or neoprene gasket. For example, one type of duct liner is coated with a phenol formaldehyde polymer, hexamethylene tetramine. Another kind of duct liner is coated with a resin made of phenol-melamine-formaldehyde. These kinds of linings can emit VOCs that can get into the air and be distributed throughout the ventilation system if they are exposed to ozone gas (from a photocopier, for example). There is usually not a problem with the emitted VOCs, unless they encounter ozone. This is because of an oxidation reaction between the ozone and the chemicals. One study showed that emissions from materials in the HVAC system were responsible for 80 percent of all the indoor emissions of VOCs in that building.
- Refrigerant leakage.
- Improper use of biocides, sealants, or cleaning compounds.

- Leaks such as natural gas or propane leaks that accidentally get pulled into the ventilation system.
- Chemicals from activities going on in the building. These depend on the type of work that is being done in the building and can include ozone, pesticides, lead, and VOCs.

Infectious Diseases

People are more likely to catch infectious diseases in buildings without enough ventilation. When someone coughs or sneezes, they spew a fine mist of droplets that contain an aerosolized virus. If there is not enough ventilation to blow away and disperse the infectious organism, the virus can stick to desks or to doorknobs and live for several hours. Therefore, if someone sneezes close to you and the air is not moving, you have a good chance of becoming infected.

Bacteria and Fungi

There should not be any problems with HVAC systems that are well designed, well maintained, and properly installed. For example, even a properly designed condensate drain system will malfunction and hold water if the pan is not correctly pitched when installed. If they are well maintained, these systems can even improve the quality of indoor air by filtering out mold and pollen that may be present in high concentrations outside and by maintaining proper humidity levels so that mold and fungi do not thrive inside. In one study, even though there was more fungus (mold) collected in the dust of buildings that were mechanically ventilated compared to those that were naturally ventilated, there was less fungus (mold) in the air of mechanically ventilated buildings compared to naturally ventilated ones.

However, if HVAC systems are not properly cleaned and maintained, over time a lot of dirt can accumulate in the ducts and form an ideal breeding ground for fungi and bacteria. Then these microbes may get into the air supply and be blown throughout the building, possibly causing health problems. Bacteria and fungi found in HVAC systems can also trigger allergies, cause infections, and be the source of outbreaks of building-related illnesses such as Legionnaires' disease.

High levels of microbial pollutants have been found on many parts of HVAC systems, including cooling coils, filters, drip pans, humidification systems, and cooling towers.

Ducts can be a particular concern if they are lined with a fiberglass lining since these types of linings can retain moisture. Fiberglass sheets were commonly used for lining the interiors of air supply ducts and air handler compartments of buildings from the early 1960s through the late 1980s. Fiberglass sheeting is an excellent moisture retainer. In laboratory experiments, the fiberglass liner has retained moisture for up to 16 days. As dust gathers in the ducts, mold will begin growing in it. Some inspectors have found mushrooms several inches tall growing inside ventilation systems!

Recirculated Air

In an effort to save energy, there has been as much as a 50 percent decrease in the amount of fresh air brought into some buildings. Some of the HVAC systems in some buildings were not even designed to let in as much fresh air as they should. Recirculating stale air can lead to problems.

Recirculating too much stale air can raise contaminants (e.g., dust, human bioeffluents, and VOCs) to unhealthy levels. Recirculation can also happen if special vents, such as those in bathrooms or smoking rooms, do not exhaust to the outside.

The ventilation and air cleaning systems of a building in which radioactive materials are handled or processed are integral parts of the building's confinement. In some cases, these systems may be shut down in the event of an operational upset, power outage, accident, fire, or other emergency. In other cases, they must remain operational to maintain the airflows and pressure differentials between building spaces and between the building and the atmosphere as required to maintain confinement. In some of these cases, airborne radioactive material may not be a problem until an emergency occurs. In all cases, however, a particular danger is damage to or failure of the final HEPA filters (and adsorbers in those facilities where radiolytic particulates could be released) that constitute the final barrier between the contained space (hot cell, glovebox, room, or building) and the atmosphere or adjacent building spaces. Even if the system can be shut down in the event of an emergency, protection of the final filters is essential to prevent the escape of contaminated air to the atmosphere or to allow personnel to occupy spaces of the building.

Consideration must be given to

- the possible effects of operational upsets, power outages, accidents, fires, and other emergencies on the ventilation and air cleaning systems, including damage to the filters and adsorbers from shock, overpressure, heat, fire, and high sensible-moisture loading;
- the design and arrangement of ducts and air cleaning components to alleviate these conditions;
- the means of switching to a redundant air cleaning unit, fan, or alternate power supply; and
- the methods of controlling or isolating the exhaust system during failure conditions.

To provide the necessary protection to the public and plant personnel, the air cleaning and ventilation system components on which confinement leakage control depends must remain essentially intact and serviceable under these upset conditions. These components must be capable of withstanding the differential pressures, heat, moisture, and stress of the most serious accident predicted for the facility, with minimum damage and loss of integrity, and they must remain operable long enough to satisfy system objectives.

8. Nuclear safety specialists shall demonstrate a familiarity level knowledge of process instrumentation principles of operation as applied to nuclear safety-related systems.

a. Explain the process-related reason for measuring temperature, pressure, flow, and fluid level.

The following definitions are taken from DOE-HDBK-1013/1-92.

Temperature

The hotness or coldness of a piece of plastic, wood, metal, or other material depends upon the molecular activity of the material. Kinetic energy is a measure of the activity of the atoms that make up the molecules of any material. Therefore, temperature is a measure of the kinetic energy of the material in question.

Whether it is the temperature of the surrounding air, the water cooling a car's engine, or the components of a nuclear facility, there must be some means to measure the kinetic energy of the material. Most temperature measuring devices use the energy of the material or system they are monitoring to raise (or lower) the kinetic energy of the device.

Pressure

Although the pressures that are monitored vary slightly depending on the details of facility design, all pressure detectors are used to provide up to three basic functions: indication, alarm, and control. Since the fluid system may operate at both saturation and sub-cooled conditions, accurate pressure indication must be available to maintain proper cooling. Some pressure detectors have audible and visual alarms associated with them when specified preset limits are exceeded. Some pressure detector applications are used as inputs to protective features and control functions.

Flow

Flow measurement is an important process measurement to be considered in operating a facility's fluid systems. For efficient and economic operation of these fluid systems, flow measurement is necessary.

Fluid Level

Remote indication is necessary to provide transmittal of vital level information to a central location, such as the control room, where all level information can be coordinated and evaluated.

There are three major reasons for utilizing remote level indication:

1. Level measurements may be taken at locations far from the main facility.
2. The level to be controlled may be a long distance from the point of control.
3. The level being measured may be in an unsafe/radioactive area.

b. For the temperature detection devices listed, explain how the instrument provides an output representative of the temperature being measured:
- **Thermocouple (TC)**
- **Resistance Temperature Detector (RTD)**

The following definitions are taken from DOE-HDBK-1013/1-92.

Thermocouple (TC)

Thermocouples will cause an electric current to flow in the attached circuit when subjected to changes in temperature. The amount of current that will be produced is dependent on the temperature difference between the measurement and reference junction, the characteristics of the two metals used, and the characteristics of the attached circuit. Heating the measuring junction of the thermocouple produces a voltage that is greater than the voltage across the reference junction. The difference between the two voltages is proportional to the difference in temperature and can be measured on the voltmeter (in millivolts). For ease of operator use, some voltmeters are set up to automatically display temperature through use of electronic circuitry. Other applications provide only the millivolt readout. To convert the millivolt reading to its corresponding temperature, the applicable conversion chart supplied by the manufacturer needs to be used.

Resistance Temperature Detector (RTD)

The RTD incorporates pure metals or certain alloys that increase in resistance as temperature increases and, conversely, decrease in resistance as temperature decreases. RTDs act somewhat like an electrical transducer, converting changes in temperature to voltage signals by the measurement of resistance. The metals that are best suited for use as RTD sensors are pure, of uniform quality, stable within a given range of temperature, and able to give reproducible resistance-temperature readings. Only a few metals have the properties necessary for use in RTD elements. RTD elements are normally constructed of platinum, copper, or nickel. These metals are best suited for RTD applications because of their linear resistance-temperature characteristics, their high coefficient of resistance, and their ability to withstand repeated temperature cycles. The coefficient of resistance is the change in resistance per degree change in temperature, usually expressed as a percentage per degree of temperature. The material used must be capable of being drawn into fine wire so that the element can be easily constructed.

RTD elements are usually long, spring-like wires surrounded by an insulator and enclosed in a sheath of metal. One design has a platinum element that is surrounded by a porcelain insulator. The insulator prevents a short circuit between the wire and the metal sheath. Inconel, a nickel-iron-chromium alloy, is normally used in manufacturing the RTD sheath because of its inherent corrosion resistance. When placed in a liquid or gas medium, the Inconel sheath quickly reaches the temperature of the medium. The change in temperature will cause the platinum wire to heat or cool, resulting in a proportional change in resistance. This change in resistance is then measured by a precision resistance measuring device that is calibrated to give the proper temperature reading.

c. For the pressure detection devices listed, explain how the instrument provides an output representative of the pressure being measured:
- **Magnehelic differential pressure device**
- **Photohelic differential pressure device**

Magnehelic Differential Pressure Device

The following is taken from "Abbreviations and Definitions" in the appendix to EPA 510-R-04-002.

A magnehelic gauge is a sensitive differential pressure or vacuum gauge manufactured by Dwyer Instrument Co. that uses a precision diaphragm to measure pressure differences. This gauge is manufactured in specific pressure or vacuum ranges such as 0 to 2 inches of water column. Magnehelic gauges are typically used to measure soil-vapor extraction system vacuums.

A magnehelic differential pressure device transmits the effects of changes in air pressure from a diaphragm to an indicating pointer by means of magnetic linkage and without the use of gears or other direct mechanical linkages. This system avoids wear and physical contact, which might destroy the accuracy and sensitivity of the instrument. Because it uses no fluid, it eliminates evaporation, freezing, or toxicity problems. It also ensures inertia-free, drift-free pointer movement and offers unusually high resistance to shock and vibration.

The gauges on this device are also unharmed by pressure surges and ambient temperature fluctuations. The device quickly provides gas pressures—positive, negative, or differential.

Because operation does not depend on gravity, the device can be either face- or flush-mounted in any position.

Photohelic Differential Pressure Device

The following is taken from Terrauniversal.com.

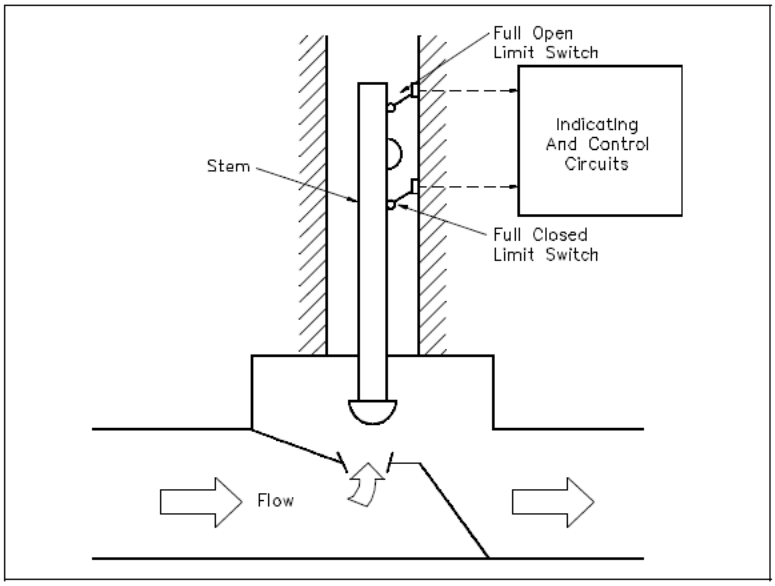
Photohelic gauges use a precise pressure switch to control low and high gas pressures. Knob controls adjust dual set points, which allow for variable dead band control. These set points contain photocells that actuate double-pull double-throw relays when pressures reach a preset upper or lower limit, and they can be set up to control corrective damper action. As the pressure changes in response to damper motion, and the indicator returns to the null band, damper motion is halted.

d. For the position detection devices listed, explain how the detector provides an output representative of the position being represented:
- **Limit switches**
- **Potentiometer**
- **Linear variable differential transformer types**

The following is taken from DOE-HDBK-1013/1-92.

Limit Switches

A limit switch is a mechanical device that can be used to determine the physical position of equipment. For example, an extension on a valve shaft mechanically trips a limit switch as it moves from open to shut or shut to open. The limit switch gives ON/OFF output that corresponds to valve position. Normally, limit switches are used to provide full open or full shut indications as illustrated in figure 9.



Source: DOE-HDBK-1013/1-92

Figure 9. Limit switches

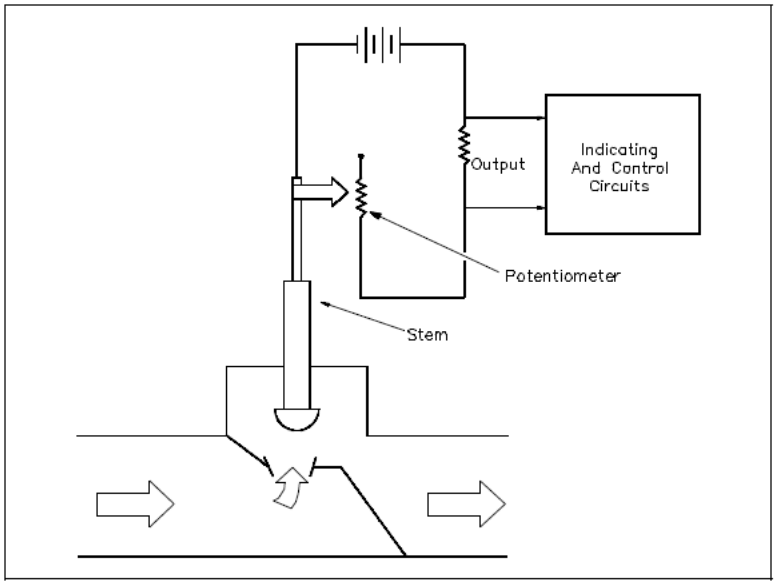
Many limit switches are the push-button variety. When the valve extension comes in contact with the limit switch, the switch depresses to complete, or turn on, the electrical circuit. As the valve extension moves away from the limit switches, spring pressure opens the switch, turning off the circuit.

Limit switch failures are normally mechanical in nature. If the proper indication or control function is not achieved, the limit switch is probably faulty. In this case, local position indication should be used to verify equipment position.

Potentiometer

Potentiometer valve position indicators (figure 10) provide an accurate indication of position throughout the travel of a valve or control rod. The extension is physically attached to a variable resistor. As the extension moves up or down, the resistance of the attached circuit changes, changing the amount of current flow in the circuit. The amount of current is proportional to the valve position.

Potentiometer valve position indicator failures are normally electrical in nature. An electrical short or open will cause the indication to fail at one extreme or the other. If an increase or decrease in the potentiometer resistance occurs, erratic indicated valve position occurs.



Source: DOE-HDBK-1013/1-92

Figure 10. Potentiometer valve position indicator

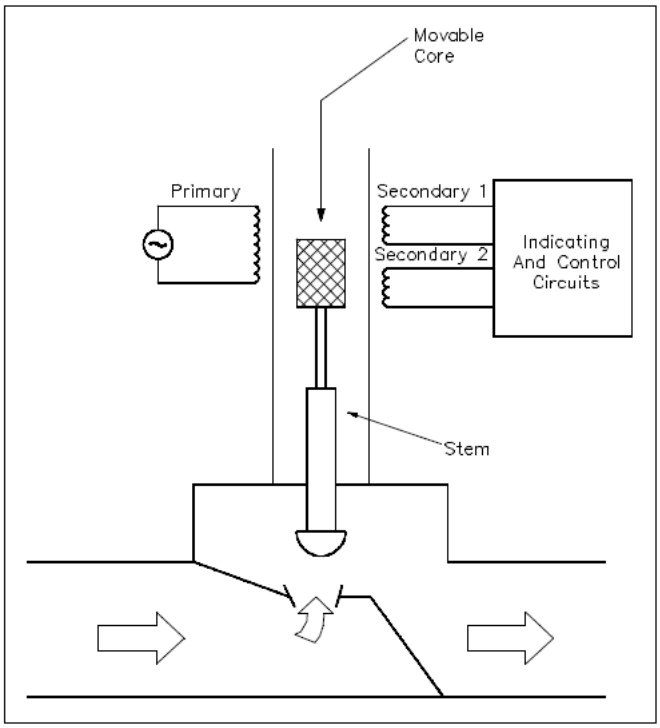
Linear Variable Differential Transformer Types

A device that provides accurate position indication throughout the range of valve or control rod travel is a linear variable differential transformer (LVDT), illustrated in figure 11. Unlike the potentiometer position indicator, no physical connection to the extension is required.

The extension valve shaft, or control rod, is made of a metal suitable for acting as the movable core of a transformer. Moving the extension between the primary and secondary windings of a transformer causes the inductance between the two windings to vary, thereby varying the output voltage proportional to the position of the valve or control rod extension.

Figure 11 illustrates a valve whose position is indicated by an LVDT. If the open and shut position is all that is desired, two small secondary coils could be utilized at each end of the extension's travel.

LVDTs are extremely reliable. As a rule, failures are limited to rare electrical faults that cause erratic or erroneous indications. An open primary winding will cause the indication to fail to some predetermined value equal to zero differential voltage. This normally corresponds to mid-stroke of the valve. A failure of either secondary winding will cause the output to indicate either full open or full closed.



Source: DOE-HDBK-1013/1-92

Figure 11. Linear variable differential transformer

e. Referring to a Piping and Instrumentation Drawing (P&ID) containing temperature, pressure, level, flow, or position detection components, explain their function in the designated system and relationship to system safety.

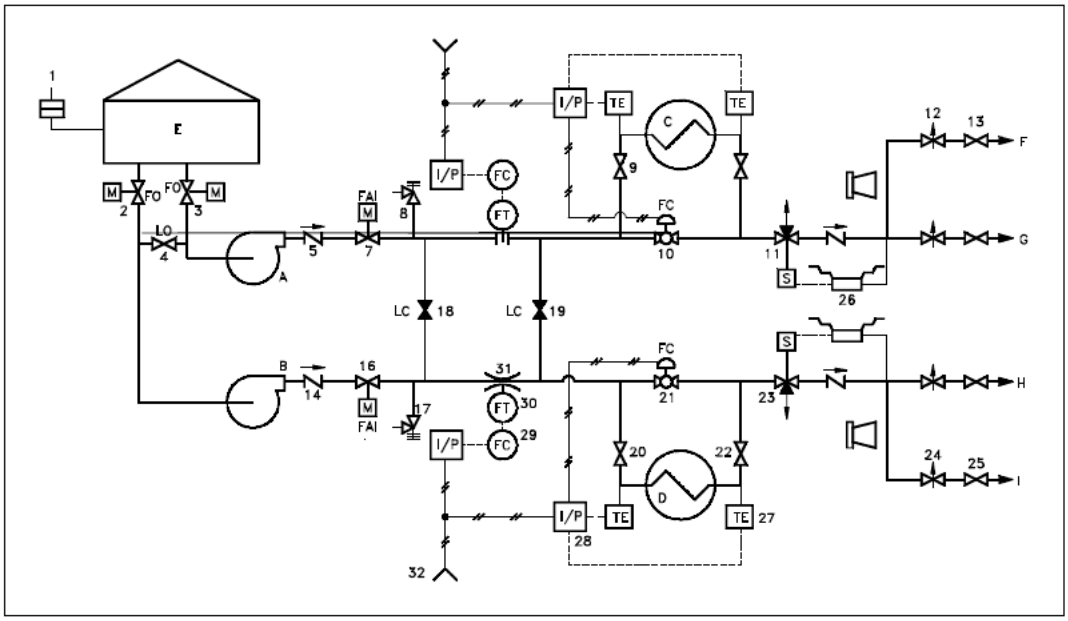
Element e is performance based. The Qualifying Official will evaluate its completion. The following information from DOE-HDBK-1016/1-93 may be helpful.

P&IDs are usually designed to present functional information about a system or component. Examples are piping layout, flowpaths, pumps, valves, instruments, signal modifiers, and controllers, as illustrated in figure 12.

As a rule P&IDs do not have a drawing scale and present only the relationship or sequence between components. Just because two pieces of equipment are drawn next to each other does not indicate that in the plant the equipment is even in the same building; it is just the next part or piece of the system. These drawings only present information on how a system functions, not the actual physical relationships.

Because P&IDs provide the most concise format for how a system should function, they are used extensively in the operation, repair, and modification of the plant.

Additional information related to P&IDs is available in DOE-HDBK-1016/1-93.



Source: DOE-HDBK-1016/1-93

Figure 12. Example P&ID

f. Discuss the importance of safety and process instrumentation to nuclear safety including redundancy and calibration requirements.

Redundancy

According to DOE Order 5480.30, design techniques, such as redundancy, physical separation, functional diversity, or diversity in component design and principles of operation, should be used to prevent loss of the protection function. The protection should be sufficient to ensure that no single failure results in the loss of protection and capability exists to test channels independently to determine failures and loss of redundancy.

The protection system should be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection system leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

According to DOE G 414.1-2A, measuring and test equipment (M&TE) used for inspections, tests, monitoring, and data collection should be calibrated, maintained, and controlled using a documented process. M&TE should be checked before use to ensure that it is of the proper type, range, accuracy, and precision and that it is uniquely identified and traceable to its calibration data. Procedures should be established for testing, retesting, adjusting, and recalibrating M&TE. M&TE should be calibrated to standards traceable to the National Institute of Standards and Technology (NIST) or other nationally recognized standards when appropriate. If no nationally recognized standard exists, the basis for calibration should be

documented. When calibrating and/or checking M&TE for use, consideration should be given to computer programs that are part of the M&TE.

The use of each item of M&TE should be traceable and associated with the item of M&TE. This is because measurements and tests performed with the M&TE may need to be reevaluated if the item of M&TE is subsequently found to be out of its acceptable calibration range. Systems that rely on recording the identity of the M&TE in work packages are ineffective because it is usually almost impossible to review all work packages to identify each use of a particular item of M&TE.

9. Nuclear safety specialists shall demonstrate a familiarity level knowledge of P&ID.

a. Given a P&ID, identify/interpret the symbols used for system components including the following at a minimum:
- **Valves**
- **Pumps**
- **Heat exchangers**
- **Filters/strainers**
- **Fans**
- **Compressors**
- **Instruments**
- **Indicators**
- **Controllers**

The following is taken from DOE-HDBK-1016/1-93.

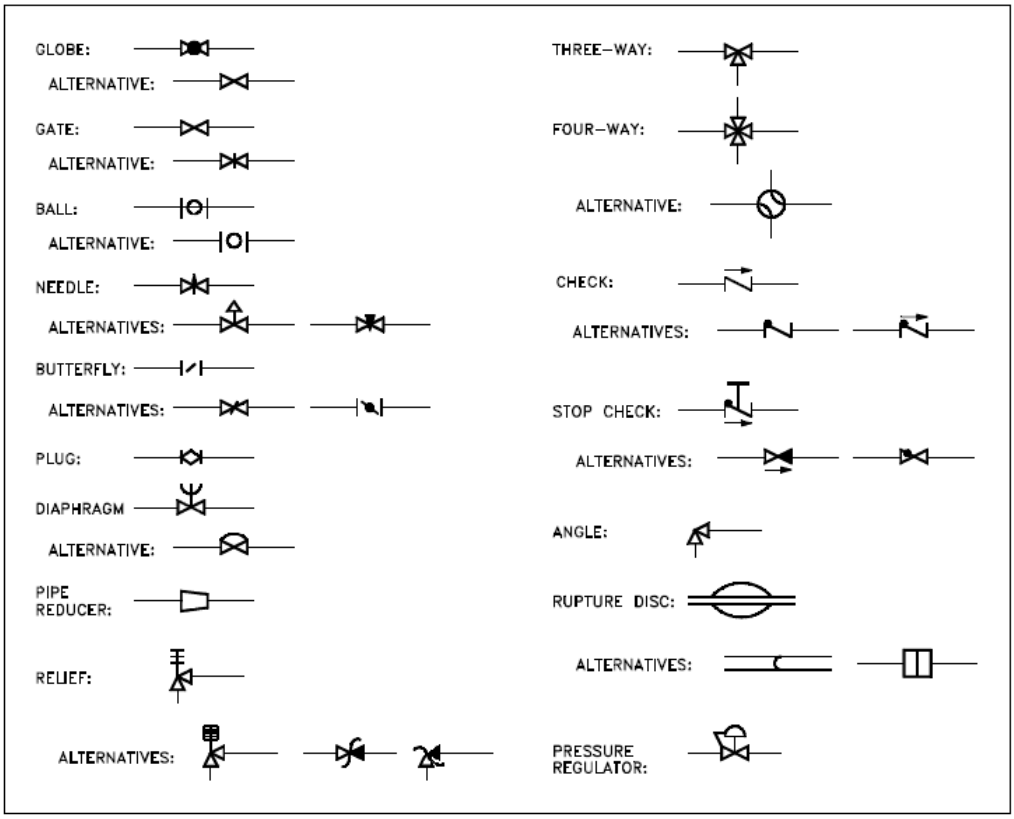
Valves

Valves are used to control the direction, flow rate, and pressure of fluids. Figure 13 shows the symbols that depict the major valve types.

It should be noted that globe and gate valves will often be depicted by the same valve symbol.In such cases, information concerning the valve type may be conveyed by the component identification number or by the notes and legend section of the drawing; however, in many instances even that may not hold true.

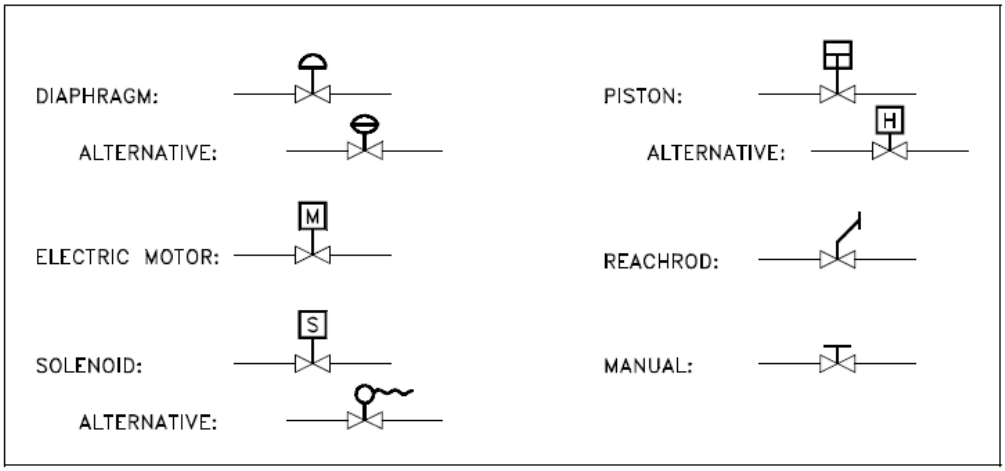
Some valves are provided with actuators to allow remote operation, to increase mechanical advantage, or both. Figure 14 shows the symbols for the common valve actuators. Note that although each is shown attached to a gate valve, an actuator can be attached to any type of valve body. If no actuator is shown on a valve symbol, it may be assumed the valve is equipped only with a hand wheel for manual operation.

The combination of a valve and an actuator is commonly called a control valve. Control valves are symbolized by combining the appropriate valve symbol and actuator symbol, as illustrated in figure 13. Control valves can be configured in many different ways. The most commonly found configurations are to manually control the actuator from a remote operating station, to automatically control the actuator from an instrument, or both.



Source: DOE-HDBK-1016/1-93

Figure 13. Valve symbols

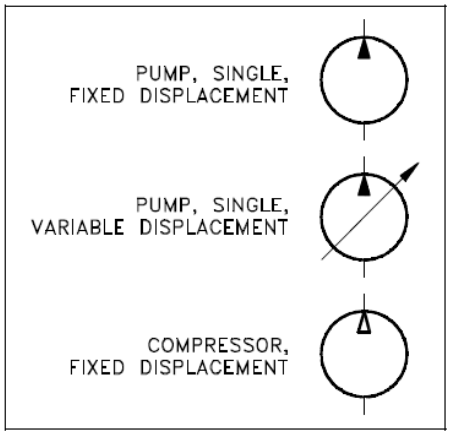


Source: DOE-HDBK-1016/1-93

Figure 14. Valve actuator symbols

Pumps

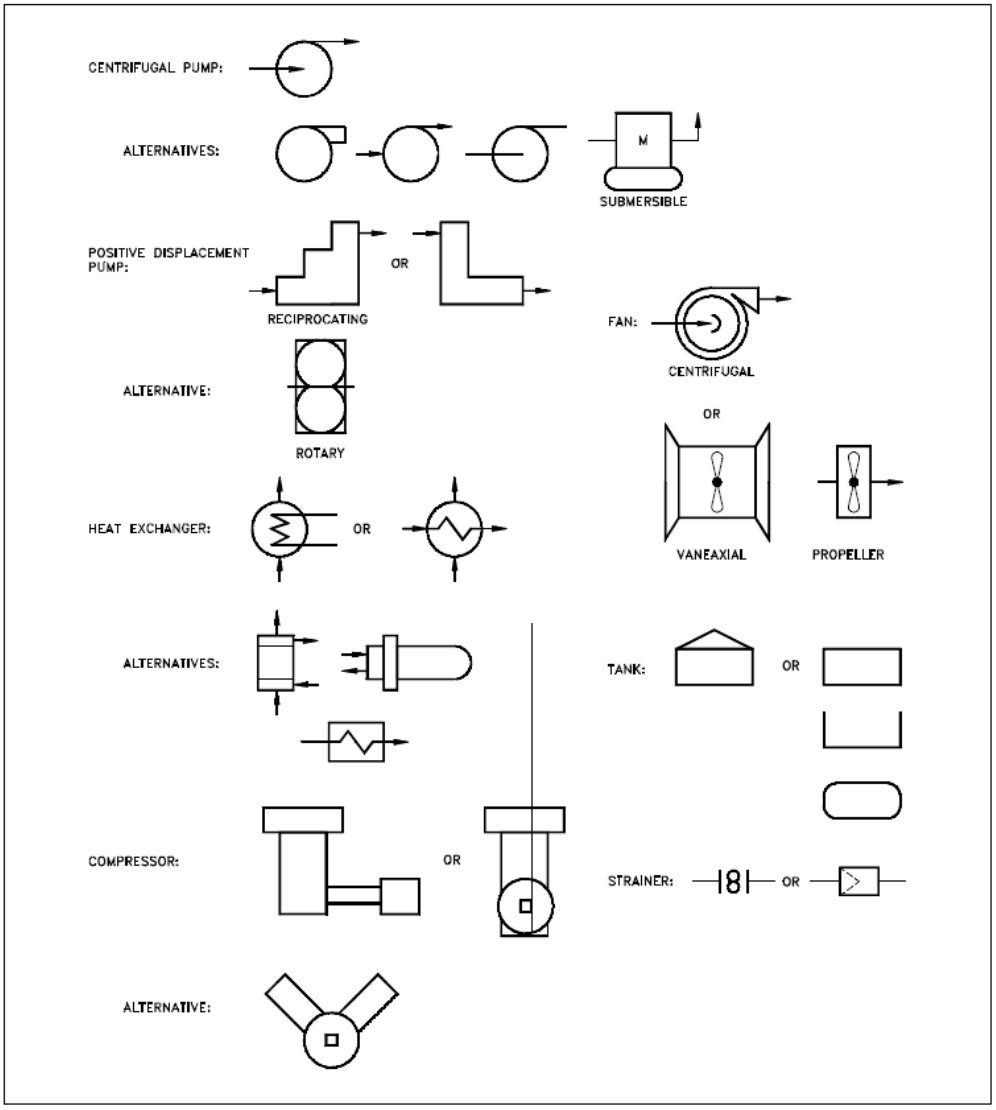
In the broad area of fluid power, two categories of pump symbols are used, depending on the motive media being used (i.e., hydraulic or pneumatic). The basic symbol for the pump is a circle containing one or more arrowheads indicating the direction(s) of flow with the points of the arrows in contact with the circle. Hydraulic pumps are shown by solid arrowheads. Pneumatic compressors are represented by hollow arrowheads. Figure 15 shows common symbols used for pumps (hydraulic) and compressors (pneumatic) in fluid power diagrams.



Source: DOE-HDBK-1016/1-93

Figure 15. Fluid power pump and compressor symbols

Figure 16 shows the engineering symbols for the most common major components, including heat exchangers, strainers, fans, and compressors.



Source: DOE-HDBK-1016/1-93

Figure 16. Symbols for major components

Instruments

One of the main purposes of a P&ID is to provide functional information about how instrumentation in a system or piece of equipment interfaces with the system or piece of equipment. Because of this, a large amount of the symbology appearing on P&IDs depicts instrumentation and instrument loops.

The symbols used to represent instruments and their loops can be divided into four categories.

Generally each of these four categories uses the component identifying (labeling) scheme identified in table 3. The first column of table 3 lists the letters used to identify the parameter being sensed or monitored by the loop or instrument. The second column lists the letters used to indicate the type of indicator or controller. The third column lists the letters used to indicate the type of component. The fourth column lists the letters used to indicate the type of signals that are being modified by a modifier.

Table 3. Instrument identifiers

Sensed Parameter	Type of Indicator or Controller	Type of Component	Type of Signal
F = flow T = temperature P = pressure I = current L = level V = voltage Z = position	R = recorder I = indicator C = controller	T = transmitter M = modifier E = element	I = current V = voltage P = pneumatic

Source: DOE-HDBK-1016/1-93

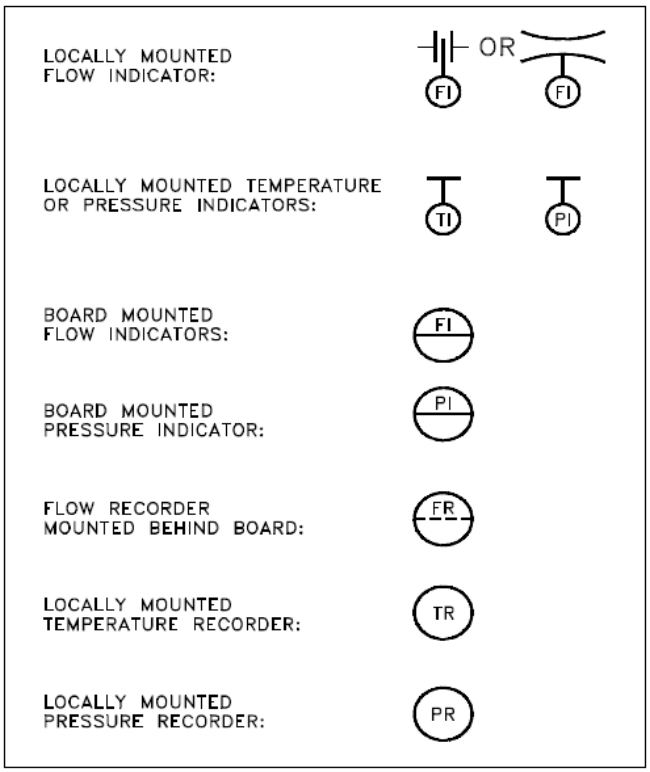
The first three columns above are combined such that the resulting instrument identifier indicates its sensed parameter, the function of the instrument, and the type of instrument. The fourth column is used only in the case of an instrument modifier and is used to indicate the types of signals being modified. The following is a list of example instrument identifiers constructed from table 3:

FIC = flow indicating controller
FM = flow modifier
PM = pressure modifier
TE = temperature element
TR = temperature recorder
LIC = level indicating controller
TT = temperature transmitter
PT = pressure transmitter
FE = flow element
FI = flow indicator
TI = temperature indicator
FC = flow controller

Indicators

Indicators and recorders are instruments that convert the signal generated by an instrument loop into a readable form. The indicator or recorder may be locally or board mounted, and like modifiers and transmitters, this information is indicated by the type of symbol used.

Figure 17 provides examples of the symbols used for indicators and recorders and how their location is denoted.



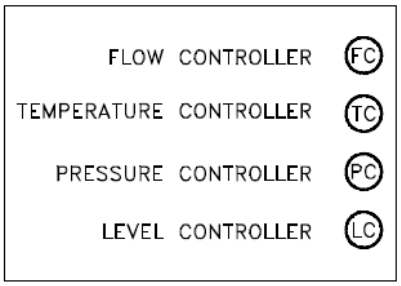
Source: DOE-HDBK-1016/1-93

Figure 17. Indicators and recorders

Controllers

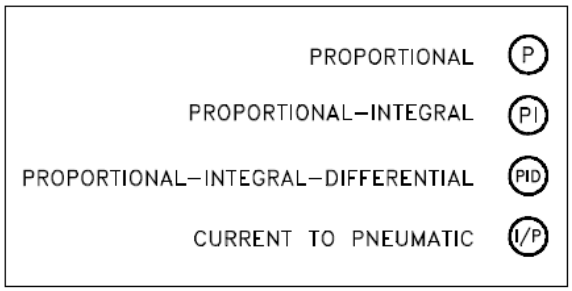
Controllers process the signal from an instrument loop and use it to position or manipulate some other system component. Generally they are denoted by placing a "C" in the balloon after the controlling parameter, as shown in figure 18.

There are controllers that serve to process a signal and create a new signal. These include proportional controllers, proportional-integral controllers, and proportional-integral-differential controllers. The symbols for these controllers are illustrated in figure 19. Note that these types of controllers are also called signal conditioners.



Source: DOE-HDBK-1016/1-93

Figure 18. Controllers



Source: DOE-HDBK-1016/1-93

Figure 19. Signal conditioners

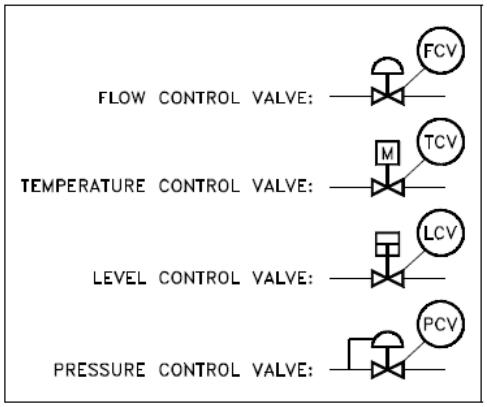
b. Identify how valve conditions (open/closed) are depicted.

The following is taken from DOE-HDBK-1016/1-93.

A control valve may serve any number of functions within a fluid system. To differentiate between valve uses, a balloon labeling system is used to identify the function of a control valve, as shown in figure 20. The common convention is that the first letter used in the valve designator indicates the parameter to be controlled by the valve. For example

- F = flow
- T = temperature
- L = level
- P = pressure
- H = hand (manually operated valve)

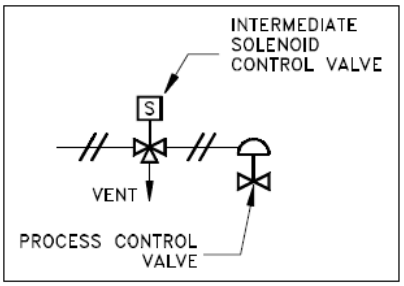
The second letter is usually a “C” and identifies the valve as a controller, or active component, as opposed to a hand-operated valve. The third letter is a “V” to indicate that the piece of equipment is a valve.



Source: DOE-HDBK-1016/1-93

Figure 20. Control valve designations

In many cases, remote control of a valve is accomplished by using an intermediate, small control valve to operate the actuator of the process control valve. The intermediate control valve is placed in the line supplying motive force to the process control valve, as shown in figure 21.



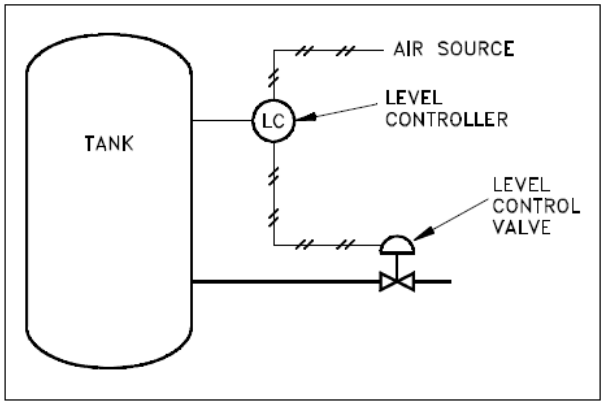
Source: DOE-HDBK-1016/1-93

Figure 21. Remotely controlled valve

In this example, air to the process air-operated control valve is controlled by the solenoid-operated, 3-way valve in the air supply line. The 3-way valve may supply air to the control valve's diaphragm or vent the diaphragm to the atmosphere.

Note that the symbols alone in figure 21 do not provide the reader with enough information to determine whether applying air pressure to the diaphragm opens or closes the process control valve, or whether energizing the solenoid pressurizes or vents the diaphragm. Further, figure 21 is incomplete in that it does not show the electrical portion of the valve control system nor does it identify the source of the motive force (compressed air). Although figure 21 informs the reader of the types of mechanical components in the control system and how they interconnect, it does not provide enough information to determine how those components react to a control signal.

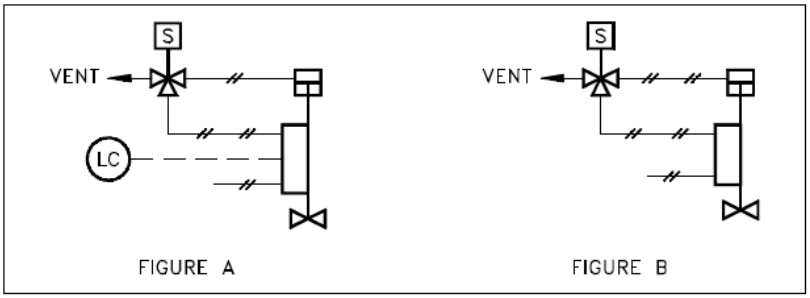
Control valves operated by an instrument signal are symbolized in the same manner as those shown previously, except the output of the controlling instrument goes to the valve actuator. Figure 22 shows a level instrument (designated "LC") that controls the level in the tank by positioning an air-operated diaphragm control valve. Again, note that figure 22 does not contain enough information to enable the reader to determine how the control valve responds to a change in level.



Source: DOE-HDBK-1016/1-93

Figure 22. Level control valve

An additional aspect of some control valves is a valve positioner, which allows more precise control of the valve. This is especially useful when instrument signals are used to control the valve. An example of a valve positioner is a set of limit switches operated by the motion of the valve. A positioner is symbolized by a square box on the stem of the control valve actuator. The positioner may have lines attached for motive force, instrument signals, or both. Figure 23 shows two examples of valves equipped with positioners. Note that, although these examples are more detailed than those of figure 21 and figure 22, the reader still does not have sufficient information to fully determine response of the control valve to a change in control signal.



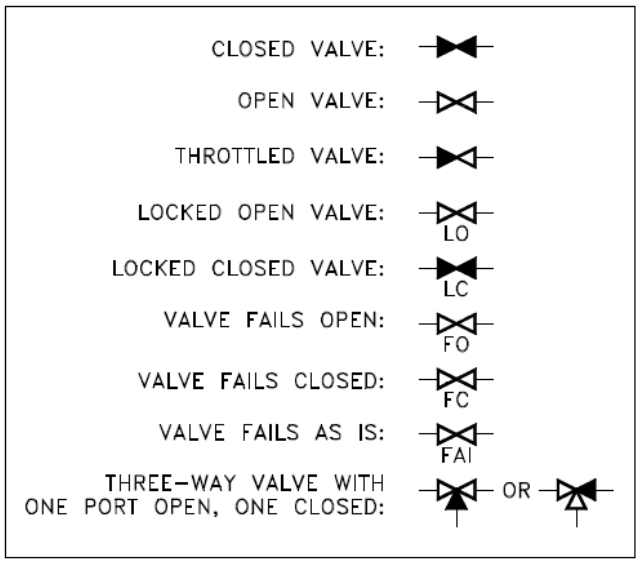
Source: DOE-HDBK-1016/1-93

Figure 23. Control valve with valve positioners

In the A example of figure 23, the reader can reasonably assume that opening of the control valve is in some way proportional to the level it controls and that the solenoid valve provides an override of the automatic control signals. However, the reader cannot ascertain whether it opens or closes the control valve. Also, the reader cannot determine in which direction the valve moves in response to a change in the control parameter. In example B of figure 23, the reader can make the same general assumptions as in example A, except the control signal is unknown. Without additional information, the reader can only assume the air supply provides both the control signal and motive force for positioning the control valve. Even when valves are equipped with positioners, the positioner symbol may appear only on detailed system diagrams. Larger, overall system diagrams usually do not show this much detail and may only show the examples of figure 23 as air-operated valves with no special features.

Before a diagram or print can be properly read and understood, the basic conventions used by P&IDs to denote valve positions and failure modes must be understood. The reader must be able to determine the valve position, know if this position is normal, know how the valve will fail, and in some cases know if the valve is normally locked in that position.

Figure 24 illustrates the symbols used to indicate valve status. Unless otherwise stated, P&IDs indicate valves in their "normal" position. This is usually interpreted as the normal or primary flowpath for the system. An exception is safety systems, which are normally shown in their standby or non-accident condition. Three-way valves are sometimes drawn in the position that they will fail to instead of always being drawn in their "normal" position. This will either be defined as the standard by the system of drawings or noted in some manner on the individual drawings.



Source: DOE-HDBK-1016/1-93

Figure 24. Valve status symbols

c. Determine and follow system flowpath(s).

Element c is performance based. The Qualifying Official will evaluate its completion.

d. Discuss the role of piping and instrumentation diagrams relative to identification of failure modes and mapping fault propagation through networks to support the identification of accident vulnerabilities.

Refer to element b of this competency for a discussion regarding identification of failure modes and the role of piping and instrumentation diagrams.

10. Nuclear safety specialists shall demonstrate a familiarity level knowledge of electrical diagrams and schematics.

a. Given a system diagram, identify/interpret the following symbols:
- **Motors**
- **Transformers**
- **Breakers**
- **Generators**
- **Batteries**

The following is taken from DOE-HDBK-1011/1-92.

The symbols for the various electrical components that will appear on electrical diagrams and schematics are shown in figure 25.

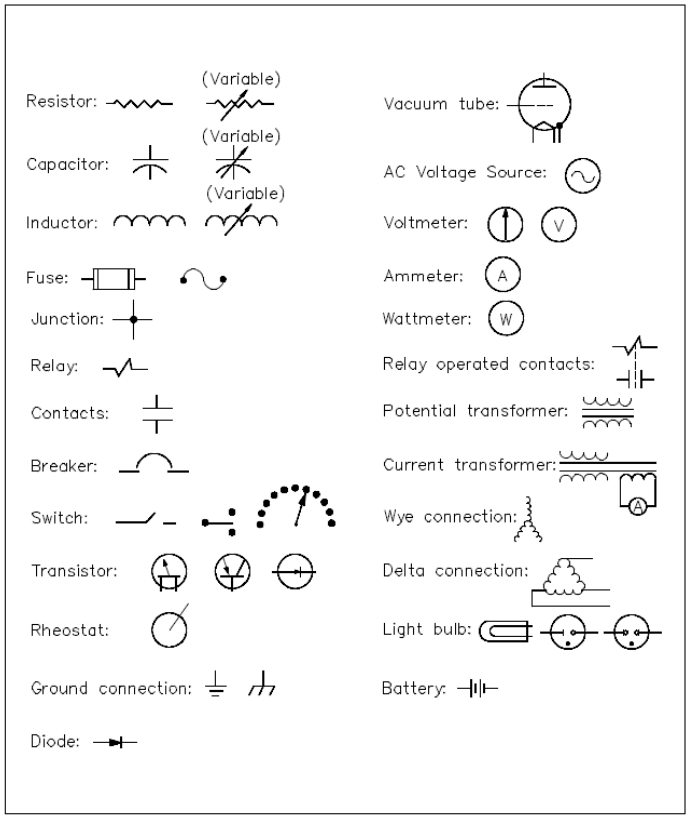
Motors

The following is taken from DOE-HDBK-1016/1-93.

Rotary actuators are generally called motors and may be fixed or variable. Several of the more common rotary symbols are shown in figure 26.

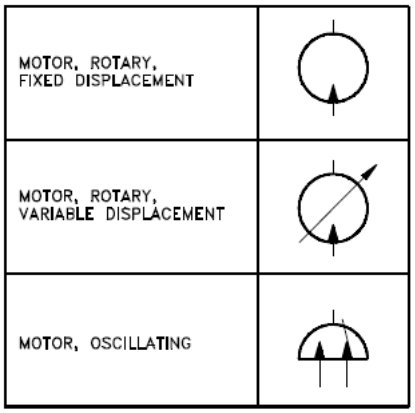
Transformers

The basic symbols for the various types of transformers are shown in figure 27A. Figure 27B shows how the basic symbol for the transformer is modified to represent specific types and transformer applications.



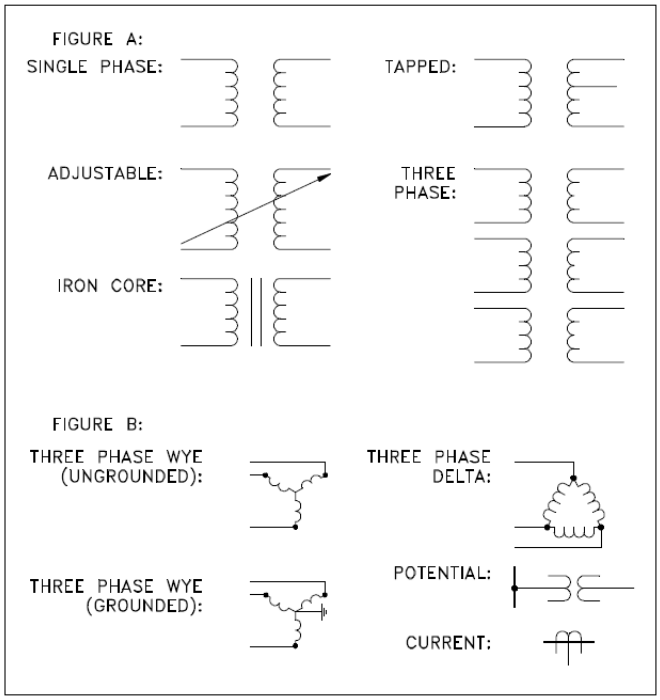
Source: DOE-HDBK-1011/1-92

Figure 25. Electrical symbols



Source: DOE-HDBK-1016/1-93

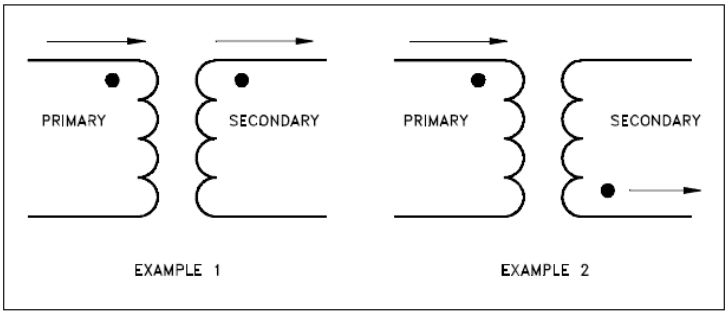
Figure 26. Symbols for motors



Source: DOE-HDBK-1016/1-93

Figure 27. Basic transformer symbols

In addition to the transformer symbol itself, polarity marks are sometimes used to indicate current flow in the circuit. This information can be used to determine the phase relationship (polarity) between the input and output terminals of a transformer. The marks usually appear as dots on a transformer symbol, as shown in figure 28.

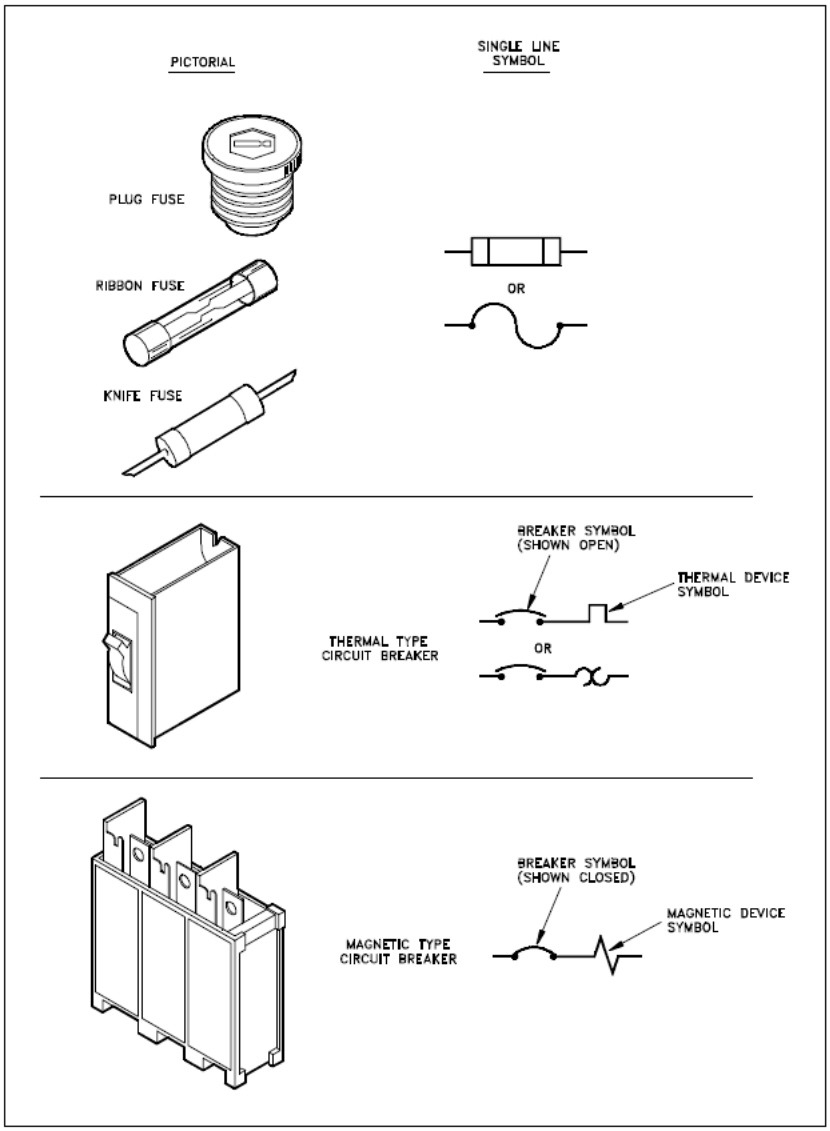


Source: DOE-HDBK-1016/1-93

Figure 28. Transformer polarity

Breakers

Figure 29 depicts basic fuse and circuit breaker symbols for single-phase applications. In addition to the graphic symbol, most drawings will also provide the rating of the fuse next to the symbol. The rating is usually in amperes.

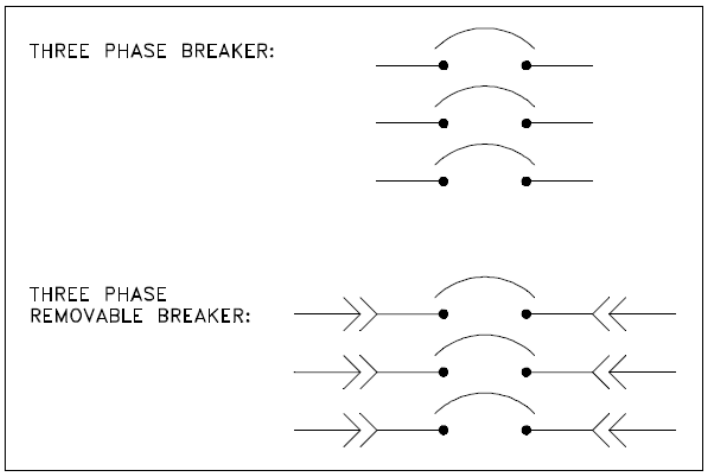


Source: DOE-HDBK-1016/1-93

Figure 29. Fuse and circuit breaker symbols

When fuses, breakers, or switches are used in three-phase systems, the three-phase symbol combines the single-phase symbol in triplicate as shown in figure 30. Also shown is the symbol for a removable breaker, which is a standard breaker symbol, placed between a set of

chevrons. The chevrons represent the point at which the breaker disconnects from the circuit when removed.



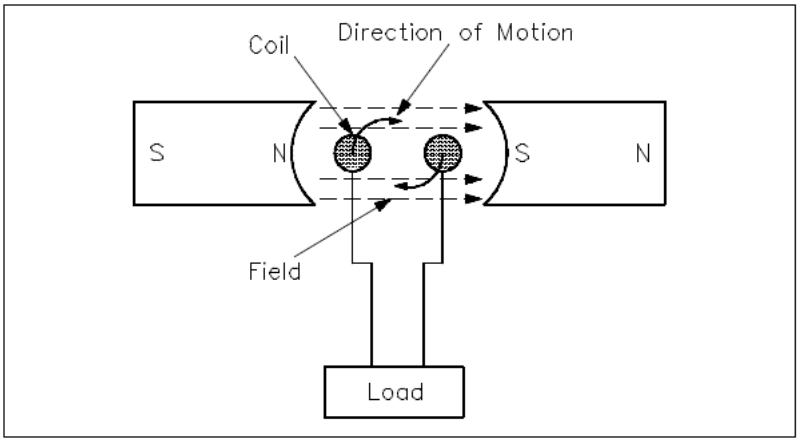
Source: DOE-HDBK-1016/1-93

Figure 30. Three-phase and removable breaker symbols

Generators

The following is taken from DOE-HDBK-1011/1-92.

A generator is a machine that converts mechanical energy into electrical energy by using the principle of magnetic induction. Magnetic induction is used to produce a voltage by rotating coils of wire through a stationary magnetic field, as shown in figure 31, or by rotating a magnetic field through stationary coils of wire. This is one of the most useful and widely employed applications of producing vast quantities of electric power.



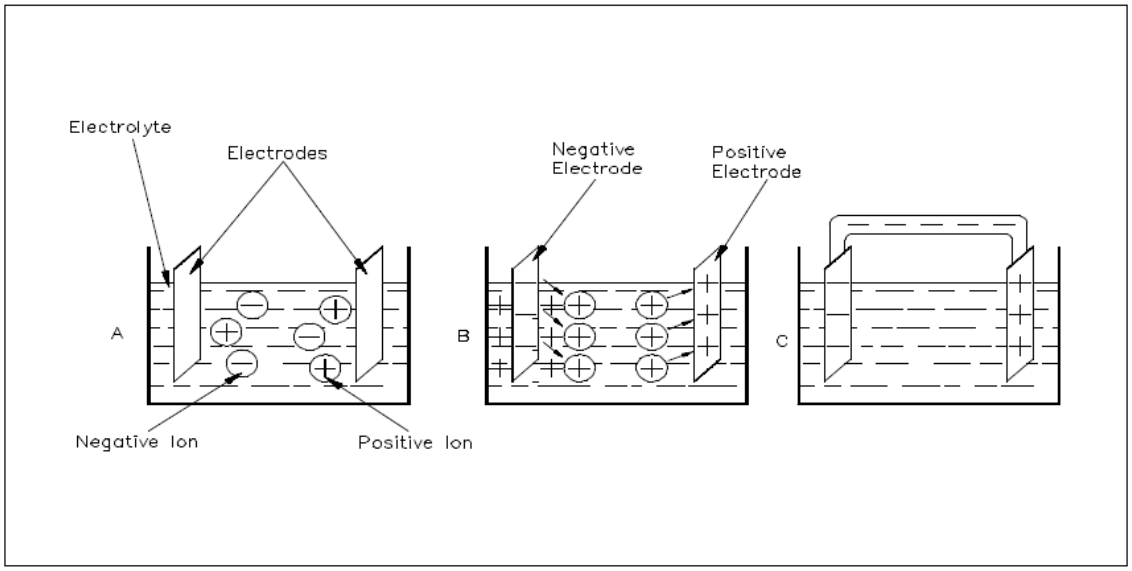
Source: DOE-HDBK-1011/1-92

Figure 31. Generator—electromagnetic induction

Batteries

A battery consists of two or more chemical cells connected in series. The combination of materials within a battery is used for the purpose of converting chemical energy into electrical energy. To understand how a battery works, the chemical cell must be discussed first.

The chemical cell is composed of two electrodes made of different types of metal or metallic compounds that are immersed in an electrolyte solution. The chemical actions that result are complicated, and they vary with the type of material used in cell construction. Some knowledge of the basic action of a simple cell will be helpful in understanding the operation of a chemical cell in general. In the cell, electrolyte ionizes to produce positive and negative ions (figure 32, part A). Simultaneously, chemical action causes the atoms within one of the electrodes to ionize.



Source: DOE-HDBK-1011/1-92

Figure 32. Basic chemical battery

b. Given the appropriate diagram, state the condition (energized/de-energized) in which all electrical devices are shown, unless otherwise noted on the diagram.

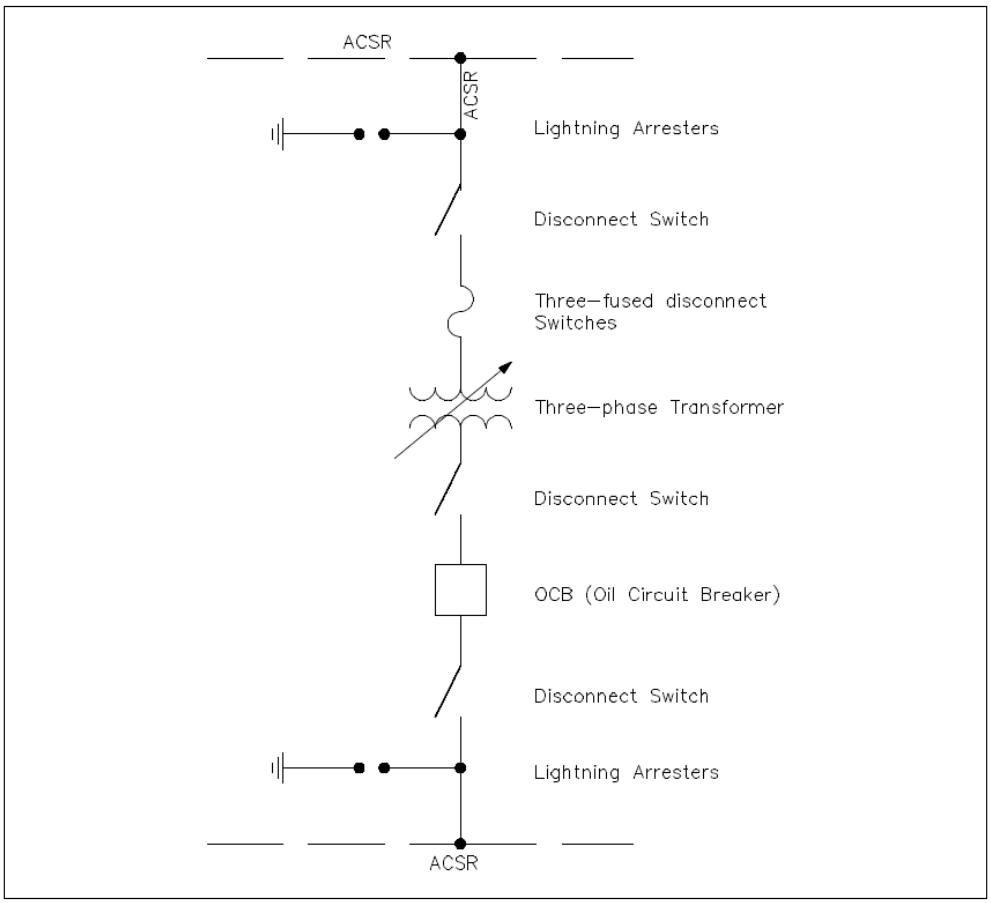
c. Given a system diagram, identify the power sources and/or loads and their status.

Elements b and c are performance based. The Qualifying Official will evaluate their completion.

d. Discuss the role of electrical one-line diagrams for identifying failure modes and for mapping fault propagation through networks to support the identification of accident vulnerabilities.

The following is taken from DOE-HDBK-1011/1-92.

The one-line, or single-line, diagram shows the components of a circuit by means of single lines and the appropriate graphic symbols. One-line diagrams show two or more conductors that are connected between components in the actual circuit. The one-line diagram shows all pertinent information about the sequence of the circuit, but does not give as much detail as a schematic diagram. Normally, the one-line diagram is used to show highly complex systems without showing the actual physical connections between components and individual conductors. As an example, figure 33 shows a typical one-line diagram of an electrical substation.



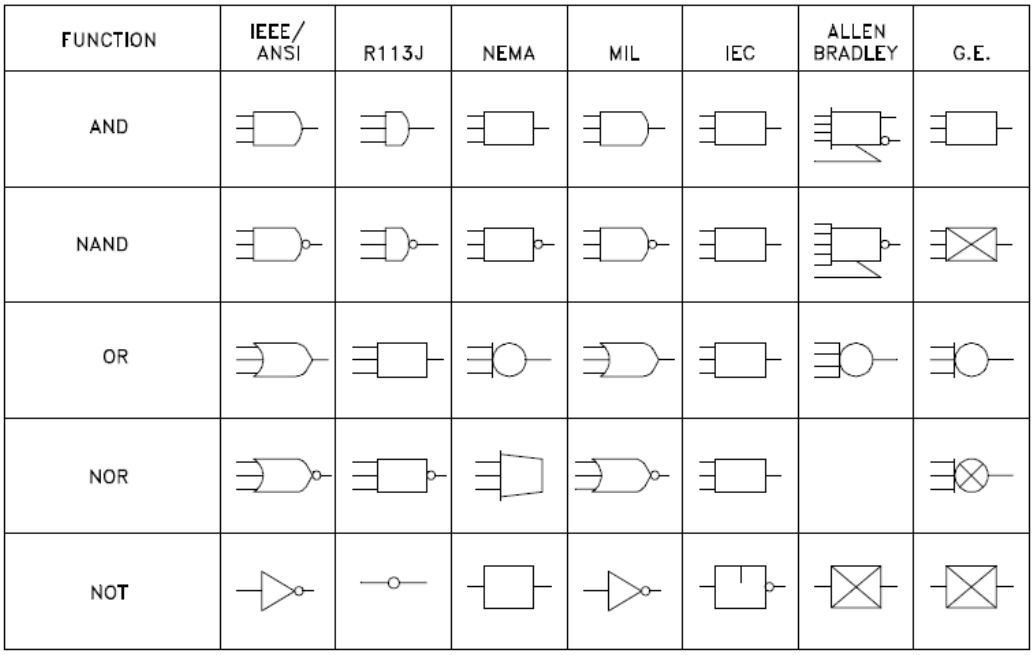
Source: DOE-HDBK-1011/1-92

Figure 33. One-line diagram

11. Nuclear safety specialists shall demonstrate a familiarity level knowledge of electrical logic diagrams.

a. Given a logic diagram, identify/interpret the symbols used on logic diagrams to represent the components.

Element a is performance based. The Qualifying Official will evaluate its completion. The following information from DOE-HDBK-1016/2-93 may be helpful.



Source: DOE-STD-1016/2-93

Figure 34. Basic logic symbols

Basic Logic Circuits

AND gate—provides an output (on) when all its inputs are on. When any one of the inputs is off, the gate's output is off.

OR gate—provides an output (on) when any one or more of its inputs is on. The gage is off only when all of its inputs are off.

NOT gate—provides a reversal of the input. If the input is on, the output will be off. If the input is off, the out put will be on.

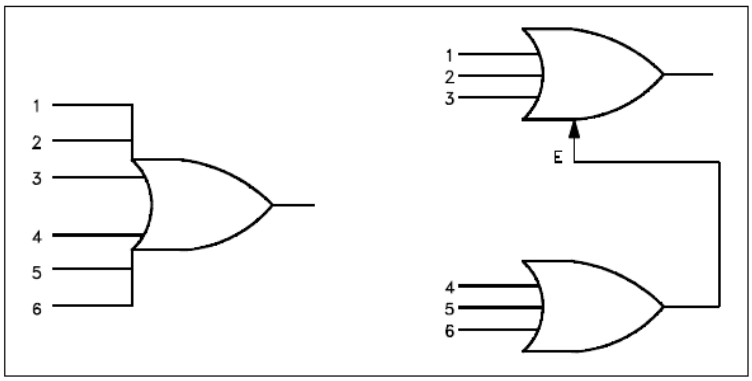
Special "Conjunction" Logic Circuit

NAND gate—is the opposite (NOT) of an AND gate's output. It provides an output (on) except when all the inputs are on.

NOR gate—is the opposite (NOT) of an OR gate's output. It provides an output only when all inputs are off.

COINCIDENCE Gate

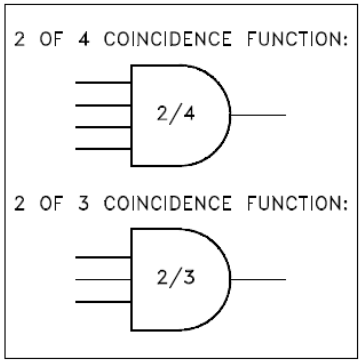
Figure 35 demonstrates two basic ways to show multiple inputs using an OR gate as an example.



Source: DOE-STD-1016/2-93

Figure 35. Conventions for depicting multiple inputs

A common variation of the AND gate is the COINCIDENCE gate, in which there are theoretically no limits to the number of inputs a gate can have. The COINCIDENCE gate behaves as an AND gate except that only a specific number of the total number of inputs needs to be on for the gate's output to be on. See figure 36.



Source: DOE-STD-1016/2-93

Figure 36. Coincidence gate

The fraction in the logic symbol indicates that the AND gate is a COINCIDENCE gate. The numerator indicates the number of inputs that must be on for the gate to be on. The denominator states the total number of inputs to the gate.

EXCLUSIVE Gate

FUNCTION	IEEE/ ANSI	R113J	NEMA	MIL	IEC	ALLEN BRADLEY	G.E.
EXCLUSIVE NOR							
EXCLUSIVE OR							

Source: DOE-STD-1016/2-93

Figure 37. EXCLUSIVE OR and EXCLUSIVE NOR gates

Two variations of the OR gate are

EXCLUSIVE OR—provides an output (on) only when one of the inputs is on. Any other combination results in no output (off).

EXCLUSIVE NOR—is the opposite (NOT) of an EXCLUSIVE OR gate's output. It provides an output (on) only when all inputs are on or when all inputs are off.

b. Given a logic diagram and appropriate information, determine the output of each component and the logic circuit.

Element b is performance based. The Qualifying Official will evaluate its completion. The following information from DOE-HDBK-1016/2-93 may be helpful.

Truth tables to aid in determining logical inputs/outputs:

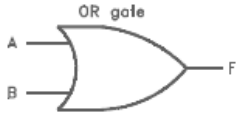
AND gate

INPUT		OUTPUT
A	B	F
0	0	0
0	1	0
1	0	0
1	1	1

NOR gate

INPUT		OUTPUT
A	B	F
0	0	1
0	1	0
1	0	0
1	1	0

OR gate



INPUT		OUTPUT
A	B	F
0	0	0
0	1	1
1	0	1
1	1	1

EXCLUSIVE OR

INPUT		OUTPUT
A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

NAND gate

INPUT		OUTPUT
A	B	F
0	0	1
0	1	1
1	0	1
1	1	0

EXCLUSIVE NOR

INPUT		OUTPUT
A	B	C
0	0	1
0	1	0
1	0	0
1	1	1

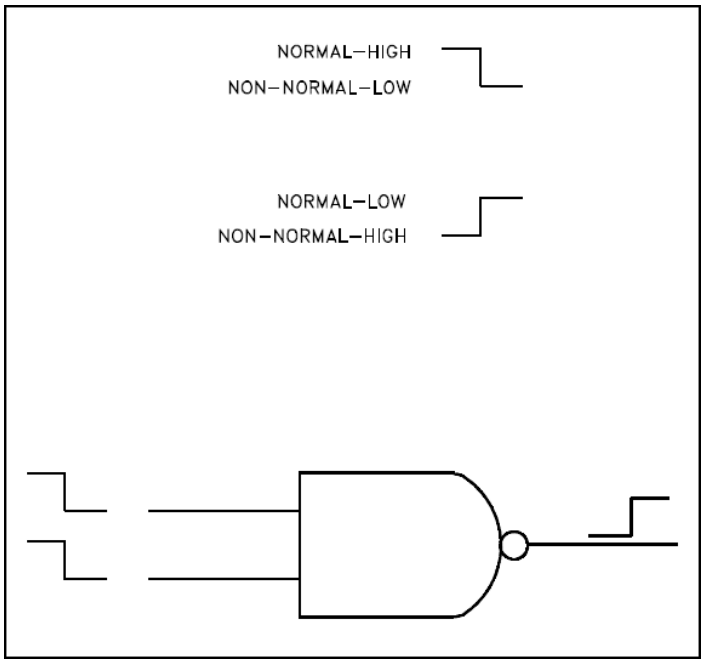
NOT gate

INPUT	OUTPUT
A	F
0	1
1	0

Source: DOE-HDBK-1016/2-93

Figure 38. Truth tables

Reading logic diagrams:



Source: DOE-HDBK-1016/2-93

Figure 39. Logic gate status notations

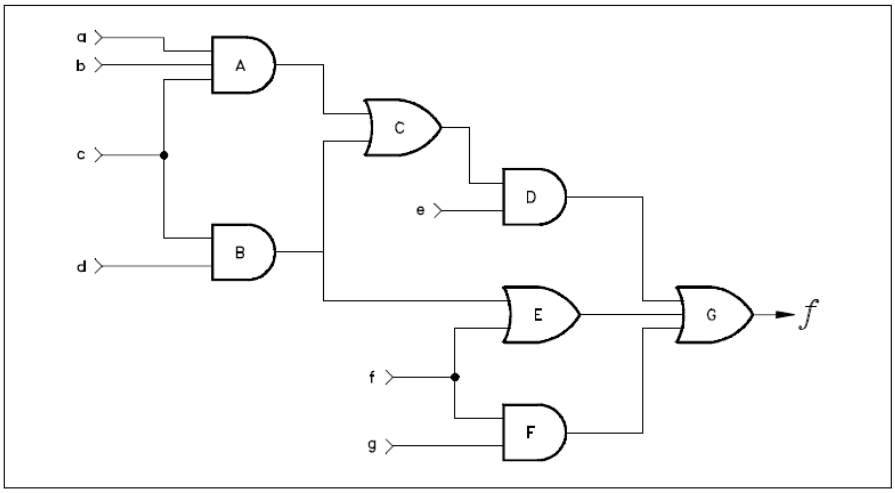
c. Given a logic diagram, identify trip settings and trace the resulting actions should a trip occur.

Element c is performance based. The Qualifying Official will evaluate its completion. The information provided in element d may be helpful.

d. Discuss the role of control logic diagrams in identifying failure modes and for mapping fault propagation through networks to support the identification of accident vulnerabilities.

The following is taken from DOE-HDBK-1016/2-93.

Logic diagrams and prints can be used to depict several types of information. The most common use is to provide a simplified functional representation of an electrical circuit, as illustrated in figure 40. For example, it is easier and faster to figure out how a valve functions and responds to various inputs signals by representing a valve circuit using logic symbols, than by using the electrical schematic with its complex relays and contacts. These drawings do not replace schematics, but they are easier to use for certain applications.



Source: DOE-HDBK-1016/1-93

Figure 40. Example of a logic print

12. Nuclear safety specialists shall demonstrate a working level knowledge of radioactivity and transformation mechanisms.

a. Define "activation."

According to DOE-HDBK-1108-2002 activation is the process of inducing radioactivity by irradiation. The process is commonly referred to as radioactivation or simply activation. Generally, energies above 10 MeV are needed to activate materials for particles other than neutrons.

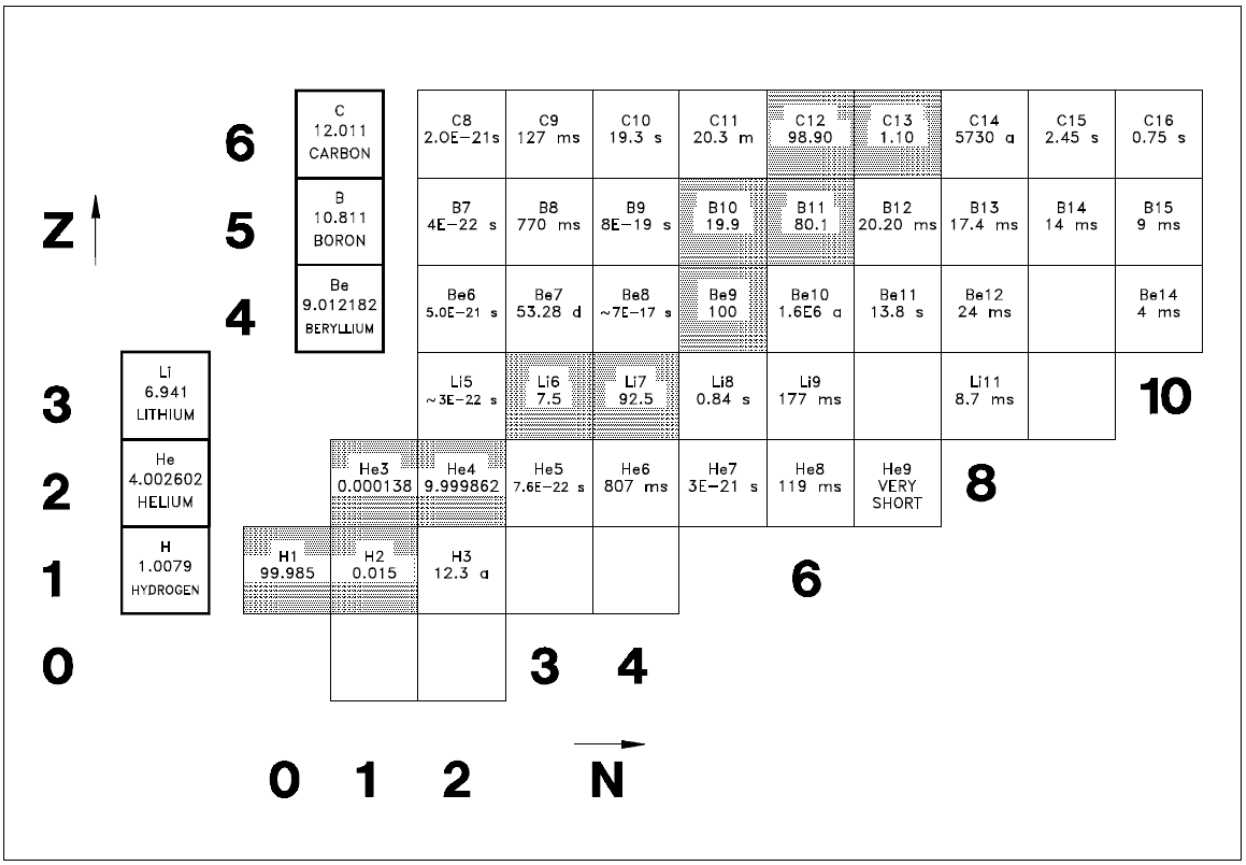
b. Given the "Chart of Nuclides," trace the decay chain for a specified nuclide.

Element b is performance based. The Qualifying Official will evaluate its completion. The following information from DOE-HDBK-1019/1-93 may be helpful.

A tabulated chart called the chart of the nuclides lists the stable and unstable nuclides in addition to pertinent information about each one. Figure 41 shows a small portion of a typical chart. This chart plots a box for each individual nuclide, with the number of protons (Z) on the vertical axis and the number of neutrons (N = A - Z) on the horizontal axis.

The completely gray squares indicate stable isotopes. Those in white squares are artificially radioactive, meaning that they are produced by artificial techniques and do not occur naturally. By consulting a complete chart, other types of isotopes can be found, such as naturally occurring radioactive types (but none are found in the region of the chart that is illustrated in figure 41).

Located in the box on the far left of each horizontal row is general information about the element. The box contains the chemical symbol of the element in addition to the average atomic weight of the naturally occurring substance and the average thermal neutron absorption cross section. The known isotopes (elements with the same atomic number Z but different mass number A) of each element are listed to the right.

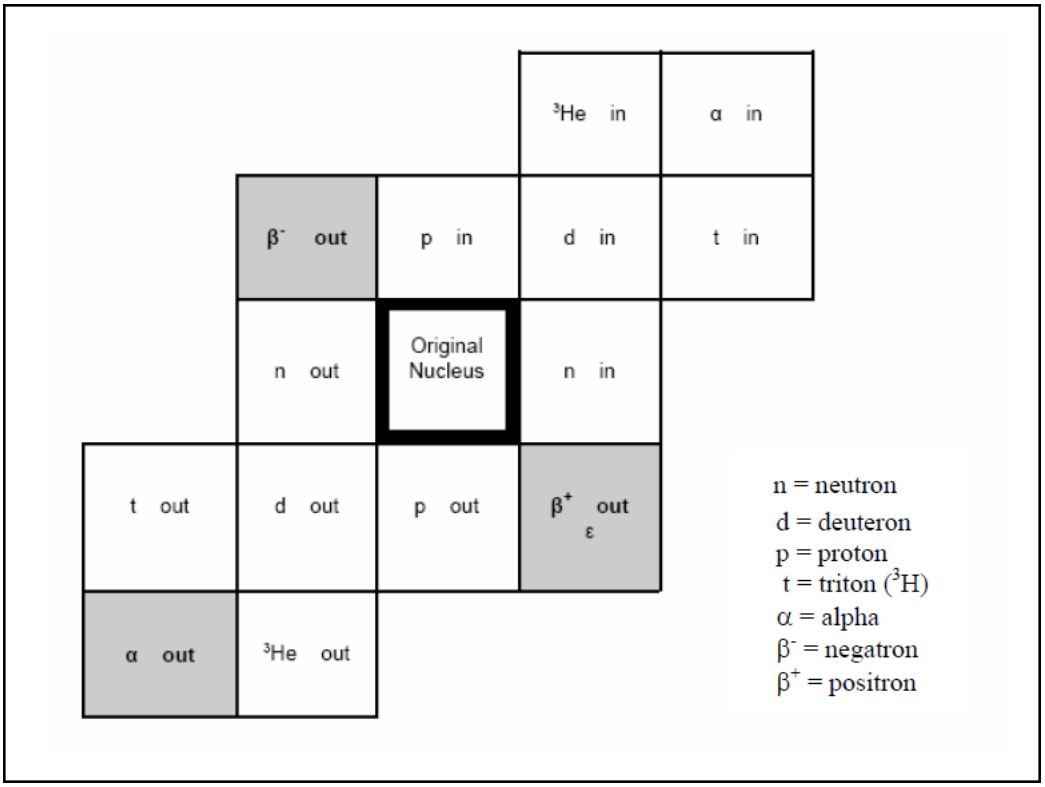


Source: DOE-HDBK-1019/1-93

Figure 41. Nuclide chart for atomic numbers 1 to 6

Depicting Nuclear Processes

As a result of decay, radionuclides shift from block to block within the chart of the nuclides. Figure 42 shows the relative locations of the products of various nuclear processes.



Source: DOE-HDBK-1122-99

Figure 42. Relative locations of the products of various nuclear processes

As can be seen, the relative locations (displacements) of the primary modes of decay are

- alpha (α) down 2, left 2 (9 9, 7 7)
- beta (β-) up 1, left 1 (8 7)
- positron (β+)/EC down 1, right 1 (9 6)

Displacements can also occur as a result of nuclear reactions brought about through bombarding given nuclides with various nuclear particles or gamma photons.

Chart of the Nuclides Summary

The chart of the nuclides provides considerable information about the behavior of nuclides. There is continuity in composition of the nuclides. For example, a line drawn through the stable nuclides forms a rather smooth curve extending from the lower left to the upper right corner of the chart of the nuclides.

Nuclides below this line are characterized by having an excess of neutrons and will, in general, be beta particle emitters.

Nuclides above this line are characterized by having an excess of protons and will, in general, decay by positron emission or electron capture.

Nuclides lying beyond the line of stability will, in general, demonstrate a tendency to seesaw between alpha decay and beta decay. All nuclides, if followed through their various decay schemes will eventually end in a gray box (stable isotope).

The chart presents in compact style much valuable information concerning the properties of the nuclides. These data include

- stable nuclides
  - relative abundance
  - cross section for activation

- radioactive nuclides
  - types of emissions
  - energy of emissions
  - half-life

c. Given either half-life or the radioactive decay constant, solve radioactive decay problems.

The following is taken from DOE-HDBK-1019/1-93.

The Basic Decay Equation

The activity (A) of a sample is the rate of decay of that sample. This rate of decay is usually measured in the number of disintegrations that occur per second. For a sample containing millions of atoms, the activity is the product of the decay constant and the number of atoms present in the sample.

The relationship between the activity, number of atoms, and decay constant is shown in the following equation:

$$A = \lambda N$$

where
A = activity of the nuclide (disintegrations/second)
λ = decay constant of the nuclide (second^{-1})
N = number of atoms of the nuclide in the sample.

Since the decay constant is just that, a constant, the activity and the number of atoms are always proportional.

Variation of Radioactivity over Time

The rate at which a given radionuclide sample decays is stated in the above equation as being equal to the product of the number of atoms and the decay constant. From this basic relationship it is possible to use calculus to derive an expression that can be used to calculate how the number of atoms present will change over time. The derivation is beyond the scope of this text, but the following equation is the useful result:

$$N = N_o e^{-\lambda t}$$

where
N = number of atoms present at time t
N_o = number of atoms initially present
λ = decay constant ($time^{-1}$)
t = time.

Since the activity and the number of atoms are always proportional, they may be used interchangeably to describe any given radionuclide population. Therefore, the following is true:

$$A_t = A_o e^{-\lambda t}$$

where
A_t = activity present at time t
A_o = activity initially present
λ = decay constant $(time)^{-1}$
t = time.

The radioactive half-life is defined as the amount of time required for the activity to decrease to one-half of its original value. A relationship between the half-life and decay constant can be developed from the above equation.

d. Using the specific activity or decay constant of an isotope, convert between mass quantities and curies.

The following is taken from *Introduction to Health Physics,* H. Cember.

Specific activity (SA)—the concentration or radioactivity, or the relationship between the mass of the radioactive material and the activity. It is the number of becquerels or curies per unit mass or volume.

Calculation of the SA of a carrier-free radioisotope (one that is not mixed with any other isotope of the same element):

$$\text{N(atoms)} = \text{Mass(g)} \times \frac{N_A(atoms/mole)}{A(g/mole)}$$

The number of atoms per unit gram consequentially is

$$\text{N(atoms/gram)} = \frac{N_A(atoms/mole)}{A(g/mole)}$$

where
N = number of atoms of the specific radionuclide

N_A = Avogadro's number = 6.03×10^{23} atoms per mole
A = mass number (or atomic weight) of the specific radionuclide.

The relationship between the decay constant and half-life:

$$\lambda = \frac{\ln(2)}{T_{1/2}} = \frac{0.693}{T_{1/2}}$$

The activity per unit (atomic) weight or SA is therefore given by

$$SA = \lambda N = \frac{\lambda \times N_A}{A} = \frac{\lambda \times 6.02 \times 10^{23}}{A}\left(\frac{Bq}{g}\right)$$

Substituting $\frac{0.693}{T_{1/2}}$ for the decay constant λ:

$$SA = \lambda N = \frac{\lambda \times N_A}{A} = \frac{\lambda \times 6.02 \times 10^{23}}{A}\left(\frac{Bq}{g}\right) = \frac{0.693}{T} \times \frac{6.02 \times 10^{23}}{A} = \frac{4.18 \times 10^{23}}{A \times T}\left(\frac{Bq}{g}\right)$$

This may be expressed more conveniently by using the fact that there are approximately 3.7×10^{10} transformations per second in 1 gram of Ra-226. Thus, the SA of Ra-226 is 3.7×10^{10} Bq/g. Thus, the ratio of the specific activity of any isotope SA_i to Ra-226 can be calculated as follows:

$$SA_i = 3.7 \times 10^{10} \times \frac{A_{RA} \times T_{RA}}{A_i \times T_i}\left(\frac{Bq}{g}\right)$$

Or in curies:

$$SA_i = \frac{A_{RA} \times T_{RA}}{A_i \times T_i}\left(\frac{Ci}{g}\right)$$

This works out to:

$$SA_i = \frac{226 \times 1600}{A_i \times T_i}\left(\frac{Ci}{g}\right)$$

for T_1 expressed in years.

13. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the biological effects of radiation.

a. Describe the effects of radiation exposure on the cellular level including:
- **Direct effects**
- **Indirect effects**

The following is taken from *Introduction to Health Physics,* H. Cember.

Radiation damage affects the vital structure of cells. The effects on these cell structures lead to a wide variety of changes within the cell, which can result in death of the cell or the entire organ, and changes in the genetic makeup of an individual that can lead to delayed effects. These effects cannot be distinguished from damage caused by various chemicals and viruses.

There are two general mechanisms of radiation damage in biological systems: direct action and indirect action mechanisms. The direct action mechanism occurs because of direct insult to a molecule by the ionizing radiation and the consequent breakup of the molecule. In this way, radiation can damage cells by changing the structure of various organic molecules such as enzymes, deoxyribonucleic acid, and ribonucleic acid. For example, the molecular structure of enzyme X, which is essential to the formation of energy used by the cell, is changed by radiation. Consequently, energy for the cell can no longer be produced and cell metabolism is disrupted. This disruption causes the cell to die.

The indirect action mechanism occurs when water in the body is irradiated. The water molecule is split. The resulting free radicals can then damage the cell. A free radical is an atom or molecule that has a single unpaired electron in one orbit (as compared to most electron orbits, which have pairs of electrons).

b. Describe the regulatory limits established by the Environmental Protection Agency (EPA) federal guidance reports No. 11 and 13, DOE emergency exposure situations from 10 CFR 835, and EPA protective action guides for nuclear accidents.

Federal Guidance Report No. 11 contains derived guides for control of occupational exposure and exposure-to-dose conversion factors for general application, based on the 1987 Federal radiation protection guidance and follow ICRP 26 and 30 recommendations. It covers internal exposures.

Federal Guidance Report No. 13 contains radionuclide-specific lifetime radiogenic cancer risk coefficients for the U.S. population, based on age-dependent intake, dosimetry, and risk models. It follows the recommendations of ICRP 60.

The regulatory limits of the EPA reports have been incorporated to varying degrees into 10 CFR 835 and 10 CFR 20. It is possible to justify using ICRP-60 based recommendations except for tissue weighting factors, which must come from 10 CFR 835. The DOE radiological evaluation guideline for safety basis accident analyses is 25 rem to the MOI. This is an evaluation guideline and not a dose equivalent limit to be achieved as a goal.

ALARA principles always apply. The 25 rem criterion originated within the NRC, not the EPA.

c. Identify and discuss the range of doses above which one may expect acute radiation illness and early fatalities.

The following is taken from U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, *Acute Radiation Syndrome: Fact Sheet for Physicians*, and *Introduction to Health Physics,* H. Cember.

Acute radiation syndrome (ARS) (sometimes known as radiation toxicity or radiation sickness) is an acute illness caused by irradiation of the entire body (or most of the body) by a high dose of penetrating radiation in a very short period of time (usually a matter of minutes). The major cause of this syndrome is depletion of immature parenchymal stem cells in specific tissues. Although there is no specific cut off as to what an acute dose is, for biological purposes, significant health effects begin to occur above 100 rad received within seconds, minutes, or hours. At high doses and high dose rates, the body is not able to repair cellular damage.

The required conditions for ARS are

- The radiation dose must be large (i.e., greater than 0.7 gray [Gy] 1, 2 or 70 rad).
  - Mild symptoms may be observed with doses as low as 0.3 Gy or 30 rad.

- The dose usually must be external (i.e., the source of radiation is outside of the patient's body).
  - Radioactive materials deposited inside the body have produced some ARS effects only in extremely rare cases.

- The radiation must be penetrating (i.e., able to reach the internal organs).
  - High-energy X-rays, gamma rays, and neutrons are penetrating radiations.

- The entire body (or a significant portion of it) must have received the dose.
  - Most radiation injuries are local, frequently involving the hands, and these local injuries seldom cause classic signs of ARS.

- The dose must have been delivered in a short time (usually a matter of minutes).
  - Fractionated doses are often used in radiation therapy. These are large total doses delivered in small daily amounts over a period of time. Fractionated doses are less effective at inducing ARS than a single dose of the same magnitude.

The three classic ARS syndromes are

1. Bone marrow syndrome (sometimes referred to as hematopoietic syndrome): the full syndrome will usually occur with a dose between 0.7 and 10 Gy (70–1,000 rad) though mild symptoms may occur as low as 0.3 Gy, or 30 rad.

- The survival rate of patients with this syndrome decreases with increasing dose. The primary cause of death is the destruction of the bone marrow, resulting in infection and hemorrhage.

2. Gastrointestinal syndrome: the full syndrome will usually occur with a dose greater than approximately 10 Gy (1,000 rad) although some symptoms may occur as low as 6 Gy, or 600 rad.
   - Survival is extremely unlikely with this syndrome. Destructive and irreparable changes in the gastrointestinal tract and bone marrow usually cause infection, dehydration, and electrolyte imbalance. Death usually occurs within 2 weeks.

3. Cardiovascular/central nervous system syndrome: the full syndrome will usually occur with a dose greater than approximately 50 Gy (5,000 rad) although some symptoms may occur as low as 20 Gy, or 2,000 rad.
   - Death occurs within 3 days. Death likely is due to collapse of the circulatory system as well as increased pressure in the confining cranial vault as the result of increased fluid content caused by edema, vasculitis, and meningitis.

As a group, the effects caused by acute doses are called deterministic. This means that the severity of the effect is determined by the amount of dose received. Deterministic effects usually have some threshold level below which the effect will probably not occur, but above which the effect is expected. When the dose is above the threshold, the severity of the effect will increase with increasing absorbed dose.

Acute whole body doses in the range of greater than 400–450 rad, may result in the statistical expectation that 50 percent of the population exposed will die within 60 days without medical treatment. This is the LD50/60.

Other acute effects:
- 200 to 300 rad to the skin—erythema (reddening of the skin)
- 125 to 200 rad to the ovaries—prolonged to permanent suppression of menstruation in about 50 percent of women
- 600 rad to the ovaries or testicles—permanent sterilization
- 50 rad to the thyroid—benign (non-cancerous) tumors

14. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the principles and use of radiological instrumentation and radiological monitoring/survey practices.

a. Discuss the purpose, principles of detection and operation, and field application of the following:
- **Continuous Air Monitors (CAM), including tritium alarms**
- **Area Radiation Monitors (ARM)**
- **Criticality detection/alarm systems**
- **Process radiation monitors**

Continuous Air Monitors (CAM), Including Tritium Alarms

The following is taken from DOE-HDBK-1079-94.

Airborne contamination monitors should meet the ANSI N317 criteria.

The primary purpose of any CAM is to detect the presence of airborne radioactivity and activate an alarm to warn personnel in the area so actions can be taken to minimize personnel exposures. The goal for any CAM should be to perform this function as quickly as possible and at the lowest detectable level of radioactive airborne concentration. The quantity of airborne radioactivity that will result in an alarm within a given time interval is defined in units of DAC-hour (h) for a particular radionuclide and is a function of the nuclide's airborne concentration in DACs, the sampling rate, the lower limit of detection of the instrument, and the time needed for the alarm to occur.

A DAC-h is the product of the concentration of the radioactive material in air, expressed as a fraction or multiple of the DAC for each radionuclide and the time of exposure to that radionuclide in hours.

At DOE facilities, the emphasis in the occupational setting is often devoted to detecting the presence of alpha-emitting transuranics such as plutonium and americium. Beta CAMs are also used.

Principles of Detection and Operation

CAMs basically function by employing a flow system to steadily draw air, containing radioactive particulates, gases, or vapors, into the monitor. Particulates are deposited on a collection substrate. For alpha radioactivity measurements, solid state detectors (typically a surface barrier or diffused junction semiconductor) work in concert with a multichannel analyzer to detect, record, and identify the radionuclide(s) of interest, and analyze the energy distribution. Zinc sulfide scintillators are also used, but for detection purposes only.

Beta particulate CAMs primarily employ gas proportional counters and/or silicon surface barrier detectors to record radiation events. Air monitors utilizing beta (plastic) scintillators, Geiger-Mueller (G-M) detectors, and ionization chambers are being phased out, principally because of problems associated with radon progeny rejection. Those monitors employing G-M detectors tend to be larger and heavier than other CAMs because of the shielding materials required to reduce the background radiation levels.

Radioactive gases and vapors containing beta emitters are primarily collected using proportional counters and beta scintillators. Ionization chambers have also been used, but only for tritium. The larger the chamber, the more sensitive the measurement becomes.

Most CAMs separate airborne particulates through the filtration process where a physical barrier (a filter) removes particulates from the air stream. To a lesser extent, the process of inertial impaction—the removal of particulates that, due to their inertia, cannot make a bend in the air stream and are therefore impacted—is used in some CAM designs. Inertial

impactors either deposit the particulates on a detector or on a collection substrate placed over the detector.

Field Application

Air sampling equipment should be positioned to measure air concentrations to which individuals are exposed. If this cannot be achieved, a program of personal breathing-zone air sampling should be initiated. Air monitoring equipment shall be routinely calibrated and maintained on an established frequency. Air monitoring equipment should be calibrated at least once each year. CAMs should be capable of measuring 1 DAC when averaged over 8 hours (8 DAC-h) under laboratory conditions. Real-time air monitoring equipment should have alarm capability and sufficient sensitivity to alert individuals that immediate action is necessary to minimize or terminate inhalation exposures. A technical basis document should be developed for the airborne radioactivity monitoring program. The technical basis document should provide the basis for air monitor selection, placement, and operation. The proper operation of CAMs should be verified daily by performing an operational check. Operational checks should include positive air-flow indication, non-zero response to background activity, and internal check sources or 60 hertz electronic checks when available. Real-time air monitoring equipment operation should be verified weekly by checking for instrument response with a check source or with ambient levels of radon daughters.

Area Radiation Monitors (ARM)

The following is taken from DOE-STD-1098-99.

Purpose

ARMs are used to control radiation exposures in a workplace setting.

Principles of Detection and Operation

A variety of ARM systems exist to detect gamma and neutron radiation. Emphasis is typically placed on the detection of gamma radiation intensities throughout the facility. To satisfy that objective, ARMs are either wall-mounted or operated as freestanding units in areas requiring monitoring. These devices tend to be fairly rugged and versatile, yet compact and lightweight. G-M or ionization chamber detectors are typically used. Depending on the detector, energy compensation is provided to allow a flat roentgen (R) response versus gamma energy. Radiation levels ranging from 0.01 milliroentgens (mR)/h up to 10,000 R/h are typical.

ARMs are designed to provide normal/fail indicators for safe operation. Remote indicators are available that include meter, audible, and visual alarms. High-radiation alarms and alarms designed to “alert” the worker that an alert level has been exceeded can be set over the entire meter range. Audible alarms often consist of a horn; visual alarms employ a light or beacon, which may flash on and off depending on the design.

ARMs for slow neutron detection can use proportional counters by taking advantage of any number of charged particle reactions, including B-10 (n, alpha) reaction, He-3 (n,p) reaction,

and Li-6 (n, alpha) reaction. Because charged particles are generated in these reactions, scintillation materials such as zinc sulfide can be used to detect neutrons. Other means of slow neutron detection are fission chambers, which contain fissile material that interacts with thermal neutrons causing fission. The neutron flux is measured by the intensity of the gamma radiation given off during fission.

Fast neutron detection usually incorporates a moderator such as paraffin to thermalize fast neutrons to induce a slow neutron reaction (discussed above). Fast neutrons can be detected by using scintillation materials with a high hydrogen content to produce a proton. Scintillation materials containing hydrogen include anthracene and stilbene.

Field Application

From a regulatory perspective, the use of stationary (area) or portable radiation instrumentation for the purpose of measuring ambient radiation dose rates is required under 10 CFR 835.403(b). The *U.S. Department of Energy Radiological Control Manual* (Article 553) recommends the following:

- ARMs should be
  - installed in frequently occupied areas where the potential exists for unanticipated increases in dose rates;
  - placed in remote locations where a need for local indication of dose rates prior to personnel entry exists;
  - used to measure only the radiation for which the calibration is valid;
  - tested at least quarterly to verify audible alarm system operability and audibility under ambient working conditions, as well as operability of visual alarms, when so equipped.

- The need and placement of an ARM should be documented and assessed when changes to facilities, systems, or equipment occur.
- Where an ARM is incorporated into a safety interlock system, the circuitry should be such that a failure of the monitor should either prevent entry into the area or prevent operation of the radiation producing device.
- ARMs should not be substituted for radiation exposure surveys in characterizing a workplace.
- If installed instrumentation is removed from service for maintenance or calibration, a radiation monitoring program providing at least equal detection capability should be maintained, consistent with the potential for unexpected increases in radiation dose rates.

Criticality Detection/Alarm Systems

As specified in ANSI/ANS-8.3, the need for a criticality accident alarm system (CAAS) shall be evaluated for all activities in which the inventory of fissionable material in individual unrelated work areas exceeds 700 grams of U-235, 520 grams of U-233, 450 grams of Pu-239, or 450 grams of any combination of these three isotopes.

- If the fissionable material mass exceeds the ANSI/ANS-8.3 limits and the probability of criticality is greater than 10^{-6} per year, a CAAS shall be provided to cover occupied

areas in which the expected dose exceeds 12 rad in free air. Nuclear accident dosimetry shall also be provided. The CAAS should include a criticality detection device and a personnel evacuation alarm.

- If the fissionable material mass exceeds the ANSI/ANS-8.3 limits and the probability of criticality is greater than 10^{-6} per year, but there are no occupied areas in which the expected dose exceeds 12 rad in free air, then only a criticality detector system (i.e., nuclear accident dosimetry) is needed.

- If the fissionable material mass exceeds the ANSI/ANS-8.3 limits, but a criticality accident is determined to be impossible or less than 10^{-6} per year (per a safety analysis report documentation), then neither a criticality alarm nor nuclear accident dosimetry is needed.

The alarm signal shall be for immediate evacuation purposes only and of sufficient volume and coverage to be heard in all areas that are to be evacuated. Information on sound levels of the alarm can be found in ANSI/ANS-8.3. The alarm trip point shall be set low enough to detect the minimum accident of concern. The minimum accident of concern may be assumed to deliver the equivalent of an absorbed dose in free air of 20 rad at a distance of 2 meters from the reacting material within 60 seconds. The alarm signal shall activate promptly (i.e., within 0.5 second) when the dose rate at the detectors equals or exceeds a value equivalent to 20 rad/minute at 2 meters from the reacting material. A visible or audible warning signal shall be provided at a normally occupied location to indicate system malfunction or loss of primary power. Each alarm system should be tested at least once every 3 months. An evacuation drill shall be conducted at least annually.

Criticality accident alarm systems may consist of one to several detectors per unit. In multi-detector units (e.g., three detectors), at least two detectors shall be at the alarm level before initiating the alarm; in redundant systems, failure of any single channel shall not prevent the CAAS from functioning.

Process Radiation Monitors

Process radiation monitors are monitors that are used just like the ARMs, but which are applied for a certain process or operation.

Process radiation monitors are designed to detect concentrations of liquid and gaseous radioactivity in work areas, stacks, ducts, laboratories, etc. A variety of these systems exists and is routinely used as indicators of normal and abnormal system operating conditions. They may also provide an estimate of the quantity of radioactivity released to the environment.

DOE/EH-0173T, *Environmental Regulatory Guide for Radiological Effluent Monitoring and Environmental Surveillance*, addresses liquid and gaseous effluent monitoring in chapters 2 and 3, respectively. Both chapters are intended to assist each DOE-controlled facility meet the requirements of DOE Order 5400.5, *Radiation Protection of the Public and the Environment.*

Monitoring of liquid wastes should be performed to

- demonstrate compliance with DOE Order 5400.5 (specifically chapter 2, "Requirements for Radiation Protection of the Public and the Environment")
- quantify radionuclides released from each discharge point
- alert appropriate personnel of upsets in processes and emissions controls

Continuous radionuclide monitoring is recommended for routine releases that could exceed one derived concentration guide (DCG) at the release point when averaged over 1 year, or unanticipated releases exceeding one DCG averaged over 1 year. Continuous sampling combined with frequent analyses can substitute for continuous monitoring if emissions cannot be detected by technically current continuous monitoring devices. Appropriate statistical parameters should be considered to determine the accuracy of sampling results.

The level of monitoring effort is determined by the importance of the sources during routine operations and the potential for accidental releases to the environment and dose to the general public.

Performance standards for a liquid effluent monitoring system are based on a careful characterization of several parameters. These include the source(s), pollutant(s), sample collection system(s), treatment system(s), and final release point(s) of the effluents.

If a facility is new or has been modified, a preoperational assessment is recommended to determine the impact on effluent release quantity, quality, and sensitivity of the monitoring or surveillance system. This assessment should be used to determine liquid effluent types and quantities, and facility monitoring needs. It is important that the system perform to a level that allows compliance with DOE Order 5400.5 (specifically, being able to detect radionuclide concentrations at or below the DCG in addition to meeting reporting requirements). Sufficient sensitivity regarding statistical detection levels is advocated.

Performance standards include consideration of continuous monitoring/sampling, sampling systems, calibration of monitoring and sampling systems, and environmental conditions.

Design criteria associated with liquid effluent systems exist to promote representative sampling. The following general criteria assist in meeting that objective:

- Location for sampling and monitoring
- Use of a highly reliable sampling pump where needed to provide uniform continuous flows
- Redundant sampling collection systems or an appropriate alternative
- Sampling ports located sufficiently downstream of the final feeder line to promote complete mixing
- Samples of a proportional amount of the full effluent flow
- Accuracies within ±10 percent regarding effluent streams and sample-line flows
- Emphasis on maintaining structural integrity of the effluent sampling lines

Design considerations for the liquid effluent monitoring systems include the following:

- Purpose—Monitoring provides a prompt signal if a significant release occurs. Written procedures are advocated to document the actions that should be taken if an abnormal signal is detected. In-line and off-line monitoring may be required to accommodate routine and emergency monitoring.

- General Design Criteria—The type of radiation influences whether actual direct measurements or sampling and analysis are required (or a combination thereof). Alpha emitters and some beta emitters pose concerns from a measurement perspective; therefore, sampling and analysis should be performed to quantify releases associated with these radiations. Gamma radiation can usually be detected by direct measurement. Shielding may be required for high background areas. In these cases, off-line monitoring is encouraged. Grab samples can be used for batch releases where the concentration of radioactivity is constant, but the release is of short duration. When continuous effluent streams are present, continuous monitoring and/or sampling should be performed. Environmental conditions influence the design of the monitoring/sampling system. Air conditioning and heating provide reliable system operation to minimize worker exposures; background dose rates are considerations in accessing the system for calibration and servicing. Shielding should be considered when warranted.

Alarms are recommended to provide timely warnings and signal the need for corrective actions prior to a release exceeding the limits or recommendations in DOE Order 5400.5. The collection of a variety of samples (grab, continuous, or proportional) is encouraged to detect the levels of radioactivity before significant impacts on the public or the environment occur.

REGULATORY

15. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.204, Documented Safety Analysis, and DOE Guide (G) 421.1-2, Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830, with respect to their impact on the Department's nuclear safety.

a. Discuss the basic purposes and objectives of a DSA.

Title 10 CFR 830 defines documented safety analysis as a documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety.

The following is taken from DOE G 421.1-2.

The DSA for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility,

- describe the facility (including the design of safety SSCs) and the work to be performed;
- provide a systematic identification of both natural and man-made hazards associated with the facility;
- evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility;
- derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use;
- define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) QA, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection; and
- with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a CSP that
  - ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions,
  - identifies applicable nuclear criticality safety standards, and
  - describes how the program meets applicable nuclear criticality safety standards.

b. Describe the responsibilities of contractors for the development and maintenance of a DSA.

The following is taken from DOE G 421.1-2.

In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must

- define the scope of the work to be performed;
- identify and analyze the hazards associated with the work;
- categorize the facility consistent with DOE-STD-1027-92;
- prepare a DSA for the facility;
- establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment.

In maintaining the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must

- update the safety basis to keep it current and to reflect changes in the facility, the work, and the hazards as they are analyzed in the DSA;

- annually submit to DOE either the updated DSA for approval or a letter stating that there have been no changes in the DSA since the prior submission;
- incorporate in the safety basis any changes, conditions, or hazard controls directed by DOE.

c. Define the following terms and discuss the purpose of each:

- **Design basis**
- **Safety analysis**
- **Safety basis**
- **BIO**
- **Transportation safety document**
- **SAR for packaging**
- **Health and safety plan**
- **Hazards analysis report**

The following definitions are taken from DOE-STD-3009-94.

Design Basis

The design basis is the set of requirements that bound the design of SSCs within the facility. These design requirements include consideration of safety, plant availability, efficiency, reliability, and maintainability. Some aspects of the design basis are important to safety, although others are not.

Safety Analysis

A safety analysis is a documented process to provide systematic identification of hazards within a given DOE operation; to describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and to analyze and evaluate potential accidents and their associated risks.

Safety Basis

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

BIO

The basis for interim operations is the documented establishment of allowable operations for a current facility and its operational controls until a fully compliant document is developed and approved by DOE.

Transportation Safety Document

The transportation safety document describes the methodology and the compliance process to meet equivalent safety for any deviation from the hazardous materials regulations.

SAR for Packaging

The following is taken from DOE O 461.1A.

A safety analysis report for packaging (SARP) is a document that provides a comprehensive technical evaluation of a package. The SARP consists of sections on general information; structural, thermal, containment, shielding and criticality evaluations; operating procedures; acceptance tests, and maintenance and quality assurance programs. The purpose of the SARP is to demonstrate compliance with the applicable sections of 10 CFR 71 and 49 CFR 100–185.

Health and Safety Plan (HASP)

For all facilities having or dealing with hazardous waste, a HASP shall be developed. It shall, at a minimum, cover each site, task, operation, activity, or project, and address the following elements:

- Health and safety risk or hazard identification for each site task, operation, activity, or project defined in the work plan. (All chemical, radiological, and physical hazards, e.g., noise and heat, must be identified in the HASP. Actions taken to mitigate risks or hazards shall be identified. This risk or hazard identification should have a common basis with, or integrate the results of, other documents such as a SAR.)
- Required training for employees for each site task, operation, activity, or project and hazard.
- Personnel protective equipment to be used by workers for each site task and operation.
- Employee medical surveillance requirements.
- Frequency and types of required personnel monitoring (including air, noise, radiation, heat, stress, etc.), including the methods of maintenance and calibration of monitoring and sampling equipment to be used.
- Site control measures, including work zones, buddy systems, security, communications, and safety work practices.
- Decontamination procedures.
- Emergency response plans for safe and effective responses to emergencies.
- Confined space entry procedures.
- Programs to protect against and mitigate spills.

Hazard Analysis Report (HAR)

A HAR documents the hazard analysis of an operation and associated activities. At a minimum, the HAR shall include the following:

- An executive summary that provides an overview of the HAR and its main conclusions.
- An introduction that provides a discussion of the objectives, the scope of the analysis, the operations conducted, and the limitations and assumptions employed in the hazard analysis.
- A description of the nuclear explosive and its intrinsic hazards.
- A description of the nuclear explosives operations and the facility(ies) where the operation is to be conducted. (The discussion should focus on the facility and nuclear explosive configurations and processes, including equipment and tooling. The discussion should also address whether interfaces between the operation and facility

have safety implications. Generic safety controls utilized during the operation should be discussed.)

- A discussion of the methodology used to conduct the hazard analysis and derive safety controls and safety requirements.
- A summary of the identification of hazards and potential hazard scenarios under normal and abnormal conditions considering both internal and external environments for each step in the operations.

d. Discuss the six items a DSA for a hazard category 1, 2, or 3 DOE nuclear facility must address:

- **Description of facility and work to be performed**
- **Systematic identification of natural and man-made hazards**
- **Evaluation of normal, abnormal, and accident conditions**
- **Derivation of hazard controls, demonstration of the adequacy of the controls, and description of how the controls are maintained**
- **Definition of the characteristics of safety management programs**
- **Definition of criticality safety program, when required**

The following information is taken from DOE-STD-3009-94.

Description of Facility and Work to Be Performed

Chapter 2 of a DSA provides descriptions of the facility and processes to support assumptions used in the hazard and accident analyses. These descriptions focus on all major facility features necessary to understand the hazard analysis and accident analysis, not just safety SSCs. Expected products of this chapter, as applicable based on the graded approach, include

- overview of the facility, its inputs, and its outputs, including mission and history;
- description of the facility structure and design basis;
- description of the facility process systems and constituent components, instrumentation, controls, operating parameters, and relationships of SSCs;
- description of confinement systems;
- description of the facility safety support systems;
- description of the facility utilities;
- description of facility auxiliary systems and support systems.

The development of this chapter for hazard category 2 and 3 facilities is an iterative process dependent on the development of the hazard and accident analyses. The facility description should provide a model of the facility that would allow an independent reader to develop an understanding of facility operations and an appreciation of facility structure and operations without extensive consultation of controlled references. The level of detail required in the facility description is based on the significance of preventive and mitigative features identified and the degree of facility context necessary to understand the analyses. For a hazard category 3 facility, a brief description of the facility, processes, and major SSCs is to be provided. Grading will be based predominantly on complexity.

Systematic Identification of Natural and Man-Made Hazards

The purpose of chapter 3 of the DSA is to provide information that will satisfy the requirements of 10 CFR 830 to evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or process that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents that may be beyond the design basis of the facility.

This chapter describes the process used to systematically identify and assess hazards to evaluate the potential internal, man-made external, and natural events that can cause the identified hazards to develop into accidents. This chapter also presents the results of this hazard identification and assessment process. Hazard analysis considers the complete spectrum of accidents that may occur due to facility operations; analyzes potential accident consequences to the public and workers; estimates likelihood of occurrence; identifies and assesses associated preventive and mitigative features; identifies safety-significant SSCs; and identifies a selected subset of accidents, designated DBAs, to be formally defined in accident analysis. Subsequent accident analysis evaluates these DBAs for comparison with the evaluation guideline. This chapter covers the topics of hazard identification, facility hazard categorization, hazard evaluation, and accident analysis.

Expected products of this chapter, as applicable based on the graded approach, include

- Description of the methodology for and approach to hazard and accident analyses.
- Identification of hazardous materials and energy sources present by type, quantity, form, and location.
- Facility hazard categorization, including segmentation in accordance with DOE-STD-1027-92.
- Identification in the hazard analysis of the spectrum of potential accidents at the facility in terms of largely qualitative consequence and frequency estimates. The summary of this activity will also include
    - identification of planned design and operational safety improvements;
    - summary of defense in depth, including identification of safety-significant SSCs, SACs and other items needing TSR coverage in accordance with 10 CFR 830;
    - summary of the significant worker safety features, including identification of safety-significant SSCs and any relevant programs to be covered under TSR and administrative controls, including those controls designated as SACs;
    - summary of design and operational features that reduce the potential for large material releases to the environment;
    - identification of the limited set of unique and representative accidents (i.e., DBAs) to be assessed further in accident analysis.

- Accident analysis of DBAs identified in the hazard analysis. The summary of this activity will include for each accident analyzed
    - estimation of source term and consequence;
    - documentation of the rationale for binning frequency of occurrence in a broad range in hazard analysis (detailed probability calculations not required);

- documentation of accident assumptions and identification of safety-class SSCs based on the EG.

Evaluation of Normal, Abnormal, and Accident Conditions

The principal purpose of the accident analysis is to identify any safety-class SSCs, SACs, and TSRs needed for protection of the public. Each accident sequence needs to be analyzed through the use of a documented, deterministic DBA. Whenever possible, DBAs are analyzed using the simplest applicable deterministic, phenomenological calculations (e.g., pressure estimates from a simple ideal gas law calculation, hand calculated Gaussian plume dispersions). The nondeterministic aspects of DBA analysis are simplified by estimating overall sequence frequencies in broad frequency ranges in hazard analysis. This process is considered sufficient for DSA purposes, and accident analysis need only document the basis for the binning performed in hazard analysis. Detailed probabilistic calculations are neither expected nor required.

Natural events and man-made external events are special cases. Natural event DBAs are those events with a phenomenon initiating frequency. External events are not typically design bases for facilities. However, they will be referred to as DBAs and analyzed as such if frequency of occurrence is estimated to exceed 10^{-6}/year (yr) conservatively calculated, or 10^{-7}/yr realistically calculated.

Accident analysis typically starts with formal descriptions of accident scenarios. Basic event trees may support such descriptions. All major assumptions in scenarios must be identified. The next step is determination of accident source terms. Source terms for accidents are obtained through phenomenological and system response calculations. Once a source term has been determined, consequences due to atmospheric dispersion or other relevant pathways of concern are determined. As with every phase of the analysis, the effort expended is a function of the estimated consequence. If the source term is small, a simple, dispersion hand calculation for consequences would be sufficient. If source terms are large, computer modeling to determine consequences may be required. The consequences finally determined are compared to the EG. From this activity, it is determined if safety-class SSC designation is needed. The need for accident specific TSRs to meet the EG will also be determined.

Derivation of Hazard Controls, Demonstration of the Adequacy of the Controls, and Description of How the Controls Are Maintained

The purpose of chapter 4 of the DSA is to provide information necessary to support the safety basis requirements of 10 CFR 830 for derivation of hazard controls.

This chapter provides details on those facility SSCs that are necessary for the facility to protect the public, provide defense in depth, or contribute to worker safety. Similarly, this chapter provides details on specific administrative controls that are significant to specific accident risk reduction. Descriptions are provided of the attributes (i.e., functional requirements and performance criteria) required to support the safety functions identified in the hazard and accident analyses and to support subsequent derivation of TSRs. Expected products of this chapter, as applicable based on the graded approach, include

- descriptions of safety SSCs and SACs including safety functions;
- identification of support systems safety SSCs depend upon to carry out safety functions;
- identification of the functional requirements necessary for the safety SSCs and SACs to perform their safety functions, and the general conditions caused by postulated accidents under which the safety SSCs or SACs must operate;
- identification of the performance criteria necessary to provide reasonable assurance that the functional requirements will be met;
- identification of assumptions needing TSR coverage.

Existing supporting documentation is to be referenced. Maximum advantage should be taken of pertinent existing safety analyses and design information (i.e., requirements and their bases) that are immediately available or can be retrieved through reasonable efforts. Include a brief summary for each such reference that explains its relevance to this chapter and provides an introductory understanding of the reference.

Definition of the Characteristics of Safety Management Programs

Typical safety-management programs include criticality protection, radiation protection, hazardous material protection, institutional safety provisions, procedures and training, operational safety, and emergency preparedness.

Definition of Criticality Safety Program, When Required

The purpose of chapter 6 of a DSA is to provide information that will support the development of a safety basis in compliance with the provisions of 10 CFR 830.204(b)(6) regarding the definition of a criticality safety program. If this information is available in a site-wide criticality safety program description, and it complies with the Rule requirements, then it can be included by reference and summarized in this chapter.

Expected products of this chapter include

- definition of a CSP that (1) ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions, (2) identifies applicable nuclear criticality safety standards, and (3) describes how the program meets applicable nuclear criticality standards;
- description of the basis and analytical approach the facility uses for deriving operational criticality limits;
- summary of design and administrative controls used by the CSP.

Existing supporting documentation is to be referenced. Include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to this chapter.

e. Discuss the approval requirements for the DSA for new facilities and subsequent changes to the DSA.

DOE-STD-1104-96, *Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements)* or successor document,

provides guidance on the preparation of safety evaluation reports (SERs). One of the guiding principles is, "The Safety Evaluation Report (SER) is primarily a management document that provides the approval authority, the basis for the extent and detail of the DSA review, and the basis for any conditions of DSA approval."

DOE line managers, including NNSA line managers supported by safety professionals, must satisfy themselves that all the hazards associated with a nuclear facility have been identified and appropriate controls have been put in place to prevent accidents and mitigate consequences of accidents associated with those hazards. Generally, it is most effective for DOE reviewers to be engaged and interact with the contractor during the DSA development process so that the reviewers know the safety issues and how they were resolved. Judgments must be made regarding what constitutes appropriate controls. These judgments should consider the level of the hazard and potential consequences, the practicality and effectiveness of possible control options, the importance of the mission of the facility, and other relevant factors, if any. These are all elements of the graded approach.

DOE-STD-1189-2008, *Integration of Safety into the Design Process*, applies to the design and construction of the following:

- New DOE hazard category 1, 2, and 3 nuclear facilities;
- Major modification to DOE hazard category 1, 2, and 3 nuclear facilities (as defined by 10 CFR 830); and
- Other modification to DOE hazard category 1, 2, and 3 nuclear facilities managed under the requirements of DOE O 413.3A.

DOE-STD-1189-2008 discusses the approval requirements for safety basis documents for new DOE nuclear facilities.

f. Define who approves facility operations prior to achieving DSA upgrade approval.

The following is taken from DOE-STD-1104-96.

By 10 CFR 830.207 (b), the DOE approves facility operations prior to upgrade of the DSA to full 10 CFR 830 requirements. The CFR states:

> Pending issuance of a safety evaluation report in which DOE approves a safety basis for a hazard category 1, 2, or 3 existing DOE nuclear facility, the contractor responsible for the facility must continue to perform work in accordance with the safety basis for the facility in effect on October 10, 2000, or as approved by DOE at a later date, and maintain the existing safety basis consistent with the requirements of this Subpart.

General information about the DOE approval process follows.

Appendix A of 10 CFR 830 states "The DOE Management Official for a DOE nuclear facility (that is, the Assistant Secretary, the Assistant Administrator, or the Office Director who is primarily responsible for the management of the facility) has primary responsibility

within DOE for ensuring that the safety basis for the facility is adequate and complies with the safety basis requirements of Part 830." It further states "The DOE Management Official is responsible for ensuring the timely and proper (1) review of all safety basis documents submitted to DOE and (2) preparation of a safety evaluation report concerning the safety basis for a facility." Paragraph 9.4.1.6 of the DOE M 411.1-1C, *Safety Management Functions, Responsibilities, and Authorities Manual* (FRAM), states that a Cognizant Secretarial Officer (CSO) can delegate this authority to the field element manager (FEM) for the facility. By assigning responsibilities for the review and approval of the DSA to another individual, the DOE Management Official for the facility establishes that individual as the new approval authority. Assigning responsibilities carries concurrent delegation of authority recognized by the line management and those responsible for monitoring and auditing implementation of 10 CFR 830.

The approval authority is responsible for providing a defensible review and approval of the DSA. Achieving defensible review and approval is facilitated by an independent review process. Since both the preparation of the DSA and its review and approval typically fall within the purview of the approval authority, the approval authority assigns a review team leader the responsibility of performing the independent review. In making this assignment, the approval authority ensures that the review team leader maintains sufficient independence of the line organization responsible for the DSA preparation (i.e., no responsibility for preparation of the DSA under review) and possesses the technical competence relevant to the DSA of concern. The details of independently reviewing the DSA, up to and including recommending approval to the approval authority, are managed by the review team leader.

The approval authority has responsibility as the single point of contact between DOE and the facility contractor for all matters regarding review of the DSA. This responsibility is typically assigned to the review team leader, but the approval authority remains the final authority on any points requiring arbitration. The single point of contact is the focal point through which DOE and the facility contractor interface and from which directions to the facility contractor originate. Requests for any material on the DSA, determination of the significance of identified issues on such material, and direction to the facility contractor for resolution of issues are approved by the single point of contact. As appropriate, transmittal of official communications and directions involving significant work effort by the facility contractor are coordinated with the facility contracting officer. Line management personnel and representatives of organizations responsible for monitoring and auditing 10 CFR 830 implementation coordinate their activities through the single point of contact as well.

The approval authority has the specific responsibility of ensuring the review and approval process represents all DOE entities with vested interest in the facility under review and considers commitments made to agencies outside DOE. Agencies external to DOE, however, have no standing under the Orders/Rules structure for approval. Identifying safety issues and their resolution may involve negotiations between concerned organizations. Discounting a safety issue raised by any vested interest without giving the issue proper consideration could reduce safety assurance.

g. Discuss the provisions for deviations and temporary and permanent exemptions from the 10 CFR 830.204 and safe harbor methodologies.

The following is taken from DOE-STD-1104-96.

If a contractor uses a method other than a safe harbor method, the contractor must obtain DOE approval of the method before developing the DSA. Likewise, if a contractor uses a safe harbor method to develop the DSA, but does not follow the method completely, the contractor should request DOE approval of the method with the specific deviations noted.

The use of alternative methods or specific deviations from the safe harbor methods must have (1) for NNSA facilities, the approval of the Deputy Administrator or for non-NNSA facilities, the approval or concurrence (if the responsibility is delegated to the FEM) of the CSO as specified in paragraph 9.3.1 of DOE M 411.1-1C and (2) the approval of the FEM and the review and concurrence (or comment if an NNSA facility is involved) of the DOE Headquarters Office of Environment, Safety, and Health as specified in paragraph 9.4.1.6 of the FRAM.

h. Discuss the application of the graded approach relative to the DSA development.

Title 10 CFR 830 prescribes the use of a graded approach for the effort expended in safety analysis and the level of detail presented in associated documentation. The graded approach applied to DSA preparation and updates is intended to produce cost-efficient safety analysis and DSA content that provide adequate assurance to the DOE that a facility has acceptable safety provisions without providing unnecessary information. As described in 10 CFR 830, the graded approach adjusts the magnitude of the preparation effort to the characteristics of the subject facility based on seven factors:

1. The relative importance to safety, safeguards, and security
2. The magnitude of any hazard involved
3. The life cycle stage of a facility
4. The programmatic mission of a facility
5. The particular characteristics of a facility
6. The relative importance of radiological and nonradiological hazards
7. Any other relevant factor

Title 10 CFR 830 provides for developing the DSA based on judgment of the facility in relation to these seven factors. For example, simple hazard category 3 facilities or facilities that have a short operational life may only require a limited but adequate analysis documented to a level less than that required for a hazard category 2 facility. In addition, facilities with short operational lives (or other compelling circumstances) should consider the appropriateness of using DOE-STD-3011-2002 to meet the requirements of 10 CFR 830. On the opposite end of the spectrum, a complex hazard category 1 facility that is just going into operation requires extensive analysis and highly detailed documentation.

The application of the graded approach may allow for much simpler analysis and documentation for some of these facilities. For facilities of little hazard, or hazards at the

hazard category 3 level, for which only a modest reduction of risk is required, the DSA may be simple and short. In such cases all of the topics for the DSA may not be necessary, and with proper technical bases some topics may be omitted or reduced in the detail that would otherwise be required of hazard category 1 or 2 facilities. Thus, with application of the graded approach, DSAs for hazard category 3 facilities or facilities with short operational lives will normally require more simplified DSA analysis and documentation. Specific minimum levels of detail for these facilities are given in options 3 and 8 in table 2 of appendix A to 10 CFR 830 subpart B and the graded approach section of each chapter in DOE-STD-3009-94.

16. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.207, DOE Approval of Safety Basis, and DOE-STD-1104-96, Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements), with respect to their impact on the Department's nuclear safety.

a. Describe the basic purpose and contents of a SER.

The following is taken from DOE-STD-1104-96.

The SER is primarily a management document that provides the approval authority the basis for the extent and detail of the review of the DSA and TSRs and the basis for and any conditions of approval. DOE-STD-1104-96endorses the concept that the contents of a SER are concise summary statements and that little benefit is gained from the wholesale recapturing of elements already contained in a DOE-owned DSA or TSRs or from reproducing original analysis that, if deemed critical, is performed as part of the review process.

SERs document the bases for approving revisions of DSAs/TSRs, including annual updates. Those revisions determined to not involve an unreviewed safety question in accordance with 10 CFR 830.203, "Unreviewed Safety Question Process," are considered administrative and/or editorial in nature and may be reviewed and approved by DOE subsequent to implementation of the changes by the facility contractor.

b. Describe the bases for approval contained in a SER.

The following is taken from DOE-STD-1104-96.

Base Information

Base information is the first of the approval bases that should be reviewed and encompasses elements of DSA preparation, completeness, and general content. Base information is not reviewed for accuracy in and of itself but for sufficiency to allow assessment of the other approval bases that rely on this information. The review for sufficiency can range from a simple screening effort to more detailed discussions, depending on the complexity of the DSA. Insufficient or incomplete base information in a DSA may prevent further review of the DSA. Reviewers should require resolution of major discrepancies in base information

(e.g., incomplete site characteristics) before evaluation of the more specific aspects (e.g., hazard and accident analyses) of the safety basis proceeds. It is for this reason that the SER need only provide a brief statement as to the adequacy of base information. For example, for DSAs adhering to DOE-STD-3009-94 change notice 2 format, the review of base information primarily determines the sufficiency of the information provided in the executive summary, site characteristics (chapter 1), facility description (chapter 2), and to some extent material generic to all DSA chapters (e.g., statutes, rules, Orders, and principal health and safety criteria). Determining the adequacy of base information generally entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The facility contractor's development and approval processes (e.g., personnel involvement in developing the DSA, management cognizance and acceptance, internal reviews, etc.) demonstrate sufficient commitment to establish the facility safety basis.

- The facility mission(s) and scope of operations (i.e., the scope of work to be performed) for which safety basis approval is being sought are clearly stated and reflected in the type and scope of operations analyzed in the DSA. For example, a DSA documenting the safety basis of a spent fuel storage facility whose mission includes size reduction of spent fuel elements would be unacceptable if the DSA omitted safety analysis of size reduction operations.

- A description of the facility's life-cycle stage, mission(s), scope of operations, and the design of safety SSCs is presented, including explanation of the impact on the facility safety basis.

- Clear basis for and provisions of exemptions, consent agreements, and open issues are presented.

- Descriptions of the site, the facility, and operational processes provide a knowledgeable reviewer sufficient background material to understand the major elements of the safety analysis.

- Correlation is established between actual facility arrangements and operations with those stated in the DSA. This may be accomplished successfully through reference to facility walkthroughs during DSA preparation. Walkthroughs may also be warranted during DSA review to provide some level of assurance that the actual physical arrangement of a facility corresponds to that documented in the DSA. For example, a walkthrough may be considered for a facility or operation that was modified between the time the DSA development began and when it was completed. This is not intended to imply the review team must perform detailed verifications of facility configuration. The objective is to allow the review team to conclude that the basic descriptions provided are fundamentally up-to-date and correct.

Hazard and Accident Analyses

Another of the DSA approval bases is hazard and accident analyses and forms the foundation upon which the remaining approval bases (i.e., safety SSCs, derivation of TSRs, and safety management program characteristics) rely. Determining the adequacy of hazard and accident analyses generally entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The hazard analysis includes hazard identification that specifies or estimates the hazards relevant for DSA consideration (i.e., both natural and man-made hazards associated with the work and the facility) in terms of type, quantity, and form, and also includes properly performed facility hazard categorization.

- The final hazard category for the facility is determined consistent with DOE-STD-1027-92, change notice 1 or successor document. Any differences between the final hazard category and the initial hazard category are explained.

- The hazard analysis includes hazard evaluation that covers the activities for which approval is sought, is consistent in approach with safe harbor methodologies, identifies preventive and mitigative features for the spectrum of events examined, and identifies dominant accident scenarios through ranking.

- The hazard analysis evaluates normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility.

- The hazard analysis results are clearly characterized in terms of public safety, defense in depth, worker safety, and environmental protection. The logic behind assessing the results in terms of safety-significant SSCs and designation of TSRs is understandable and internally consistent.

- Subsequent accident analysis clearly substantiates the findings and delineations of hazard analysis for the subset of events examined and confirms their potential consequences. Events potentially exceeding evaluation guidelines need to clearly identify associated safety-class SSCs and basis of TSR deviations. The goal of the review is to ensure that the safety basis is comprehensive relative to hazards presented and is based on a consistent, substantiated logic.

Safety Structures, Systems, and Components

The next DSA approval basis is safety SSCs. Identification of safety SSCs (i.e., safety-class SSCs and safety-significant SSCs) is a product of the hazard and accident analyses. Determining the adequacy of safety SSCs generally entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The safety SSCs identified and described are consistent with the logic presented in the hazard and accident analyses.

- Safety functions for safety SSCs are defined with clarity and are consistent with the bases derived in the hazard and accident analyses.
- Functional requirements and system evaluations are derived from the safety functions and provide evidence that the safety functions can be performed.
- Control of safety SSCs relevant to TSR development is clearly defined.

Derivation of Technical Safety Requirements

Derivation of TSRs is the next of the DSA approval bases. Hazard controls are derived to eliminate, limit, or mitigate hazards and are generally safety SSCs or commitments to safety management programs, which are ultimately included in TSRs. Identification of TSRs results from the most significant preventive and mitigative features identified in the hazard and accident analyses and from the designation of safety SSCs. Determining the adequacy of the derivation of TSRs generally entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- TSRs are identified to ensure adequate protection of workers, the public, and the environment.
- The bases for deriving TSRs, which are identified and described in the hazard and accident analyses and safety SSC chapters, are consistent with the logic and assumptions presented in the analyses.
- The bases for deriving SLs, limiting control settings, LCOs, surveillance requirements, and administrative controls are provided as appropriate.
- The process for maintaining the TSRs current at all times and for controlling their use is defined.

Safety Management Program Characteristics

The following is taken from DOE-STD-1104-96.

Safety management program characteristics is the last of the DSA approval bases and encompasses the elements of institutional programs and facility management that are necessary to ensure safe operations based on assumptions made in the hazard and accident analyses. While these elements must be addressed in the DSA, generic descriptions of these institutional programs should not be duplicated in the DSA if they can be referenced in Integrated Safety Management System (ISMS) documents or site-wide manuals. These institutional programs include (where applicable) QA, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, radiation protection, and criticality safety. Identification of safety management program characteristics is a product of hazard and accident analyses, designation of safety SSCs, and derivation of TSRs.

Determining the adequacy of safety management program characteristics generally entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The major programs needed to provide programmatic safety management are identified.

- Basic provisions of identified programs are noted, and references to facility or site program documentation are provided. The acceptance of safety management program characteristics does not constitute acceptance of the adequacy of program compliance with DOE directives. That can only be accomplished by detailed compliance review of each of the programs, which is beyond the scope of a DSA.
- Hazard controls that are discussed in the DSA are faithfully translated into TSR provisions.
- The TSR provisions are appropriate and consistent with the DSA.

The approval bases for the TSR document are the TSR provisions. These TSR provisions may be design features, SLs, operating limits (OLs), limiting control settings, and LCOs, surveillance requirements, or administrative controls (primarily commitments to implement safety management programs according to the facility-specific characteristics described in the DSA). The approval bases for a TSR document include a disciplined analysis and tracing of commitments to hazard controls through appropriate provisions that implement these controls in a TSR document. In some cases the specific treatment of safety controls in the TSR is committed to in the DSA; in other cases, it is a judgment call as to the appropriate TSR treatment. Determining the adequacy of the TSR provisions generally entails being able to conclude that

- hazard controls that are discussed in the DSA are faithfully translated into TSR provisions;
- the TSR provisions are appropriate and consistent with the DSA.

The sources of information in a DSA regarding these provisions are the hazard analysis, including description of hazard controls; the description of SSCs, the classification of these SSCs as , SS, or other important defense-in-depth SSCS, the description of the functional requirements for the safety SSCs, and the derivation of TSRs section; and the descriptions of the safety management programs.

A hazard analysis will include a disciplined analysis of all hazards within the scope of the DSA, including a listing of applicable preventive and mitigative hazard controls. These controls may include safety SSCs, design features, and provisions of various safety management programs. These controls should be regarded as DSA commitments. They should be traced through DSA documentation to specific TSR provisions.

Safety SSCs must be described in sufficient detail in a DSA so that their functional requirements are defined and the bases for TSR requirements are derived. These safety SSCs will be either active or passive. If passive, they should also be considered for designation as design features in the TSR. These are features of facility design that may not be changed without DOE review and approval. A crosscheck between DSA-identified important design features and the “Design Features” section of the TSR should be conducted to assure consistency. If active, safety-class SSCs will usually have safety limits and limiting control settings associated with them, as well as surveillance requirements. An active SS SSC may have a limiting condition of operation and surveillance requirement and/or specific provisions of a maintenance management program associated with it. In any case, safety SSCs must be addressed specifically in TSR provisions. Technical bases for limiting control

settings and SRs in the "Bases" appendix of the TSR should be reviewed for adequacy. All these provisions are directed at assurance that the safety function of the SSC will be protected.

DOE standards define only SC and SS SSCs, criteria for their designation, and design requirements (in the case of new design). Provisions exist for line management to designate additional important defense-in-depth items, independent of safety analysis. If such items are designated, it should be confirmed that any management direction relative to assurance of safety function is implemented through the TSR.

Hazards analyses may invoke particular aspects of safety management programs, such as emergency preparedness, criticality safety, procedures and training, etc. Any particular provisions of these programs unique to the facility should have been described in the DSA. The administrative controls section of the TSR should include commitments to implement those programs identified in the DSA as important to the facility's safety basis.

Mandatory Performance Activities:

a. Demonstrate by direct preparation or assistance in the development of at least two (2) SERs consistent with DOE-STD-1104-96 for a new safety basis, significant update, or safety basis amendment.

Mandatory performance activities are performance based. The Qualifying Official will evaluate the completion of this competency.

17. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.206, Preliminary Documented Safety Analysis, with respect to its impact on the Department's nuclear safety.

a. Describe the application of the requirements of DOE Order (O) 420.1B, Facility Safety, and its guidance to the development process for the PDSA.

Per DOE O 420.1B, safety analyses must be performed as early as practical in conceptual or preliminary design processes to ensure that required safety SSCs are specified in the final design. Safety analyses must be used to establish the identity and functions of safety SSCs and the significance to safety of functions performed by these SSCs. In that light, the safety analyses must address hazards inherent to the facility and its activities, NPH, and external man-made hazards. Safety analyses must be performed in accordance with the requirements for safety analysis defined in DOE directives and technical standards for a DSA. In addition, hazard category 1, 2, and 3 nuclear facilities with uncontained radioactive material must have the means to confine the materials to minimize their potential release in facility effluents during normal operations and during and following accidents. Confinement design considerations must include the adequacy of confinement systems to perform required functions as documented and accepted through the PDSA. Hazard category 1, 2, or 3 nuclear facilities must also be designed to facilitate safe deactivation, decommissioning, and decontamination, including incorporation of design considerations during the operational

period that facilitate future deactivation and decommissioning; facilitate inspections, testing, maintenance, repair, and replacement of safety SSCs as part of a reliability, availability, and maintainability program; and keep occupational radiation exposures within statutory limits and ALARA. These are all design considerations that must be evaluated as early as possible and documented in the PDSA.

Application of the requirements of DOE O 420.1B and its guidance to the development process for PDSAs is discussed in detail in DOE-STD-1189-2008.

DOE-STD-1189-2008, *Integration of Safety into the Design Process,* provides the Department's expectations for incorporating safety into the design process for new or major modifications to DOE hazard category 1, 2, and 3 nuclear facilities.

The standard describes the safety-in-design philosophies to be used with the project management requirements of DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, and incorporates the facility safety criteria in DOE O 420.1B, *Facility Safety*, as a key foundation for safety-in-design determinations.

b. Describe the sequencing of the PDSA relative to design, procurement, construction, and operation of new facilities.

Per DOE G 421.1-2, to obtain early agreement between DOE and its contractors regarding what safety systems and design features are needed in new nuclear facilities, a contractor responsible for a new DOE nuclear facility or a major modification to an existing DOE nuclear facility that is hazard category 1, 2, or 3 must submit a PDSA to DOE for approval. DOE approves the PDSA prior to procuring materials or components, or beginning construction.

PDSAs for new facilities serve as the principal safety basis for the DOE decision to authorize design, procurement, construction, and pre-operational testing. The safety analysis should be initiated and technical interchanges conducted with DOE at the earliest practical point in conceptual or preliminary design, so that required functional attributes of safety SSCs can be specified in the detailed design. These early interchanges are intended to support development of a consensus on the safety issues between the various design and safety organizations involved in the project. The PDSA will identify preliminary commitments to the facility's ultimate design and operation. During design and construction, the governing safety basis document is the PDSA. It is updated as the design matures and is approved prior to procurement and construction activities. Until approval, the PDSA and its updates serve to keep DOE informed as to how DOE nuclear safety design criteria are being addressed in the design. Project design reviews provide the vehicle by which safety related changes are reviewed and DOE can provide guidance to the contractor. Prior to operations, the PDSA evolves to a final DSA that reflects the facility as actually constructed.

DOE-STD-1189-2008 provides several tables illustrating the sequencing of the design process to the development of safety basis documents.

c. Describe the circumstances when a PDSA must be prepared.

The following is taken from DOE G 421.1-2 and DOE-STD-1189-2008.

In accordance with DOE O 413.3A, contractors responsible for the design of DOE hazard category 1, 2, and 3 nuclear facilities must implement DOE-STD-1189-2008, including the safety criteria of appendix A, and submit the following safety basis documents for DOE approval (unless otherwise agreed to):

- Conceptual design stage: safety design strategy
- Conceptual design stage: conceptual safety design report (CSDR)
- Preliminary design stage: preliminary safety design report (PSDR)
- Final design stage: preliminary documented safety analysis
- Prior to operations: documented safety analysis and technical safety requirements

The Federal Project Director is responsible for ensuring the implementation of the requirements of DOE O 413.3A and does this through contract requirements and through support of DOE entities. The Federal Project Director approves or concurs on the approval of all safety submittals of the project. The DOE Safety Basis Approval Authority approves the CSDR, PSDR, and PDSA based on a review by a safety basis review team.

Table 2-1 of DOE-STD-1189-2008 shows the entities responsible for preparation, review, and approval of these safety documents.

Specifically, a PDSA is required for new construction or a major modification (i.e., substantial changes to the safety basis of a facility) of an existing facility or activity. DOE does not expect a PDSA to be needed for activities that do not involve significant construction—such as environmental restoration activities, decontamination and decommissioning activities, specific nuclear explosive operations, transition surveillance and maintenance activities—or for activities that are not major modifications. For activities that are not major modifications, the USQ process should be used to determine if DOE approval is needed. If so, a safety analysis that supports the request for approval should be developed.

d. Describe the relationship between the PDSA and the design process.

Per DOE G 421.1-2, for the design and construction of a new facility or activity, it is imperative that safety be addressed early so that it can be "designed-in" instead of "added-on." To achieve this integration of safety into design, there needs to be continuous interaction between safety analysts and the designers throughout the design process, as described in DOE O 420.1B and DOE G 420.1-1. All the hazards identified in DOE O 420.1B (nuclear, explosive, NPH, fire, criticality, etc.) should be addressed as early as possible in the design of new nuclear facilities and major modifications so that passive and active design concepts can be economically incorporated into the design.

DOE-STD-1189-2008 provides additional information.

18. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.202, Safety Basis, and DOE-STD-1027-92, Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports, with respect to their impact on the Department's nuclear safety.

a. Describe when a contractor must establish a safety basis for a facility.

According to 10 CFR 830.202, a contractor that is responsible for a hazard category 1, 2, or 3 DOE nuclear facility must establish and maintain the safety basis for the facility.

b. Describe the requirements for the safety basis.

The following is taken from 10 CFR 830.202.

In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must

- define the scope of the work to be performed;
- identify and analyze the hazards associated with the work;
- categorize the facility consistent with DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques,* for compliance with DOE Order 5480.23, *Nuclear Safety Analysis Reports*, change notice 1, March 10, 1994;
- prepare a DSA for the facility;
- establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment.

c. Describe the requirements the contractor must perform to maintain the safety basis.

The following is taken from 10 CFR 830.202.

In maintaining the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must

- update the safety basis to keep it current and to reflect changes in the facility, the work, and the hazards as they are analyzed in the DSA;
- annually submit to DOE either the updated DSA for approval or a letter stating that there have been no changes in the DSA since the prior submission; and
- incorporate in the safety basis any changes, conditions, or hazard controls directed by DOE.

d. Discuss the purpose of hazard categorization and determine the hazard categorization of an operating nuclear facility.

The following is taken from DOE-STD-1027-92.

Title 10 CFR 830.202 (b)(3) requires the contractor to categorize the facility consistent with DOE-STD-1027-92. DOE-STD-1027-92 focuses on

- the hazard categorization methodology to be applied to all facilities and
- the accident analysis techniques appropriate for the graded approach.

Facilities that do not meet or exceed category 3 threshold criteria but still possess some amount of radioactive material may be considered radiological facilities. Radiological facilities are exempt from having to prepare nuclear facility DSAs, but not exempt from other safety requirements (they must meet 10 CFR 835 requirements). The hazard categories are

- Category 1 hazard: The hazard analysis shows the potential for significant offsite consequences.
- Category 2 hazard: The hazard analysis shows the potential for significant onsite consequences.
- Category 3 hazard: The hazard analysis shows the potential for only significant localized consequences.

The preliminary assessment of hazards at a DOE nuclear facility requires only a minimal effort to identify the inventory of hazardous material in order to perform an initial hazard categorization. This step results in the preliminary categorization of a DOE nuclear facility in a hazard category 1, 2, or 3 or below category 3 (radiological facility). Attachment 1 of DOE-STD-1027-92 classifies a facility as either hazard category 1, 2, or 3, depending only on the quantities of radioactive material in the facility, and gives the threshold quantities as well as the appropriate ground rules for evaluating the facility.

Once a hazards analysis has been performed, the hazard categorization can be finalized. The final categorization is based on an "unmitigated release" of available hazardous material. For the purposes of hazard categorization, "unmitigated" is meant to consider material quantity, form, location, dispersibility, and interaction with available energy sources, but not to consider safety features (e.g., ventilation system, fire suppression, etc.) that will prevent or mitigate a release.

e. Describe the exclusion types for radionuclides associated with hazard categorization determination.

The following is taken from DOE-STD-1027-92.

Sealed radioactive sources that are engineered to pass the special form testing specified by the Department of Transportation (DOT) in 49 CFR 173.469 or testing specified by ANSI N43.6, *Sealed Radioactive Sources*, may be excluded from summation of a facility's radioactive inventory. The facility must have documentation that the source or prototypes of the source have been tested and have passed the tests specified by DOT or ANSI. Facilities must also have in place a source control policy that complies with DOE Notice 5400.9, *Sealed Radioactive Source Accountability*, and the source control policy specified in Article 431 of the *U.S. Department of Energy Radiation Control Manual.* Should a sealed radioactive source fail, as indicated by an increase in the removable activity, the source shall be removed from service and handled in accordance with the source control policy

established for the facility. Hazardous materials used in exempted, commercially available products should not be considered part of a facility's inventory. These materials include timepieces, illumination devices, thermostats, electron tubes, microwave receiver tubes, etc. Additionally, material contained in DOT Type B shipping containers may also be excluded from summation of a facility's radioactive inventory if the certificates of compliance are kept current, and the materials stored are authorized by the certificate. However, Type B containers without overpack should have heat protection provided by the facility's fire suppression system. These exclusions do not apply to fissile material in the determination of hazard category 2 status relative to criticality.

It is important to remember that these exclusions only apply to the hazard categorization of a facility and do not carry over to the safety analysis for the consideration of facility MAR in accident scenario development.

f. Describe the differences between initial and final hazard categorizations and where these designations occur in the DSA development process.

The following is taken from DOE-STD-1027-92.

Initial Radiological Hazards Classification

The preliminary assessment of hazards at a DOE nuclear facility requires only a minimal effort to identify the inventory of hazardous material in order to perform an initial hazard categorization. Reviewing basic facility information on intended facility operations and using estimates of material quantities should lead to an acceptable assessment. Whenever questions concerning appropriate facility categorization arise, provide for a margin of error by selecting the higher hazard category. This step results in the preliminary categorization of a DOE nuclear facility in a hazard category 1, 2, or 3 or below category 3 (radiological facility).

Tables, sections, figures, and attachments mentioned in the following are from DOE-STD-1027-92.

Final Hazard Categorization

Once a hazard analysis has been performed as defined in section 4 of DOE-STD-1027-92, the hazard categorization can be finalized. The final categorization is based on an "unmitigated release" of available hazardous material. For the purposes of hazard categorization, "unmitigated" is meant to consider material quantity, form, location, dispersibility, and interaction with available energy sources, but not to consider safety features (e.g., ventilation system, fire suppression, etc.) that will prevent or mitigate a release.

The hazard analysis or other existing safety analyses) provides an understanding of the material which can physically be released from the facility. This inventory should be compared against the threshold quantities (TQs) identified in attachment 1. The airborne release fractions used in generating the TQ values for category 2 in table A.1 are provided on page A-9 of attachment 1. As discussed in the attachment, these are intended to be generally conservative for a broad range of possible situations. Therefore, the inventory values of table A.1 may be used directly for determination as to whether a facility exceeds category 2.

Alternatively, for final categorization, for facilities initially classified as hazard category 2, if the credible release fractions can be shown to be significantly different than these values based on physical and chemical form and available dispersive energy sources, the threshold inventory values for category 2 in table A.1 may be divided by the ratio of the maximum potential release fraction to that found on page A-9. All assumptions that are used to reduce the inventory at risk should be supported in the hazard analysis. This also applies to ground rules identified in attachment 1, to demonstrate that the ground rule conditions exist.

Mandatory Performance Activities:

a. Participate in at least two (2) hazard categorization designation reviews.

Mandatory performance activities are performance based. The Qualifying Official will evaluate the completion of this competency.

19. Nuclear safety specialists shall demonstrate a familiarity level knowledge of DOE O 420.1B, Facility Safety; DOE G 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE O 420.1, Facility Safety; and DOE-STD-1020-2002, Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities; with respect to their impact on the Department's nuclear safety.

a. Discuss the purpose and policy associated with DOE O 420.1B.

The purpose of this Order is to establish facility safety requirements for DOE/NNSA for

- nuclear safety design
- criticality safety
- fire protection
- natural phenomena hazards mitigation
- a system engineer program

This Order applies to all DOE/NNSA facilities with responsibility for DOE-owned or DOE-leased facilities as follows:

- All DOE nuclear and non-nuclear facilities
- All DOE nonreactor nuclear facilities that are classified as hazard category 1, 2, or 3
- All DOE explosives facilities
- All DOE hazard category 1, 2, and 3 nuclear facilities

The objectives of the nuclear safety requirements are to ensure that DOE nonreactor nuclear facilities are designed and constructed so as to assure adequate protection for the public, workers, and the environment from nuclear hazards.

The objective of the explosive safety requirements is to establish mandatory standards for explosives safety in the design and construction of DOE explosives facilities or modifications thereof.

The objectives of the fire protection requirements are to establish requirements for a comprehensive fire and related hazards protection program for facilities sufficient to minimize the potential for

1. the occurrence of a fire or related event;
2. a fire that causes an unacceptable onsite or offsite release of hazardous or radiological material that will threaten the health and safety of employees, the public, or the environment;
3. vital DOE programs suffering unacceptable interruptions as a result of fire and related hazards;
4. property losses from a fire and related events exceeding defined limits established by DOE; and
5. critical process controls and SC systems being damaged as a result of a fire and related events.

The objectives of the nuclear criticality requirements are to ensure that

1. criticality safety is comprehensively addressed and receives an objective review, with all identified risks reduced to acceptably low levels and management authorization of the operation documented; and
2. the public, workers, property, both government and private, the environment, and essential operations are protected from the effects of a criticality accident.

The objectives of the NPH requirements are to ensure that all DOE facilities are designed, constructed, and operated so that the general public, workers, and the environment are protected from the impact of NPH, including seismic, wind, flood, and lightning.

b. Discuss the role of the Department's NSSs with respect to the implementation of the requirements of DOE O 420.1B.

Nuclear safety specialists shall ensure that facilities under their purview falling within the scope of this Order are in compliance. NSSs are responsible for understanding the design requirements associated with this Order and assessing adequate compliance to these requirements for existing facilities or during the design of new facilities or major modifications.

c. Discuss the Department policy and objectives with respect to safety-class and safety-significant criteria.

The following is taken from 10 CFR 830, DOE-STD-3009-94, and DOE G 421.1-2.

Some principles that should be incorporated in a functional classification process are listed below:

- Protection of the public is contributed to by all facets of safety in design, including safety-class SSCs as well as safety-significant SSCs. The expectation is that public DBA dose consequences 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. Administrative controls such as disciplined conduct of operations, training, and safety management programs are also important in assuring worker safety.

In prioritization of items for a facility safety strategy, the following is the preferred order of priority:

- Minimization of hazardous materials (MAR) is the first priority
- Safety SSCs are preferred over ACs
- Passive SSCs are preferred over active SSCs
- Preventive 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

d. Discuss the facility and activity applicability of DOE O 420.1B, with respect to implementation associated with the design of nuclear facilities.

Section 4 Requirements

In complying with this DOE O 420.1B, DOE and contractors must ensure that any work done is consistent with any other safety, design, or other analysis or requirements applicable to the affected facility. In particular, work must be performed in accordance with the ISM requirements of 48 CFR 970.5223-1, "Integration of Environment, Safety, and Health into Work Planning and Execution," and the QA requirements of either subpart A of 10 CFR 830, "Nuclear Safety Management," or DOE O 414.1C, *Quality Assurance*, dated June 17, 2005, or successor document, as applicable. All new construction, as a minimum, must comply with national consensus industry standards and the model building codes applicable for the state or region, supplemented in a graded manner with additional safety requirements for the associated hazards in the facility that are not addressed by the codes.

DOE implementation guidance and technical standards referenced in this Order are not mandatory; however they must be considered in conjunction with the specific requirements. Such guidance, along with both DOE and industry standards referenced therein, represent acceptable methods to satisfy the provisions of this Order. Alternate methods that satisfy the requirements of this Order are also acceptable. Any implementation method selected must be justified to ensure that an adequate level of safety commensurate with the identified hazards is achieved.

The following is a summary of the five chapters of DOE O 420.1B.

<u>Chapter I ("Nuclear and Explosives Safety Design Criteria")</u>: New hazard category 1, 2, and 3 nuclear facilities as defined by 10 CFR 830, new explosive facilities, and major modifications to such facilities that could substantially change the approved facility safety analysis. (See note 1.)

Chapter II ("Fire Protection"): Fire protection programs and facility safety design for all DOE elements with the responsibility for DOE nuclear, non-nuclear, and weapons facilities. (See note 2.)

Chapter III ("Nuclear Criticality Safety"): For DOE elements with responsibility for nuclear facilities and activities involving or potentially involving nuclides in quantities that are equal to or greater than the single parameter limits for fissionable materials listed in ANSI/ANS 8.1 and 8.15. Any facility or activity involving or potentially involving amounts of fissionable material in excess of these limits has by definition a fissionable material operation.

Chapter IV ("Natural Phenomena Hazards Mitigation"): All DOE facilities and sites. To the extent that design, construction, operation, or decommissioning responsibilities for DOE facilities and sites are assigned to DOE contractors, the cognizant DOE elements must ensure that the requirements for this chapter are implemented. (See note 2.)

Chapter V ("System Engineer Program"): All hazard category 1, 2, and 3 nuclear facilities. The System Engineer Program must be applied to active SC and SS SSCs as defined in the facility's DOE-approved safety basis, and to other active systems that perform important defense-in-depth functions as designated by the facility line management.

Notes:

1. For explosives facilities that are also nuclear facilities, requirements for nuclear safety design also apply.
2. Activities within weapons facilities relating to accidental or unauthorized nuclear detonation are also subject to the requirements of the 452 series of DOE directives.

e. Identify and discuss the use of DOE standards for seismic safety.

Executive Order 12699, "Seismic Safety of Federal and Federally Assisted or Regulated New Building Construction," establishes the minimum seismic requirements for new Federal buildings. The National Earthquake Hazards Reduction Program (NEHRP) updates the provisions required to meet these requirements every 3 years. The Interagency Committee on Seismic Safety in Construction (ICSSC) compares model building codes with the NEHRP provisions. Designers must consider the NEHRP provisions and ICSSC comparisons to ensure the use of the proper model building code in their design and evaluation. Currently the International Building Code (IBC) 2000 and the American Society of Civil Engineers (ASCE) 7-05, *Minimum Design Loads for Buildings and Other Structures*, meet the requirements of the NEHRP provisions. While using the IBC 2000 or successor documents, designers must consider the seismic use group and seismic design category.

Evaluations of existing SSCs must follow, or at least be measured against, the NPH criteria provided in DOE-STD-1020-2002. For SSCs not meeting these criteria and which cannot be easily remedied, budgets and schedule for required strengthening must be established on a prioritized basis. In addition, it is consistent with the intent of the Federal program developed by the ICSSC. When upgrading becomes necessary, the design should be based on the

current design criteria in the standard for the new facility. DOE G 420.1-2 provides guidance for facilities with a remaining service life of less than 5 years.

f. Define PC-1, PC-2, PC-3, and PC-4 and its relationship to nuclear facility design and the DSA.

The following is taken from DOE-STD-1020-2002.

Table 4 provides the flood criteria for performance categories 1 through 4. The criteria are specified in terms of the flood hazard input, hazard annual probability, design requirements, and emergency operation plan requirements. The hazard annual probability levels in table 4 correspond to the mean hazard.

Evaluation of the flood design basis for SSCs consists of

- determination of the design basis flood (DBFL) for each flood hazard as defined by the hazard annual probability of exceedance and applicable combinations of flood hazards;
- evaluation of the site storm water management system (e.g., site runoff and drainage, roof drainage);
- development of a flood design strategy for the DBFL that satisfies the criteria performance goals (e.g., build above the DBFL, harden the facility); and
- design of civil engineering systems (e.g., buildings, buried structures, site drainage, retaining walls, dike slopes, etc.) to the applicable DBFL and design requirements.

g. Discuss aspects of fire protection and fire hazards analysis and their relationship to nuclear facility design and the DSA.

DOE O 420.1B requires a fire protection program that incorporates the requirements of DOE O 420.1B, related DOE directives, and other applicable Federal, state, and local fire protection requirements. It also requires a system to ensure that the requirements of the DOE fire protection program are documented and incorporated in the plans and specifications for all new facilities and for significant modifications of existing facilities. This includes a documented review by a qualified fire protection engineer of plans, specifications, procedures, and acceptance tests. Fire protection programs are typically a credited safety management program in a nuclear facility's DSA and TSRs.

Table 4. Flood criteria summary

Item	Performance Category			
	1	2	3	4
Flood hazard input	Flood insurance studies or equivalent input	Site probabilistic hazard analysis	Site probabilistic hazard analysis	Site probabilistic hazard analysis
Mean hazard annual probability	2×10^{-3}	5×10^{-4}	1×10^{-4}	1×10^{-5}
Design requirements	Applicable criteria (e.g., governing local regulations, IBC 2000) shall be used for building design for flood loads (i.e., load factors, design allowables), roof design, and site drainage. The design of flood mitigation systems (i.e., levees, dams, etc.) shall comply with applicable standards.			
Emergency operation plans	Required to evacuate onsite personnel if facility is impacted by the DBFL	Required to evacuate onsite personnel and to secure vulnerable areas if site is impacted by the DBFL	Required to evacuate onsite personnel not involved in essential operations. Provide for an extended stay for personnel who remain. Procedures must be established to secure the facility during the flood such that operations may continue following the event	

Source: DOE-STD-1020-2002

Fire hazard analyses (FHAs) for all nuclear facilities, significant new facilities, and facilities that represent unique or significant fire safety risks are also required by the Order. The FHA should be developed using a graded approach, and the conclusions of the FHA should be incorporated into the accident analysis of the DSA and shall be integrated into design basis and beyond DBA conditions.

h. Identify and discuss the strengths and weaknesses of methods utilized to analyze the initiation and propagation of fires and of their potential release of hazardous materials.

The following is taken from NIST Special Report 1026 and DOE G 420.1-3.

Per the CFAST guidance report, CFAST is a zone-based fire model that was developed by NIST. The code has been widely used in the fire protection community to support alternate design approaches and post-fire investigations and as a research tool to better understand fire phenomena.

The CFAST code, while part of the toolbox collection of software, still may require software quality assurance (SQA) upgrades prior to meeting current established standards for software. However, until these CFAST upgrades are completed, CFAST can be applied safely under the guidance contained in the CFAST guidance report.

An uncontrolled fire in a nuclear facility can be a very energetic event. Severe smoke, excessive temperatures, and large thermal gradients are common. Such fires can breach containment barriers (glove box, ventilation ductwork, and building envelope), and because of the significant thermal gradients, readily disperse radioactive material. While DOE has a good record on fire safety, an uncontrolled fire remains a dominant risk in many nuclear facilities. To adequately evaluate the fire risk, calculations must be prepared that establish the fire severity and consequences expected for credible fire scenarios.

DOE G 420.1-3 states, "A tool that may be used in the development of a fire hazard analysis (FHA) is a fire model, such as those developed by NIST, as applied by qualified fire protection engineers. However, the use of such models is predicated on their being conservative and validated. As of this date, DOE has not sanctioned the use of any one model for use in an FHA. DOE acceptance of individual models will be considered on a case-by-case basis." The CFAST guidance report does not alleviate this requirement—outside of its use to evaluate source terms, CFAST will still require the case-by-case authorization from the appropriate authority having jurisdiction.

CFAST is a zone (or control volume) fire model that relies on the stratification behavior observed in most fires and represents the two layers as separate control volumes (i.e., upper layer and lower layer). Each layer is assumed to be uniform (i.e., temperature, smoke, and gas concentrations are assumed to be homogeneous throughout the layer). The time-dependent fire response for each layer is predicted based on Navier-Stokes equations integrated over the zones. Mass and energy exchange between the control volumes is estimated using both numerical techniques and correlations that approximate fire behavior.

When developing a DSA to the requirements of 10 CFR 830, there is an expectation that the accident analysis modeling results will be reasonably bounding. A single fire modeling simulation or even a small set will not usually support this expectation. As discussed earlier, there are many variables associated with fire phenomena, and sometimes the conservatism of the results is not necessarily intuitive. Because some fire behaviors can be counter-intuitive it is strongly recommended that a fire model begin with nominal conditions, rather than forcing specific parameters to their most bounding state. When the nominal model is working successfully, the inputs can be systematically varied to demonstrate a reasonably bounding solution. The single best metric to evaluate the severity of a fire is the heat release rate. Three of the most common thresholds that can influence the results of an FHA are secondary ignition, flashover, and steel failure.

i. Identify and discuss the methods used to determine the seismic hazard level to be used in design.

Specific technical details for addressing NPH events are provided in several DOE NPH standards:

- 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-1023-96, *Natural Phenomena Hazards Assessment Criteria*

The design and evaluation criteria developed in these standards are intended to ensure NPH issues are evaluated both consistently and with a consensus standard of conservatism. The basic approach begins with site-specific probabilistic severity data developed in accordance with DOE standards. Performance categories are then assigned to structures, systems, and components based on their safety function. Each performance category has a target performance goal, specified in terms of mean annual probabilities of exceedance. Consequently, the combination of performance category and site-specific severity data yields natural phenomena events of specified strength against which safety issues are evaluated.

The following is taken from DOE-STD-1021-93.

Five performance categories are currently defined. They are, in order of decreasing importance,

1. Performance category 4—Associated with SSCs whose failure during an NPH event could result in offsite consequences greater than or equal to the unmitigated release from a large (>200 MW) category A reactor severe accident. This definition is comparable to that for a hazard category 1 nuclear facility as used in 10 CFR 830.
2. Performance category 3—Associated with SSCs whose failure during an NPH event could result in offsite consequences greater than the SC SSC EG of 25 rem.
3. Performance category 2—Associated with SS SSCs, buildings in which more than 300 people assemble, or related to emergency functions to preserve the health and safety of workers.
4. Performance category 1—Associated with human occupancy, SSC failure resulting in worker fatality or injury, or cost-effective improvements possible.
5. Performance category 0—All other SSCs.

j. Identify and discuss the methods used to assess the structural response of structures and determine whether safety systems may be expected to remain functional following an earthquake of postulated intensity.

The following is taken from DOE-STD-1020-2002.

Seismic loading is defined in terms of a site-specific design response spectrum. Either a site-specific design response spectrum developed for the site, or a generic design response spectrum that is appropriate or conservative for the site may be used. PC-2 and lower SSCs may be designed or evaluated using the approaches specified in IBC 2000 seismic provisions. Common cause effects and interaction effects per DOE-STD-1021-93 should be taken into account. However, for PC-3 or higher, the seismic evaluation must be performed using a dynamic analysis approach that requires

- the input to the SSC model be defined by either a design response spectrum or a compatible time history input motion;
- the important natural frequencies of the SSC be estimated or the peak of the design response spectrum be used as input—multi-code effects must be considered;
- the resulting seismic induced inertial forces be appropriately distributed, and a load path evaluation for structural adequacy be performed.

A "dynamic analysis approach" does not imply that complex dynamic models must be used in the evaluation. Often equivalent static analysis models are sufficient if the three factors listed above are incorporated. However, use of such simplified models for structures in PC-3 or higher must be justified and approved by DOE. This dynamic analysis approach should comply with the seismic response analysis provisions of ASCE 4 (*Seismic Analysis of Safety-Related Nuclear Structures and Commentary)* except where specific exemptions are noted.

k. Identify the methods for evaluating the tolerance of structures and systems for natural phenomenon.

The following is taken from DOE-STD-1020-2002.

For existing SSCs, an assessment must be made for the as-is condition. This assessment includes reviewing drawings and conducting site visits to determine deviations from the drawings and any in-service deterioration. In-place strength of the materials can be used when available. Corrosive action and other aging processes should be considered. Evaluations should be conducted in order of priority, with highest priority given to those areas identified as weak links by preliminary investigations and to areas that are most important to personnel safety and operations with hazardous materials.

If an existing SSC does not meet the natural phenomena hazard design/evaluation criteria, several options need to be considered. Potential options for existing SSCs are to

- Conduct a more rigorous evaluation of SSC behavior to reduce conservatism that may have been introduced by simple techniques used for initial SSC evaluation. Alternatively, a probabilistic assessment of the SSC might be undertaken in order to demonstrate that the performance goals for the SSC can be met.
- The SSC may be strengthened to provide resistance to natural phenomena hazard effects that meet the NPH criteria.
- The usage of the SSC may be changed so that it falls within a lower performance category and consequently, less stringent requirements.

If SSC evaluation uncovers deficiencies or weaknesses that can be easily remedied, these should be upgraded without considering the other options. It is often more cost-effective to implement simple SSC upgrades than to expend effort on further analytical studies.

Evaluations of existing SSCs must follow or, at least, be measured against the NPH criteria in DOE-STD-1020-2002. For SSCs not meeting these criteria and which cannot be easily remedied, budgets and schedule for required strengthening must be established on a prioritized basis.

Priorities should be established on the basis of performance category, cost of strengthening and margin between as-is SSC capacity and the capacity required by the criteria. For SSCs that are close to meeting criteria, it is probably not cost-effective to strengthen the SSC in order to obtain a small reduction in risk. As a result, some relief in the criteria is allowed for evaluation of existing SSCs. It is permissible to perform such evaluations using NPH exceedance probability of twice the value specified for new design. For example, if the natural phenomena hazard annual probability of exceedance for the SSC under consideration was 10^{-4} it would be acceptable to reconsider the SSC at hazard annual probability of exceedance of 2×10^{-4}. This would have the effect of slightly reducing the seismic, wind, and flood loads in the SSC evaluation. Where it is not practical to undertake analysis based on double the probability, no more than 20 percent reduction in forces may be permissible. This amount of relief is within the tolerance of meeting the target performance goals and is only a minor adjustment of the corresponding NPH design and evaluation criteria.

The design and evaluation criteria for SSCs in PCs 0, 1, and 2 are similar to those given in model building codes. PC 0 recognizes that for certain lightweight equipment items, furniture, etc., and for other special circumstances where there is little or no potential impact on safety, mission, or cost, design or evaluation for NPHs may not be needed. Assignment of an SSC to PC 0 is intended to be consistent with, and not take exception to, model building code NPH provisions.

PC 1 criteria include no extra conservatism against NPHs beyond that in model building codes that include earthquake, wind, and flood considerations. PC 2 criteria are intended to maintain the capacity to function and to keep the SSC operational in the event of NPHs. Model building codes would treat hospitals, fire and police stations, and other emergency-handling facilities in a manner similar to PC 2 NPH design and evaluation criteria in DOE-STD-1020-2002.

PCs 3 and 4 SSCs handle significant amounts of hazardous materials or have significant programmatic impact. Damage to these SSCs could potentially endanger worker and public safety and the environment or interrupt a significant mission. As a result, it is very important for these SSCs to continue to function in the event of NPHs, such that the hazardous materials may be controlled and confined. For these categories, there must be a very small likelihood of damage due to NPHs. DOE-STD-1020-2002 NPH criteria for PC 3 and higher SSCs are more conservative than requirements found in model building codes and are similar to U.S. Department of Defense (DoD) criteria for high-risk buildings and NRC criteria for various applications, as illustrated in table B-2 in DOE-STD-1020-2002. Table 5 illustrates

how DOE-STD-1020-2002 criteria for the performance categories defined in DOE O 420.1B and the associated guides compare with NPH criteria from other sources.

Table 5. Comparison of performance categories from various sources

Source	**SSC Categorization**			
DOE-STD-1020, DOE Natural Phenomena Hazard Criteria	1	2	3	4
Uniform Building Code	General	Essential	—	—
DoD Tri-Service Manual for Seismic Design of Essential Buildings	—	—	High risk	
Nuclear Regulatory Commission		—	NRC fuel facilities	Evaluation of existing reactors

Source: DOE-STD-1020-2002

I. Discuss the importance of integrating safety analysis development with facility design.

The following is taken from DOE O 420.1B and DOE-STD-1189-2008.

1. Safety analyses must be used to establish
   - the identity and functions of SC and SS SSCs and
   - the significance to safety of functions performed by SC and SS SSCs.

2. Safety analyses must address
   - hazards inherent to the facility and its activities,
   - NPH (See chapter IV for examples of NPH and additional requirements), and
   - external, man-induced hazards (factors such as proximity to airports, pipelines, hazardous traffic on roads or waterways, and adjacent facilities).

3. Safety analyses must be performed as early as practical in conceptual or preliminary design processes to ensure that required safety SSCs are specified in the final design.
4. Safety analyses must be performed in accordance with the requirements for safety analysis defined in DOE directives and technical standards for a DSA.

DOE-STD-1189-2008 provides DOE's expectations for the integration of safety into the design process.

20. Nuclear safety specialists shall demonstrate a working level knowledge of the TSRs as described in 10 CFR 830.205, Technical Safety Requirements, and DOE G 423.1-1, Implementation Guide for Use in Developing Technical Safety Requirements, with respect to their impact on the Department's nuclear safety.

a. Discuss the purpose of TSRs.

The following is taken from DOE G 423.1-1.

TSRs identify the limitations of each DOE-owned, contractor-operated nuclear facility based on the documented safety analysis and any additional safety requirements established for the facility.

TSRs are aimed at confirming that SSCs and personnel can perform their intended safety functions under normal, abnormal, and accident conditions. TSRs play a key role in safety oversight for both the contractor and the DOE. They provide the clear definition of the safety envelope imposed on the facility operations.

b. Describe the responsibilities of contractors authorized to operate nuclear facilities for TSRs.

The following is taken from DOE G 423.1-1.

Contractors, in the preparation of DSAs, identify how the safety requirements of the safety management rule apply to a specific facility, and describe how the contractor undertakes to design, build, and operate the facility to be in conformance with the applicable statutes and DOE rules and directives to ensure facility safety. The analysis of operations and accidents defines the limits of safe operations, identifies the required performance of safety-class and safety-significant SSCs, and describes any ACs or procedures that are necessary to meet the specific safety criteria for the facility.

Per 10 CFR 830.205: A contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility must

- develop technical safety requirements that are derived from the documented safety analysis;
- prior to use, obtain DOE approval of technical safety requirements and any change to technical safety requirements; and
- notify DOE of any violation of a technical safety requirement.

c. Define the following terms and discuss the purpose of each:

- **SL**
- **Operating limits**
- **Limiting control settings**
- **LCO**
- **Surveillance requirements**
- **ACs**
- **SAC**

SL

Safety limits are the limits on process variables associated with those safety-class physical barriers, generally passive, that are necessary for the intended facility functions and which are required to guard against the uncontrolled release of radioactive materials.

Operating Limits

OLs are the limits required to ensure the safe operation of a nuclear facility, including limiting control settings and LCOs.

Limiting Control Settings

Limiting control settings are boundaries on safety systems that regulate process variables to prevent exceeding a safety limit.

LCOs

LCOs are the limits that represent the lowest functional capability or performance level of safety SSCs required for safe operations.

Surveillance Requirements

SRs are requirements relating to testing, calibration, or inspection to ensure the necessary operability and quality of safety SSCs and their support systems required for safe operations.

ACs

ACs are provisions relating to organization and management procedures, record keeping, assessment, and reporting necessary to ensure the safe operation of a facility.

SAC

SACs are ACs that are selected to provide preventive and/or mitigative functions for specific potential accident scenarios, and that also have safety importance equivalent to engineered controls that would be classified as safety-class or safety-significant if the engineered controls were available and selected.

d. Describe the general content of each of the following sections of the TSR:
- **Use and Application**
- **Basis**
- **Design Features**

The following definitions are taken from DOE G 423.1-1.

Use and Application

The use and application section of the TSR should contain basic information and instructions for using and applying the TSR. The following elements should be addressed under separate headings in this section:

- Definitions. Provide an alphabetical list of terms used throughout the TSR and their corresponding definitions. Include a note on the first page of the list stating that defined terms appear in uppercase type throughout the TSR.

- Operational Modes (Reactors). Define the operational modes for reactor facilities, and state that in the interest of uniformity, the operational conditions or modes listed are preferred, and an attempt should be made to fit each reactor facility into this scheme.
- Operational Modes (Nonreactor Nuclear Facilities). Define the operational modes for nonreactor facilities, and state that in the interest of uniformity, the operational conditions and modes listed are preferred, and an attempt should be made to fit each nonreactor nuclear facility into this scheme. If, however, a nonreactor nuclear facility cannot be made to fit, modes may be defined as needed, provided the definitions are clear, and there are definite lines of demarcation between modes.
- Frequency Notation. The frequency notations, as used in the surveillances and elsewhere, should be defined when included in the TSR.

Basis

The TSR basis provides summary statements of the reasons for the selection of each specific SL, OL, and SR. The bases show how the numerical values, conditions, surveillances, and action statements fulfill the purpose derived from the safety documentation. Included in the basis should also be a description of the safety functions that each safety system provides and identification of what is included in each safety system.

The primary purposes for describing the bases of each requirement are to ensure future changes to the requirement will not affect its original intent or purpose by invalidating the safety analysis and to aid in understanding why the requirement exists.

Design Features

This section describes those design features that, if altered or modified, would have a significant effect on the safe operation of the facility. The important attributes of the passive design features that are taken credit for in the accident analysis should be described completely. These design features are normally passive characteristics of the facility not subject to change by operations personnel, e.g., shielding, structural walls, relative locations of major components, installed poisons, or special materials. Active safety features are normally described in the DSA and are the subject of the various TSRs, so they are not normally described in the design features section.

e. Discuss the definition and implementation principles for the term "operability" as used in a TSR.

The following is taken from DOE G 423.1-1.

Operability embodies the principle that a system, subsystem, train, component, or device can perform its safety function(s) only if all necessary support systems are capable of performing their related support functions. A system or component can be degraded but still operable if it remains capable of performing its required safety function at the level assumed in the accident analysis. If systems, components, or equipment are observed to be functioning, but under stress, then judgment must be used concerning a declaration of inoperability. General principles of operability should be followed in generating LCOs:

- General principle 1. A system is considered operable as long as there are assurances that it is capable of performing its specified safety function(s).
- General principle 2. A system can perform its specified safety function(s) only when all of its necessary support systems are capable of performing their related support functions.
- General principle 3. When all systems designed to perform a certain safety function are not capable of performing that safety function, a loss of function condition exists.
- General principle 4. When a system is determined to be incapable of performing its intended safety function(s), the declaration of inoperability should be immediate.

f. Discuss the relationship of functional requirements and performance criteria to the TSR.

The following is taken from DOE G 423.1-1.

TSRs define the performance requirements of SSCs and identify the safety management programs used by personnel to ensure safety. TSRs are aimed at confirming that SSCs and personnel can perform their intended safety functions under normal, abnormal, and accident conditions. These requirements are identified through hazard analysis of the activities to be performed and identification of the potential sources of safety issues. Safety analyses to identify and analyze a set of bounding accidents that take into account all potential causes of releases of radioactivity also contribute to development of TSRs. Through analyses of the encompassing bounding accidents, the necessary safety systems and accident mitigating systems are identified and their characteristics are defined. Flowing from the analyses is information that provides the bases for controls, limits, and conditions for operation, known as TSRs. The content of the DSA must remain valid so that the safety basis of the facility, as implemented in operations through the TSR, remains valid. Therefore, there is a commitment to the process of unreviewed safety questions regarding any proposed change to the facility or its operations as described in the DSA. Likewise, all changes to the TSR bases presented in the DSA should be incorporated into the TSRs to ensure the information contained therein reflects the current safety basis of the facility. Any proposed revision to a TSR should be examined to ensure the basis for the change is supported in the DSA. The TSR rule requires that such revisions be submitted to DOE for review with the basis for the proposed change. The change to the TSR must be approved by DOE before it is implemented.

g. Discuss the conditions that constitute a violation of the TSR and state the reporting requirements should a violation occur.

The following is taken from DOE G 423.1-1.

Although the TSR elements have an importance hierarchy, a TSR violation can occur for each type of TSR. Violations of a TSR occur as a result of the following four circumstances:

1. Exceeding an SL
2. Failure to complete an action statement within the required time limit following exceeding a limiting control setting or failing to comply with an LCO

3. Failure to perform a surveillance within the required time limit
4. Failure to comply with an AC statement

Failure to comply with an AC statement is a TSR violation when either the AC is directly violated, as would be the case with not meeting minimum staffing requirements for example, or the intent of a referenced program is not fulfilled. To qualify as a TSR violation, the failure to meet the intent of the referenced program would need to be significant enough to render the DSA summary invalid. TSR violations involving SLs require the facility to begin immediately to go to the most stable, safe condition attainable, including total shutdown. A grace period is sometimes provided to perform a missed surveillance to provide time for the performance of the missed surveillance, thereby avoiding the need for a facility to take immediate, possibly unnecessary corrective action. Entering the grace period remains a TSR violation even though an immediate corrective action may not be required.

Reporting of all TSR violations should be made in accordance with the provisions of DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*. The reporting of violations on ACs can involve judgment since the details of programs, like a program for criticality control, do not appear directly as a TSR, and some program requirements are more important than others. Violations of controls identified in the accident or criticality scenarios in the DSA should be reported as if they were TSR violations. To ensure consideration for mitigation in potential enforcement actions, identified TSR violations should be evaluated for voluntary reporting to the DOE Noncompliance Tracking System.

h. Discuss the requirements for AC of the TSR.

The following is taken from DOE G 423.1-1.

ACs are the provisions relating to organization and management, procedures, record keeping, reviews, and audits necessary to ensure safe operation of the facility. ACs may include reporting deviations from TSRs, staffing requirements for facility positions important to safe operation of the facility, ACs of the criticality safety program, and commitments to safety management programs important to worker safety. In general, the ACs should document all those administrative functions that are required to meet facility safety criteria as identified in the DSA, including commitments to safety management programs. It is expected that the ACs will be tailored to the facility activities and the hazards identified in the DSA. This tailoring should be a direct result of the DSA, but it may also result from institutional requirements that address many facilities.

As a general practice, safety controls for individual accident scenarios based on engineered SSCs are preferred to ACs because they are usually more reliable and more predictable. The tendency to use ACs as an expedient alternative to an LCO or limiting control settings should be avoided when possible. Efforts should be made to use engineered SSCs whenever possible for controlling the likelihood and consequences of accidents. ACs should be considered for defense in depth rather than the primary or redundant controls. While ACs may be acceptable for ensuring safe operation, their generally lower reliability, compared with engineered

controls, should be evaluated carefully when choosing safety measures for long-term hazardous activities.

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

- Use of reader/worker/checker systems
- Independent verification
- Positive feedback systems
- Human factor analysis
- Operator training and certification
- Continuing training and requalification
- Abnormal event response drills
- Ergonomic considerations in procedures

When invoking ACs for control of accident scenarios, the preceding attributes, appropriate to the consequences of the accidents they are intended to prevent, should be considered and also invoked.

i. Discuss the role of DSA in selecting a TSR and the respective flowdown.

The following is taken from DOE G 423.1-1.

The DSA required by 10 CFR 830.204 furnishes the technical basis for TSRs. For some facilities, other documentation such as the SER may provide additional safety controls or operating restrictions that should be reflected in the TSRs. The TSR derivation section in the DSA is intended to provide a link between the safety analysis and the list of variables, systems, components, equipment, and administrative procedures that must be controlled or limited in some way to ensure safety.

j. Discuss the requirements for emergency actions that depart from the approved TSR.

The following is taken from DOE G 423.1-1.

In an emergency, if a situation develops that is not addressed by the TSR, site personnel are expected to use their training and expertise to take actions to place the facility in a safe and stable configuration. Also, site personnel may take actions that depart from the requirements of a TSR provided (a) an emergency situation exists, (b) these actions are needed immediately to protect workers, the public, or the environment from imminent and significant harm, and (c) no action consistent with the TSR is immediately apparent. Such action must be approved by a certified operator for reactor facilities or by a person in authority as designated in the TSRs for nonreactor nuclear facilities. If emergency action is taken, both a verbal notification should be made to the responsible head of the field element and a written report made to the CSO within 24 hours.

k. Discuss the provisions a contractor may follow to develop alternatives to TSR for environmental restoration activities.

The following is taken from DOE G 423.1-1.

A contractor for an environmental restoration activity may follow the provisions of 29 CFR 1910.120 or 1926.65 for construction activities to develop the appropriate hazard controls (rather than TSR guidance) provided the activity involves either (1) work not done within a permanent structure, or (2) the decommissioning of a facility with only low-level residual fixed radioactivity. Implicit in this guidance is an understanding that reasonable efforts to remove radioactive systems, components, and stored materials have been completed, and that the work does not prudently require the use of active safety systems or components designed to prevent or mitigate the accidental release of hazardous radioactive materials. DOE-STD-1120-2005 also provides guidance that should be considered in the development of alternatives to TSRs for decommissioning activities.

l. Discuss the requirements for the contractor to change the TSR.

The following is taken from DOE G 423.1-1.

Changes to the TSR should be designated in the following manner:

- A list of pages in effect, with page number and date
- A record of revision pages
- Sidebar changes in the TSR text
- The page number, the document number, and the revision number on each page

m. Discuss the application of the graded approach relative to the TSR.

The following is taken from DOE G 423.1-1.

The graded approach is not directly applicable to the TSRs required by 10 CFR 830.205. However, the graded approach is specified for DSAs required by 10 CFR 830.204. Thus, the level of detail in the DSA, and the number of safety parameters identified in the DSA section deriving the TSRs, will have a direct effect on the number and type of resulting TSRs.

<u>Mandatory Performance Activities</u>:

a. Participate on a combination of at least five (5) safety basis document reviews and/or review of safety basis documents and/or performance of a field walk-down of a safety related SSC [including the associated surveillance requirements and LCO/Limiting Condition Statements (LCS)] to determine proper derivation of SL/LCS/LCO/SAC/AC, including associated surveillance requirements.

Mandatory performance activities are performance based. The Qualifying Official will evaluate the completion of this competency.

21. Nuclear safety specialists shall demonstrate a working level knowledge of 10 CFR 830.203, Unreviewed Safety Question Process, and DOE G 424.1-1A, Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements, with respect to their impact on the Department's nuclear safety.

a. Discuss the purpose of the USQ process.

The following is taken from DOE G 424.1-1A.

The USQ process allows contractors to make physical and procedural changes and to conduct tests and experiments without prior DOE approval if the proposed change can be accommodated within the existing safety basis.

b. Discuss the reasons for performing a USQ determination.

Title 10 CFR 830.203 requires an unreviewed safety question determination (USQD) for a

- temporary or permanent change in the facility as described in the existing DSA
- temporary or permanent change in procedures as described in the existing DSA
- test or experiment **not** described in the existing DSA
- potential inadequacy of the DSA because the analysis may not be bounding or may be otherwise inadequate (potential inadequacy of the safety analysis [PISA])

c. Define the following terms:

- **Discrepant as-found condition**
- **Potential inadequacy in the safety analysis**
- **Proposed change**

The following definitions are taken from DOE-G 424.1-1A.

Discrepant As-Found Condition

A discrepant as-found condition is a condition where the actual physical configuration of a facility, process, or TSR control does not match the analysis of the facility, process, or TSR.

Potential Inadequacy in the Safety Analysis

A potential inadequacy in the safety analysis occurs when a contractor identifies or is informed of a situation that indicates that the safety analyses that support the DOE-approved safety basis may not be bounding or may be otherwise inadequate.

Proposed Change

Title 10 CFR 830.203, "Unreviewed Safety Question Process," allows contractors to make physical and procedural changes and to conduct tests and experiments without prior DOE approval if the proposed change can be accommodated within the existing safety basis. The contractor must evaluate any proposed change to ensure that it will not affect the safety basis of the facility either explicitly or implicitly.

d. Define the conditions for a USQ.

The following is taken from DOE G 424.1-1A.

Seven criteria are used to determine if a positive USQD exists:

1. Could the probability of the occurrence of an accident previously evaluated in the DSA be increased?
2. Could the consequences of an accident previously evaluated in the DSA be increased?
3. Could the probability of occurrence of malfunction of equipment important to safety previously evaluated in the DSA be increased?
4. Could the consequences of a malfunction of equipment important to safety previously evaluated in the DSA be increased?
5. Could the possibility of an accident of a different type than any evaluated previously in the DSA be created?
6. Could the possibility of a malfunction of a different type than any evaluated previously in the DSA be created?
7. Could a margin of safety be reduced?

e. Describe the responsibilities of contractors authorized to operate nuclear facilities for the performance of safety evaluations.

The following is taken from DOE G 424.1-1A.

USQ requirements relating to PISAs include that in the event of a PISA, and after a formal USQ determination, an evaluation of the safety of the situation be performed and the results submitted to DOE prior to removing any operational restrictions taken to maintain the facility in a safe condition.

This terminology is in 10 CFR 830.203(g)(1) and (4), and refers to the actions to be taken in the event of a PISA. Basically, a safety evaluation is a safety analysis that demonstrates adequate safety with the existing situation so that any interim measures (operational restrictions) to maintain the facility in a safe condition can be removed. If that is not the case (adequate safety), then the analysis should be accompanied by, or followed with, a proposed resolution, also with a safety analysis that demonstrates adequate safety.

f. Describe the actions to be taken by a contractor upon identifying information that indicates a potential inadequacy of safety analyses or a possible reduction in the margin of safety as defined in the TSR.

The following is taken from DOE G 424.1-1A.

For purposes of performing the USQ determination, a margin of safety is defined by the range between two conditions. The first is the most adverse condition estimated or calculated in safety analyses to occur from an operational upset or family of related upsets. The second condition is the worst-case value known to be safe, from an engineering perspective. This value would be expected to be related to the condition at which some accident prevention or

mitigation action is taken in response to the upset or accident, not the actual predicted failure point of some component.

Hazard control documents set forth the minimum acceptable limits for operation under normal and specified failure conditions; they ensure that the available safety equipment and operating conditions meet the assumptions in the existing safety analyses. They distill those aspects of the safety analyses that are required to ensure the performance of safety SSCs and personnel as relied on and defined in the safety analyses.

The bases for a hazard control should define the margin of safety. If the bases of a hazard control do not specifically identify a margin of safety, the DSA and other appropriate safety basis documents should be reviewed to determine whether the proposed change, test or experiment, or new information has or would result in a reduction in a margin of safety. The judgment on whether the margin is reduced should be based on physical parameters or conditions that can be observed or calculated.

The safety margin is sometimes implicitly described. A margin of safety can depend on a parameter other than one of the process variables. Therefore, the precise determination of a numerical value associated with a change is not always possible. Implicit margins are, for example, conditions for acceptance for a computer code, method, or industry-accepted practice. It may be sufficient to determine only the direction of the margin change (that is, increasing or decreasing) due to the proposed change.

Safety margins generally include worst-case assumptions of initial conditions, conservative assumptions in computer modeling and codes, allowance for instrument drift and system response time, redundancy and independence of components in safety trains, and plant response during operating transient and accident conditions. A change that affects initial conditions, a system response time, or some other parameter that can affect the course of an accident analysis supporting the bases of hazard controls is evaluated to determine whether the change would reduce a margin of safety.

Title 10 CFR 830.205 requires that changes to the TSRs be submitted to DOE for review and approval. Changes to the TSRs could involve the need either to modify an existing TSR or to add a new TSR. If it is known that a proposed change only involves a TSR change, it is not required to go through the USQ determination to determine if DOE approval is also required by 830.203. Similarly, if a change involves a TSR change, calling the change a positive USQ determination just because it requires DOE approval would be inappropriate.

g. Discuss the qualification and training requirements for personnel who implement the USQ process.

The following is taken from DOE G 424.1-1A.

Implementing procedures should establish the training and qualifications for personnel performing the USQ process, such as educational background; years and/or types of work experience and knowledge of the facility; understanding of DOE facility safety basis

requirements, including the USQ process; and familiarity with the facility-specific safety basis.

All personnel responsible for preparing, reviewing, or approving USQ documents should receive training on the application of 10 CFR 830.203, including any facility-specific procedures. The recommended interval for retraining is every 2 years.

The contractor should maintain a list of those personnel who are currently qualified to perform the USQ process.

h. Discuss the actions to be taken if it is determined that a potential inadequacy in the safety analysis is involved.

The following is taken from DOE G 424.1-1A.

When a PISA is declared, the contractor must first "take action, as appropriate, to place or maintain the facility in a safe condition" (10 CFR 830.203(g)(1)). A safe condition may allow continued facility operation (possibly with operational restrictions or compensatory measures) if the impact on safety is judged to be acceptable, even when an SSC may be degraded or nonconforming. An operability determination is a forward-looking evaluation by the operating contractor of whether there is a reasonable expectation that continued operation of the facility is safe even when a degraded or nonconforming condition (PISA) and a USQ exist. An immediate operability determination should be made based on the best available information and operational restrictions imposed, if necessary, upon confirmation of the condition. Subsequently, a final determination should be made and documented following a thorough engineering evaluation. The elements of the final operability determination should include

- description of the degraded or nonconforming condition of the SSC;
- description of the relationships on safe operations of the SSC functions;
- evaluation of the operability of the SSC given its condition
  - using analysis, tests, operating experience, and/or engineering judgment,
  - considering availability of other equipment, conservatisms and margins, and cumulative effects of other outstanding degraded or nonconforming conditions;

- specification of additional operating restrictions if necessary (e.g., compensatory measures, additional engineering analysis by a certain date);
- specification of restoration actions (may be added later).

Restoration actions for the degraded or nonconforming condition are to be developed by the contractor and scheduled at the first available opportunity commensurate with the safety significance and extent of restoration actions in an integrated manner with other facility commitments and resources. The final operability determination may be included as part of the evaluation of the safety of the situation required to be submitted to DOE before removal of any operational restrictions.

Written USQDs are needed when a contractor identifies or is informed of a situation that indicates that the safety analyses that support the DOE-approved safety basis may not be bounding or may be otherwise inadequate.

Because a safety analysis inadequacy has potential to call into question information on which authorization of operations is based, the contractor is to

1. take appropriate action to place or maintain the facility in a safe condition,
2. expeditiously notify DOE when the information is discovered,
3. perform a USQD and notify DOE of the results promptly, and
4. complete evaluation of the safety of the situation and submit it to DOE before removing any operational restrictions implemented to compensate for the discrepancy.

Notification (the second step) allows reasonable time (hours or days but not weeks) to confirm that a safety analysis is inadequate.

The time frame after initial notification of DOE until submittal of the results of the USQD (the third step) should be on the order of hours or days, not weeks or months. If a USQ is determined to be present, the evaluation of the safety of the situation should receive not only DOE's review, but also its approval before any operational restrictions are removed.

The facility DSA and the PISA requirements of 10 CFR 830.203 are important because the DSA defines the safety risks that DOE has accepted when authorizing operation of the facility, and the PISA process provides a means to resolve inadequacies in the safety analysis. Because that analysis is the baseline reference for the USQ process, if it were inadequate, the USQ process would be compromised; that is, USQDs would be performed against a faulty baseline.

The USQ process includes special actions to be taken if it appears that the safety analyses might be inadequate. In general, potential for inadequate analysis arises from the following entry conditions:

- a discrepant as-found condition;
- an operational event or incident; or
- new information, including discovery of an error, sometimes from an external source.

The main consideration is that the analysis does not match the current physical configuration, or the analysis is inappropriate or contains errors. The analysis might not match the facility configuration because of a discrepant as-found condition. Analytical errors might involve using incorrect input values, invalid assumptions, improper models, or calculation errors. The USQ process starts when facility management has information that gives reason to believe that there is a potential that the facility DSA might be inadequate.

A justification for continuing operations (JCO) offers an alternative to ceasing operations when an unplanned condition arises that would otherwise require shutting down the facility. A JCO is a mechanism by which a contractor may request that DOE review and approve a temporary amendment to the facility safety basis that would allow the facility to continue

operating in view of a specific and unexpected situation, the safety significance of the situation, and the compensatory measures being applied during this period. When DOE approves such a JCO, the approval is in effect a temporary amendment of the safety basis that would permit operations to continue under specified conditions, including a defined termination point. The DOE-approved JCO becomes a part of the facility safety basis for a defined limited period.

A JCO is expected to define an appropriate set of temporary hazard controls (that is, compensatory measures) to be in effect during the life of the JCO. In some cases, these hazard controls might involve temporary changes to the facility TSRs.

A JCO should have a predefined, limited life only as may be necessary to perform the safety analysis of the unexpected situation, to identify and implement corrective actions, and to update the safety basis documents on a permanent basis. The JCO should define the termination point of the life of the JCO. In most cases, this would take the form of a functional point, such as the completion of turnover of a physical modification for routine operations, which would occur after implementing the modification, post-modification testing, updating critical documentation, and training of the operations staff.

A JCO is not an appropriate means to request a change of the safety basis for a planned operation. In that case, a request for a change to the facility safety basis should be prepared by the contractor and submitted to DOE for approval. Because the JCO is established in response to an unexpected condition, event, or new information, it is inappropriate to use it in planning new activities without specific DOE approval. A JCO amendment of the safety basis should not be used for performing a USQD for a proposed new activity.

A special case regarding PISAs exists when dealing with external audit team multiple concerns, each of which may (or may not) indicate the possibility of a potential inadequacy in the safety analyses. It may be impractical for facility staff to assess the situation quickly and disposition multiple concerns in the time frame normally expected for deciding that a concern indicates a PISA (hours to days) and performing a USQD for each finding that qualifies as a PISA. In the face of multiple issues, it might be concluded that the short-term response to assuring a safe condition is to shut down operations. This might not be appropriate in all cases.

As an option in these cases, except where it is apparent that an imminent hazard exists, DOE should be consulted without delay, and a mutually agreed upon approach to handling the concerns, including an expeditious schedule, should be developed. This approach should have a high priority for addressing the concerns, should prioritize the safety-related concerns, and should disposition each as described for individual PISAs. Where it is apparent that an imminent hazard exists, the four steps for a potential inadequacy should be undertaken without delay.

A similar situation exists for design basis reconstitution projects where the original design bases may be lost or outdated. In this case, it can be expected that a team of engineers may identify many questions or issues that may not have current documentation and which may or

may not constitute PISAs. For the purposes of the USQ process, design reconstitution projects can be regarded as DSA upgrades; that is, for DSA upgrades, USQs should not result from the use of new analytical tools or in response to new requirements.

The USQ process is not applicable when new requirements are being implemented or different analysis methods that are used result in changed accident consequences or probabilities. The USQ process is applicable when the project identifies situations where it is apparent that the existing safety basis may not be bounding or may be otherwise inadequate. A reconstitution project should have a process for prompt sorting and prioritizing of the questions and issues between those that can be addressed as a normal part of the reconstitution project and those that are to be handled promptly as PISAs. This process should be sufficiently timely to ensure that the expectations for PISAs can be met.

The USQ process does not apply to DSA upgrades in response to new requirements or to the use of new or different analytical tools during the upgrade process. However, the USQ process does apply when there is reason to believe that the current safety basis might be in error or otherwise inadequate.

i. Discuss the following terms as they apply to USQs:

- **Categorical exclusions**
- **Prior USQ determinations**
- **Inconsequential changes**
- **Margin of safety**
- **Design/evaluation basis accidents**
- **Important to safety**
- **Safety basis**
- **Restoration modification**
- **Evaluation of safety**
- **USQ**
- **Justification for Continued Operations (JCO)**

The following definitions are taken from DOE G 424.1-1A unless another reference is identified.

Categorical Exclusions

A categorical exclusion is an exclusion from the requirements that USQDs be performed on proposed changes to a category of SSCs or procedures as a result of a determination that the category cannot credibly have the capability of creating a USQ if changed. Categorical exclusions are regarded as part of the contractor's USQ procedure and require DOE approval.

Prior USQ Determinations

Because application of the USQ process depends on facility-specific information, results of a USQD in one facility generally cannot be extrapolated to other facilities.

Inconsequential Changes

Title 10 CFR 830.203 allows contractors to make physical and procedural changes and to conduct tests and experiments without prior DOE approval if the proposed change can be accommodated within the existing safety basis. The contractor must evaluate any proposed change to ensure that it will not affect the safety basis of the facility either explicitly or implicitly. The USQ process is applicable to the DSA, conditions of approval in safety evaluation reports, and facility-specific commitments made in compliance with DOE rules, Orders, or policies.

Margin of Safety

For purposes of performing the USQ determination, a margin of safety is defined by the range between two conditions. The first is the most adverse condition estimated or calculated in safety analyses to occur from an operational upset or family of related upsets. The second condition is the worst-case value known to be safe, from an engineering perspective. This value would be expected to be related to the condition at which some accident prevention or mitigation action is taken in response to the upset or accident, not the actual predicted failure point of some component.

Hazard control documents set forth the minimum acceptable limits for operation under normal and specified failure conditions; they ensure that the available safety equipment and operating conditions meet the assumptions in the existing safety analyses. They distill those aspects of the safety analyses that are required to ensure the performance of safety SSCs and personnel as relied on and defined in the safety analyses.

The bases for a hazard control should define the margin of safety. If the bases of a hazard control do not specifically identify a margin of safety, the DSA and other appropriate safety basis documents should be reviewed to determine whether the proposed change, test or experiment, or new information has or would result in a reduction in a margin of safety. The judgment on whether the margin is reduced should be based on physical parameters or conditions that can be observed or calculated.

Design/Evaluation Basis Accidents

The following is taken from DOE-STD-3009-94.

The major categories of DBAs are internally initiated operational accidents (e.g., fires, explosions, spills, criticality); natural phenomena events for the site (e.g., earthquakes, tornadoes) that could affect the facility; and externally initiated, man-made events such as airplane crashes, transportation accidents, adjacent facility events, etc., that can either cause releases at the facility under examination or have a major impact on facility operations.

A DBA is an accident from which the design requirements for a facility or SSC were derived. An evaluation basis would apply to older facilities where the original design bases may be lost or outdated or never clearly defined. Often termed “derivative DBAs,” evaluation basis accidents are used to estimate the response of SSCs to “the range of accident scenarios” and

stresses that bound "the envelope of accident conditions to which the facility could be subjected" in order to evaluate accident consequences.

Important to Safety

Equipment important to safety includes any equipment whose function, malfunction, or failure can affect safety directly or indirectly. This includes safety-class and safety-significant SSCs, and other systems that perform an important defense-in-depth function, equipment relied on for safe shutdown, and in some cases, process equipment. Support systems to safety systems that are required for the safety function are also safety systems, and should be included.

Safety Basis

According to DOE-STD-3009-94, a safety basis is 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.

Restoration Modification

Restoration actions for the degraded or nonconforming condition are to be developed by the contractor and scheduled at the first available opportunity commensurate with the safety significance and extent of restoration actions in an integrated manner with other facility commitments and resources. The final operability determination may be included as part of the evaluation of the safety of the situation required to be submitted to DOE before removal of any operational restrictions.

Evaluation of Safety

USQ requirements relating to PISAs include that in the event of a PISA, and after a formal USQ determination, an evaluation of the safety of the situation be performed and the results submitted to DOE prior to removing any operational restrictions taken to maintain the facility in a safe condition. This terminology is in 10 CFR 830.203(g)(1) and (4), and refers to the actions to be taken in the event of a PISA.

Basically, a safety evaluation is a safety analysis that demonstrates adequate safety with the existing situation so that any interim measures to maintain the facility in a safe condition can be removed. If that is not the case, then the analysis should be accompanied by, or followed with, a proposed resolution, also with a safety analysis that demonstrates adequate safety.

USQ

A USQ exists when

- the probability of the occurrence or the consequences of an accident or the malfunction of equipment important to safety previously evaluated in the DSA could be increased,
- the possibility of an accident or malfunction of a different type than any evaluated previously in the DSA could be created, or
- a margin of safety could be reduced.

Justification for Continued Operations (JCO)
The following is taken from DOE G 424.1-1A.

A JCO offers an alternative to ceasing operations when an unplanned condition arises that would otherwise require shutting down the facility. A JCO is a mechanism by which a contractor may request that DOE review and approve a temporary amendment to the facility safety basis that would allow the facility to continue operating in view of a specific and unexpected situation, the safety significance of the situation, and the compensatory measures being applied during this period. When DOE approves such a JCO, the approval is in effect a temporary amendment of the safety basis that would permit operations to continue under specified conditions, including a defined termination point. The DOE-approved JCO becomes a part of the facility safety basis for a defined limited period.

A JCO is expected to define an appropriate set of temporary hazard controls (that is, compensatory measures) to be in effect during the life of the JCO. In some cases, these hazard controls might involve temporary changes to the facility TSRs.

A JCO should have a predefined, limited life only as may be necessary to perform the safety analysis of the unexpected situation, to identify and implement corrective actions, and to update the safety basis documents on a permanent basis. The JCO should define the termination point of the life of the JCO. In most cases, this would take the form of a functional point, such as the completion of turnover of a physical modification for routine operations, which would occur after implementing the modification, post-modification testing, updating critical documentation, and training of the operations staff.

A JCO is not an appropriate means to request a change of the safety basis for a planned operation. In that case, a request for a change to the facility safety basis should be prepared by the contractor and submitted to DOE for approval. Because the JCO is established in response to an unexpected condition, event, or new information, it is inappropriate to use it in planning new activities without specific DOE approval. A JCO amendment of the safety basis should not be used for performing a USQD for a proposed new activity.

j. Discuss the responsibilities of the contractor associated with USQ summaries and the USQ procedure.

According to DOE G 424.1-1A, all contractors responsible for nuclear facilities submit annual summary descriptions to DOE of all USQDs performed. Items that were screened out and a USQD was not necessary do not need to be included in the annual summary (although they should be retained in the records of USQ actions). This report should be submitted on a schedule commensurate with annual update of the DSA.

k. Describe DOE's responsibilities when not agreeing with a negative determination.

According to DOE G 424.1-1A, DOE, as part of its oversight responsibility of the USQ process, can declare that a USQ exists. Such a declaration might result from a disagreement with a contractor's negative USQ determination or might result from a condition for which

the contractor has not done a USQ determination. When DOE declares a USQ, it is because DOE believes it should be involved in the review and approval of the situation to fulfill its responsibilities.

l. Discuss why the application of the graded approach does not apply to the USQ process.

According to DOE G 424.1-1A, no steps of the USQ process can be eliminated based on a graded approach. In some situations, attempts to apply the graded approach to the USQ process have resulted in inadequate USQ determinations. For example, some contractors have applied the graded approach to the change control processes in a manner that does not require the application of formal change controls unless the change involves equipment, procedures, or operations important to safety. Caution needs to be applied in such a situation to ensure that this approach does not prevent changes from being considered by the USQ process, which is a subset of change control. The only application of the graded approach to the USQ process is indirect. The graded approach may give a rough indication of how much justification or basis information should be provided when explaining the answers to each of the seven USQ determination criteria. More elaborate and thorough basis information would be expected for changes to safety equipment than for non-safety equipment. In any case, the justification for the answers to the USQ determination criteria needs to be defensible.

<u>Mandatory Performance Activities</u>:

a. Demonstrate by participation on either at least one (1) assessment of the contractor USQ process or one (1) regulatory review of either a new or revised contractor USQ procedure or review of one (1) JCO.

Mandatory performance activities are performance based. The Qualifying Official will evaluate the completion of this competency.

22. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the relationships between the problems being addressed by safety analysis and computer codes, the design requirements for the codes, and the components of the codes.

a. Identify how functional requirements and applicability of safety analysis and design computer codes are defined, documented, and controlled relative to modeling and data assumptions, design constraints, sizing and timing conditions, and input/output parameters.

Section 5 of DOE O 414.1C prescribes safety software quality requirements. These requirements are necessary to ensure that DOE/NNSA safety software in nuclear facilities performs its intended specific functions in relation to SSCs and that the classification, design, and analysis associated with nuclear facility operations is correct. These requirements complement those of 10 CFR 830 and provide detail for work associated with safety software

that is conducted under the nuclear facility quality assurance program (QAP) compliant with 10 CFR 830.

Work processes involving safety software must be developed and implemented using national or international consensus standards and must include the following elements:

- Involve facility design authority in identifying software specification, acquisition, design, development, verification and validation (including inspection and test), configuration management, maintenance, and retirement.
- Identify, document, and maintain safety software inventory.
- Establish grading levels for safety software. Document those grading levels in the QAP.
- Using the grading levels established and approved above, select and implement the applicable software QA work activities from the following list to ensure that safety software performs its intended functions. ASME NQA-1-2000, Quality Assurance Requirements for Nuclear Facility Applications, or other national or international consensus standards that provide an equivalent level of quality assurance requirements as NQA-1-2000, must be used to implement these work activities. The standards used must be specified by the user and approved by DOE.

DOE G 414.1-4 provides acceptable implementation standards for the following work processes, which are listed in requirement 5.d of attachment 2 to DOE O 414.1C:

- Software project management and quality planning
- Software risk management
- Software configuration management
- Procurement and supplier management
- Software requirements identification and management
- Software design and implementation
- Software safety
- Verification and validation
- Problem reporting and corrective action
- Training of personnel in the design, development, use, and evaluation of safety software

b. Explain how a safety analysis problem being addressed by software is translated into functional requirements, how these requirements are established and controlled, and how the code is reconciled with the original safety analysis problem.

The following is taken from DOE G 200.1-1.

Functional requirements define what the software product must do to support the system owner's business functions and objectives. The functional requirements should answer the following questions:

- How are inputs transformed into outputs?
- Who initiates and receives specific information?
- What information must be available for each function to be performed?

Identify requirements for all functions whether they are to be automated or manual. Describe the automated and manual inputs, processing, outputs, and conditions for all functions. Include a description of the standard data tables and data or records that will be shared with other applications. Identify the forms, reports, source documents, and inputs/outputs that the software product will process or produce to help define the functional requirements.

A functional model should be developed to depict each process that needs to be included. The goal of the functional model is to represent a complete top-down picture of the software product.

Flow diagrams should be used to provide a hierarchical and sequential view of the system owner's business functions and the flow of information through the processes.

c. Discuss the DOE toolbox codes (reference http://www.hss.energy.gov/CSA/CSP/sqa/central_registry.htm), their strengths, weaknesses, and other factors governing their appropriate use and the applicable DOE standards and guides for modeling their phenomena.

Areal Locations of Hazardous Atmospheres (ALOHA)

ALOHA is an atmospheric dispersion model maintained by the Hazardous Materials Division of the National Oceanic and Atmospheric Administration. ALOHA is one of three separate, integrated software applications in the Computer-Aided Management of Emergency Operations suite.

ALOHA is used primarily for the evaluations of the consequences of atmospheric releases of chemical species. In addition to safety analysis applications in the DOE complex, ALOHA is applied for emergency response situations and for training. ALOHA allows the user to estimate the downwind dispersion of a chemical cloud based on the toxicological/physical characteristics of the released chemical, atmospheric conditions, and specific circumstances of the release. Graphical outputs include a "cloud footprint" that can be plotted on maps with MARPLOT (Mapping Applications for Response, Planning, and Local Operational Tasks) to display the location of other facilities storing hazardous materials and vulnerable locations.

In May 2004, the DOE performed an evaluation of ALOHA against DOE's safety SQA criteria. A gap analysis report was generated that identifies the strengths and weaknesses based upon ASME NQA-1 criteria. The results of that evaluation are available at DOE-EH-4.2.1.3-ALOHA-Gap Analysis, *Software Quality Assurance Improvement Plan: ALOHA Gap Analysis*, http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/ALOHA/Final_ALOHA_Gap_Analysis_Report050304.pdf.

Consolidated Model of Fire and Smoke Transport (CFAST)

CFAST is a computer program that fire investigators, safety officials, engineers, architects, and builders can use to simulate the impact of past or potential fires and smoke in a specific building environment. CFAST is a two-zone fire model used to predict the environment in a

multi-compartment structure subjected to a fire. It calculates the time evolving distribution of smoke and fire gases and the temperature throughout a building during a user-specified fire.

DOE and NIST have entered into an interagency agreement to enhance CFAST based on the DOE 2004 evaluation and gap analysis. The results of the gap analysis are available at DOE-EH-4.2.1.3-CFAST-Gap Analysis, *Software Quality Assurance Improvement Plan: CFAST Gap Analysis,* *http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/CFAST/Final_CFAST_Gap_Analysis_Report050304.pdf*.

Emergency Prediction Information Code (EPIcode)

The EPIcode program was developed to provide emergency response personnel and emergency planners with a software tool to help evaluate the atmospheric release of toxic substances. EPIcode allows fast estimation and assessment of chemical release scenarios associated with accidents from industry and transportation. The software can also be used for safety analysis planning purposes for facilities handling toxic materials. EPIcode performs calculations for chemical source terms and resulting downwind concentrations. Source term calculations determine the rate at which the chemical material is released to the atmosphere, release height, release durations, and the form and properties of the chemical upon release. The release chemical may be a gas, a vapor, or an aerosol.

In May 2004, the DOE performed an evaluation of EPIcode against DOE's safety SQA criteria. A gap analysis report was generated that identifies the strengths and weaknesses based upon ASME NQA-1 criteria. The results of that evaluation are available at DOE-EH-4.2.1.3-EPIcode-Gap Analysis, *Software Quality Assurance Improvement Plan: EPIcode Gap Analysis,* http://www.hss.energy.gov/csa/csp/sqa/central_registry/EPICode/Final_EPICode_Gap_Analysis_Report050304.pdf.

GENII

GENII is a second generation of environmental dosimetry computer code compiled in the Hanford environmental dosimetry system (Generation II). GENII provides a state-of-the-art, technically peer reviewed, documented set of programs for calculating radiation dose and risk from radionuclides released into the environment. The GENII system includes capabilities for calculating radiation doses following postulated chronic and acute releases.

The GENII gap analysis was performed to determine the actions needed to bring the code into compliance with SQA criteria. The results of that analysis are available at DOE-EH-4.2.1.3-GENII-Gap Analysis, *Software Quality Assurance Improvement Plan: GENII Gap Analysis*, http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/Genii/Final_GENll_Gap_Analysis_Report050304.pdf.

Integrated Modules for Bioassay (IMBA)

IMBA Expert™ (IX) software suite comprises a series of independent modules (referred to as sub-modules) that implement the ICRP Publication 66, *Human Respiratory Tract Model,* and the ICRP Publications 30 (series), 67 through 69, and 71 biokinetic models.

In July 2006, the DOE completed an evaluation of IMBA Expert™ and IMBA Professional Plus. A gap analysis report was generated that identifies the strengths and weaknesses based on DOE O 414.1C and DOE G 414.1-4 safety software requirements and criteria. The results of that evaluation are available at DOE/EH-0711, *Gap Analysis for IMBA and DOE Safety Software Central Registry Recommendation,* http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/IMBA/IMBAGapAnalysisFinal20060831.pdf.

The MELCOR Accident Consequence Code Systems (MACCS)

The MACCS code, developed originally for the NRC, and its successor code, MACCS2, are based on the straight-line Gaussian plume model. MACCS2 evaluates doses and health risks from the accidental atmospheric releases of radionuclides. The principal phenomena considered in MACCS2 are atmospheric transport and deposition under time-variant meteorology, short-term and long-term mitigative actions and exposure pathways, deterministic and stochastic health effects, and economic costs.

In May 2004, DOE Office of Quality Assurance Programs (EH-31) performed an evaluation of MACCS2 against DOE's safety SQA criteria. The results of that evaluation are available at DOE-EH-4.2.1.3-MACCS2-Gap Analysis, *Software Quality Assurance Improvement Plan: MACCS2 Gap Analysis,* http://www.hss.energy.gov/csa/csp/sqa/central_registry/MACCS2/Final_MACCS2_Gap_Analysis_Report050304.pdf.

Methods for Estimation of Leakages and Consequences of Releases (MELCOR)

MELCOR is a fully integrated, engineering-level computer code whose primary purpose is to model the progression of accidents in light-water reactor nuclear power plants. Major uses of MELCOR for nonreactor facilities include estimation of confinement behavior due to radiological source terms under postulated accident conditions (and their sensitivities and uncertainties in a variety of applications), evaluation of leak path factors (LPFs), and survivability of fans, filters, and other engineering safety features.

The MELCOR gap analysis was performed to determine the actions needed to bring the code into compliance with SQA criteria. The results of that analysis are available at DOE-EH-4.2.1.3-MELCOR-Gap Analysis, *Software Quality Assurance Improvement Plan: MELCOR Gap Analysis,* http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/MELCOR/Final_MELCOR_Gap_Analysis_Report050304.pdf.

23. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the following criticality safety-related American National Standards Institute/American Nuclear Society (ANSI/ANS) standards:

- **ANSI/ANS-8.1, Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors**
- **ANS-8.3 (ANSI N-16.2), Criticality Accident Alarm System**
- **ANS-8.5 (ANSI N-16.4), Use of Borosilicate-Glass Raschig Rings as a Neutron Absorber in Solutions of Fissile Material**
- **ANSI/ANS-8.7, Guide for Nuclear Criticality Safety in the Storage of Fissile Materials**
- **ANS-8.15, Nuclear Criticality Control of Special Actinide Elements**
- **ANS-8.19, Administrative Practices for Nuclear Criticality Safety**

a. Describe the contents, requirements, and relationship among the above ANSI/ANS standards.

ANSI/ANS-8.1, Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors

ANSI/ANS-8.1 is applicable to operations with fissionable materials outside nuclear reactors, except for the assembly of these materials under controlled conditions, such as in critical experiments. Generalized basic criteria are presented, and limits are specified for some single fissionable units of simple shape containing U-233, U-235, or Pu-239, but not for multiunit arrays. Requirements are stated for establishing the validity and areas of applicability of any calculation method used in assessing nuclear criticality safety. This standard does not include the details of administrative controls, the design of processes or equipment, the description of instrumentation for process control, or detailed criteria to be met in transporting fissionable materials.

ANS 8.3 (ANSI N-16.2), Criticality Accident Alarm System

ANS 8.3 is applicable to all operations involving fissionable materials in which inadvertent criticality can occur and cause personnel to receive unacceptable exposure to radiation. This standard is not applicable to detection of criticality events where no excessive exposure to personnel is credible, nor to nuclear reactors or critical experiments. This standard does not include details of administrative actions or of emergency response actions that occur after alarm activation.

ANS 8.5(ANSI N-16.4), Use of Borosilicate-Glass Raschig Rings as a Neutron Absorber in Solutions of Fissile Material

This standard provides guidance for the use of borosilicate-glass Raschig rings as a neutron absorber for criticality control in ring-packed vessels containing solutions of U-233, U-235, or Pu-239. The chemical and physical environment, properties of the rings and packed vessels, maintenance inspection procedures, and operating guidelines are specified.

ANSI/ANS-8.7, Guide for Nuclear Criticality Safety in the Storage of Fissile Materials

Note: ANSI/ANS-8.7 was withdrawn in 1997.

ANSI/ANS-8.7 is applicable to the storage of fissile materials. Mass and spacing limits are tabulated for uranium containing greater than 30 weight percent U-235, for U-233, and for plutonium as metals and oxides. Criteria for the range of application of these limits are provided.

ANS 8-15, Nuclear Criticality Control of Special Actinide Elements

ANSI/ANS 8.1 provides guidance for the nuclides U-233, U-235, and Pu-239. These three nuclides are of primary interest in out-of-reactor criticality safety since they are the most commonly encountered in the vast majority of operations. However, some operations can involve nuclides other than U-233, U-235, and Pu-239 in sufficient quantities that their effect on criticality safety could be of concern. ANS 8-15 provides guidance for fifteen such nuclides.

ANS 8-19, Administrative Practices for Nuclear Criticality Safety

ANS 8-19 provides criteria for the administration of a nuclear CSP for outside-of-reactor operations in which there exists a potential for nuclear criticality accidents. Responsibilities of management, supervision, and the nuclear criticality safety staff are addressed. Objectives and characteristics of operating and emergency procedures are included.

b. Discuss the applicability of the above ANSI/ANS standards to the Department's facilities and processes.

Chapter III of DOE O 420.1B, ties in the ANSI/ANS and ANS standards to the development and implementation of a CSP. Chapter III is applicable to nuclear facilities with activities that involve nuclides in quantities that are greater than or equal to the single parameter limits for fissionable materials involving ANSI/ANS-8.1 and 8.15. This means that any facility or activity involving or potentially involving amounts of fissionable material in excess of these limits has, by definition, a fissionable material operation.

CSPs must satisfy the requirements of the revisions to consensus nuclear criticality safety standards of ANSI/ANS 8 in effect as of the date of DOE O 420.1B, unless otherwise modified or approved by DOE. All recommendations in applicable ANSI/ANS standards must be considered, with an explanation to DOE given through the CSP description document for those recommendations that are not implemented. Furthermore, the double contingency principle defined in ANSI/ANS 8.1 is a requirement that must be implemented for all processes, operations, and facility designs within the scope of chapter III of DOE O 420.1B, unless the deviation is documented, justified, and approved by DOE.

c. Discuss the role of the Department's NSSs in implementing the requirements of these standards.

The following is taken from DOE-STD-1183-2007.

NSS personnel are not necessarily criticality control and safety subject matter experts (SMEs). That is the function of the criticality safety engineer SME who has his or her own qualification program. NSSs interface with a variety of technical SMEs and managers to

oversee the implementation of nuclear safety requirements and programs through oversight of contractors' implementation of 10 CFR 830, subpart B ("Safety Basis Requirements") and related activities (e.g., ISM, safety-related QA [subpart A], Price-Anderson Amendments Act [PAAA] evaluations, design reviews, accident/incident investigations, emergency response activities, rules, policies, standards, guides, etc., development, review, and implementation).

d. Define the following terms associated with nuclear criticality safety:

- **Criticality incident**
- **Double contingency principle**
- **Geometry control**
- **Nuclear criticality safety**
- **Significant quantity of fissionable material**
- **Temporary exemption**

Criticality Incident

According to DOE G 420.1-1, a nuclear criticality safety incident is a change in process condition or a loss of control beyond the evaluated process variances of the nuclear criticality safety analysis.

Double Contingency Principle

Per DOE O 420.1B, process designs shall incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible. This requires the control of at least two independent process parameters. This approach is consistent with the double contingency principle as stated in ANSI/ANS-8.1 and is the approach preferred by DOE to be taken to prevent common-mode failure. The double contingency principle defined in ANSI/ANS 8.1 is a requirement that must be implemented for all processes, operations, and facility designs unless the deviation is documented, justified, and approved by DOE.

Geometry Control

Per ANSI/ANS 8.1, where practicable, reliance should be placed on equipment design in which dimensions are limited rather than on administrative controls. Full advantage may be taken of any nuclear characteristics of the process materials and equipment. All dimensions and nuclear properties on which reliance is placed shall be verified prior to the beginning of operations, and controls shall be exercised to maintain them.

Nuclear Criticality Safety

Per DOE G 421.1-1 and ANSI/ANS 8.1, nuclear criticality safety means protecting against the consequences of an inadvertent nuclear fission chain reaction, preferably by preventing the reaction.

Significant Quantity of Fissionable Material

DOE G 421.1-1 defines significant quantity of fissionable material as the minimum quantity of fissionable material for which control is required to maintain sub-criticality under all normal and credible abnormal conditions.

Temporary Exemption

According to DOE Order 5480.30, review and concurrence by Headquarters-level offices are required for permanent exemptions. Program Secretarial Officers (PSOs) may grant temporary exemptions with notification of appropriate Headquarters-level offices. Temporary exemptions may be granted for durations up to 1 year, while permanent exemptions apply for the life of a facility.

e. *Discuss the contractor's responsibilities for the following in relation to criticality safety activities:
- **Criticality safety evaluations**
- **Monitoring**
- **Surveillance**
- **Transportation**
- **Storage**

[*Note: In the FAQS, competency 23 has two KSAs identified as d.]

Criticality Safety Evaluations

Chapter III of the contractor requirements document in DOE O 420.1B requires that the contractor develop and implement a CSP that includes criticality safety evaluations (CSEs) for fissionable materials operations that document parameters, limits, and controls required to maintain sub-criticality for all normal and credible abnormal conditions. Provisions for implementing limits and controls must also be identified in the CSE.

The methodology for conducting CSEs must be approved by DOE, unless the evaluations are conducted in accordance with the DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*, or successor document and evaluated in accordance with DOE-STD-1134-1999, *Review Guide for Criticality Safety Evaluations*, or successor document.

Monitoring

Chapter III of the contractor requirements document in DOE O 420.1B requires that CSPs include periodic reviews of operations and conditions to ensure that (1) limits and controls are implemented effectively and (2) process conditions have not been altered, thus resulting in the compromise of safety limits and controls. Furthermore, section 3.b.(6) requires that facilities that conduct operations using fissionable material in a form that could inadvertently accumulate in significant quantities include a program and procedures for detecting and characterizing accumulations.

Surveillance

Section 5.5 of DOE-STD-1158-2002 discusses maintaining compliance with requirements. The contractor must establish and implement appropriate surveillance frequencies or engineered controls relied upon for criticality safety to ensure that the controls are performing their intended function.

Transportation

According to DOE-STD-1135-99, nuclear criticality safety evaluations are performed to demonstrate technically the sub-criticality of fissionable material processes, operations, and situation for transportation and storage under all normal and credible abnormal conditions. In other words, control of fissile parameters must be maintained for all activities, including transportation and storage.

Storage

Storage provisions must control physical parameters to maintain nuclear criticality safety. The contractor is required to develop and maintain fissile material storage areas in conformance with the requirements of ANSI/ANS 8.7, *Guide for Nuclear Criticality Safety in the Storage of Fissile Materials*.

24. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the following DOE Orders, technical standards, and Guides:

- **DOE-STD-3011-2002, Guidance for Preparation of Basis for Interim Operation (BIO) Documents**
- **DOE-STD-3014-96*, Accident Analysis for Aircraft Crash into Hazardous Facilities**
- **DOE-STD-1120-2005, Integration of Environment, Safety, and Health into Facility Dispositions Activities**
- **US NRC Guide 1.70, Standard Format and Content of Safety Analysis Reports of Nuclear Power Plants**
- **29 CFR 1910.120, Safety and Health Programs, Work Plans, Health and Safety Plan**
- **DOE-STD-1163-2003**, Integration of Multiple Hazard Analysis Requirements and Activities**
- **DOE-NA-STD-3016-2006, Hazard Analysis Reports for Nuclear Explosive Operations**
- **DOE O 460.1B, Packaging and Transportation Safety**
- **DOE G 460.1-1, Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety**
- **DOE O 461.1A, Packaging and Transfer or Transportation of Materials of National Security Interest**
- **DOE M 461.1-1 CHG 1, Packaging and Transfer of Materials of National Security Interest Manual**
- **Secretary of Energy Notice (SEN) SEN-35-91, Nuclear Safety Policy**

[Notes: *DOE-STD-3014-96 has been superseded by DOE-STD-3014-2006. **Presumably DOE-HDBK-1163-2003 is meant instead of DOE-STD-1163-2003.]

a. Describe the contents and requirements of and relationship among the above technical standards.

It is DOE policy that the general public be protected such that no individual bears significant additional risk to health and safety from the operation of a DOE nuclear facility above the risks to which members of the general population are normally exposed. The purpose of the

documents listed in this competency is to establish the basic nuclear safety policy from which specific safety rules, Orders, standards, and other requirements shall follow. DOE facilities will be designed, constructed, operated, and decommissioned to assure the protection of the public, workers, and the environment. Adherence to appropriate national and international standards in the design, construction, operation, and decommissioning of DOE's nuclear facilities and activities is necessary for the successful implementation of the Department's nuclear safety policy. Standards proven through years of experience and accepted by professional and technical societies shall be used wherever applicable.

DOE-STD-3011-2002, Guidance for Preparation of Basis for Interim Operation (BIO) Documents

DOE-STD-3011-2002 provides guidance for the development of a BIO document, which is an acceptable form of a DSA under the provisions of 10 CFR 830, subpart B, for a DOE nuclear facility with a limited operational life, the deactivation of a DOE nuclear facility, or the transition surveillance and maintenance of a DOE nuclear facility.

DOE-STD-3014-96, Accident Analysis for Aircraft Crash into Hazardous Facilities

DOE-STD-3014-96 has been superseded by DOE-STD-3014-2006.

DOE-STD-3014-2006 provides the user with sufficient information to evaluate and assess the significance of aircraft crash risk on facility safety without expending excessive effort where it is not required. It establishes an approach for performing a conservative analysis of the risk posed by a release of hazardous radioactive or chemical material resulting from an aircraft crash into a facility containing significant quantities of such material. This approach can establish whether a facility has a significant potential for an aircraft impact, and, given an aircraft impact, whether a facility has the potential for an accident producing significant offsite or onsite consequences. The analysis is based on the structural properties of a facility and the inventory at a facility.

DOE-STD-1120-2005, Integration of Environment, Safety, and Health into Facility Dispositions Activities

DOE-STD-1120-2005 provides a DOE-approved methodology for preparing a DSA for decommissioning nuclear facilities, as well as environmental restoration activities that involve work not done within a permanent structure.

U.S. NRC Guide 1.70, Standard Format and Content of Safety Analysis Reports of Nuclear Power Plants

U.S. NRC Guide 1.70 provides a standard format for safety analysis reports considered acceptable to the NRC for nuclear reactor facilities. It is identified as a safe harbor method in 10 CFR 830 for the safety basis documentation requirements for a DOE reactor.

29 CFR 1910.120, *Safety and Health Programs, Work Plans, Health and Safety Plan*

29 CFR 1910.120 is identified in 10 CFR 830 as an element of a safe harbor method for developing safety basis documentation for either the decommissioning of a DOE nuclear facility or a DOE environmental restoration activity that involves either work not done within

a permanent structure or the decommissioning of a facility with only low-level residual fixed radioactivity. The provisions in 29 CFR 1910.120 are to be used for developing a safety and health program, work plans, health and safety plans, and emergency response plans.

DOE-HDBK-1163-2003, Integration of Multiple Hazard Analysis Requirements and Activities

DOE-HDBK-1163-2003 is intended to provide DOE and contractor safety personnel with a resource to support the planning, technical review, or conduct of hazard analysis activities. Clarifications of requirements and discussions of best practices can be used to help improve cost effectiveness, clarify organizational roles and responsibilities, and provide a basis for enhancing the technical quality of hazard analysis activities. The concepts presented in the handbook are supportive of ISMS and can be applied to nuclear or hazardous non-nuclear facilities that are operating, shutdown, or actively conducting facility disposition activities.

DOE-NA-STD-3016-2006, Hazard Analysis Reports for Nuclear Explosive Operations

DOE-NA-STD-3016-2006 applies to the conduct of hazard analyses and preparation of HARs for nuclear explosive operations conducted by the DOE. This standard addresses operation-specific HARs and their interface with facility safety basis documents.

DOE O 460.1B, Packaging and Transportation Safety

DOE O 460.1B establishes safety requirements for the proper packaging and transportation of DOE/NNSA offsite shipments and onsite transfers of hazardous materials and for modal transport. Offsite is any area within or outside a DOE site to which the public has free and uncontrolled access; onsite is any area within the boundaries of a DOE site or facility to which access is controlled. Excluded from the requirements of the Order are classified shipments; shipments of nuclear explosives, components, and special assemblies; and facilities and activities of the Naval Nuclear Propulsion Program.

DOE G 460.1-1, *Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety*

DOE G 460.1-1 supplements DOE O 460.1B by providing clarifying information for the implementation of packaging and transportation safety of hazardous materials.

DOE O 461.1A, Packaging and Transfer or Transportation of Materials of National Security Interest

DOE O 461.1A establishes requirements and responsibilities for offsite shipments of naval nuclear fuel elements, category I and category II special nuclear material (SNM), nuclear explosives, nuclear components, special assemblies, and other materials of national security interest; onsite transfers of naval nuclear fuel elements; and certification of packages for category I and II SNM, nuclear components, and other materials of national security interest.

DOE M 461.1-1 Chg 1, Packaging and Transfer of Materials of National Security Interest Manual

All DOE facilities are required to develop and implement an onsite packaging and transfer procedure detailing both the means by which those facilities will comply with the

requirements of DOE O 461.1A, which governs transfer and transportation of specific materials, and the packaging or container used to minimize the risk of release of those materials to the public, the worker, and the environment. DOE M 461.1-1 also provides mandatory and appropriate site-specific approval processes for technical safety requirements and policy objectives for development of an onsite packaging and transfer program, which each contractor must document in its onsite packaging and transfer procedures. This manual, when implemented, satisfies the requirements of 10 CFR 830, subpart B, for all DOE nuclear facilities.

Secretary of Energy Notice (SEN) SEN-35-91, Nuclear Safety Policy

The purpose of SEN-35-91 is to establish the basic nuclear safety policy from which specific safety rules, Orders, standards, and other requirements shall follow. DOE facilities will be designed, constructed, operated, and decommissioned to assure the protection of the public, workers, and the environment. To implement this policy, DOE and its contractors shall (1) establish and maintain management involvement and accountability to ensure that nuclear safety requirements are met and individual responsibility is articulated and understood by all parties; (2) develop and foster technically competent personnel and the technical standards necessary to achieve nuclear safety; (3) use established nuclear safety goals to serve as aiming points for performance; (4) establish and maintain vigorous oversight to assure adherence to this policy and its implementing directives; and (5) promote a culture that is dedicated to continuously striving to enhance nuclear safety.

b. Describe the role of NSSs with respect to the requirements in these Orders and standards.

DOE-STD-1183-2007 states that the duties and responsibilities of NSSs are to oversee the implementation of nuclear safety requirements and programs. The "Nuclear Safety Management Rule," 10 CFR 830, governs the conduct of DOE contractors, DOE personnel, and other persons conducting activities (including providing items and services) that affect or may affect the safety of DOE nuclear facilities. NSSs participate in the oversight of contractor implementation of 10 CFR 830. The nuclear safety specialist ensures that all safety considerations taken are adequate to meet DOE goals.

c. Describe the application of DOE-STD-3011, Guidance for Preparation of Basis for Interim Operations (BIO) Documents, to nuclear facilities safety basis.

Appendix A of 10 CFR 830, subpart B, states that the contractor responsible for (1) a DOE nuclear facility with a limited operational life, (2) the deactivation of a DOE nuclear facility, or (3) the transition surveillance and maintenance of a DOE nuclear facility may prepare its DSA using the methodology in DOE-STD-3011-2002. A BIO under 10 CFR 830 must fully satisfy the requirement of 10 CFR 830.202 and 204. Specifically, the BIO must include

- facility categorization according to DOE-STD-1027-92;
- a description of the facility (including the work to be performed);
- a systematic identification of hazards associated with the facility;
- evaluation of normal, abnormal, and accident conditions (including potential natural phenomenon hazards that might be associated with long-term status) that might be

associated with the generation or release of radioactive or other hazardous materials, including consideration of the need for analysis of beyond-design-basis accidents;
- derivation and classification of hazard controls necessary to protect workers, the public, and the environment;
- definition of the characteristics of safety management programs, necessary to ensure safe operation, including criticality safety, when criticality hazards exist.

In the context of DOE-STD-3011-2002, a limited operational life or transition facility is interpreted to be interim operations, since the expected normal lifetime for these activities is ideally anticipated to be the short (i.e., less than 5 years for limited operational life) interim transitional periods immediately prior to, during, or after deactivation. While this standard allows for an abbreviated and graded approach to development of a safety basis, the expectation exists that the completeness of the analysis will be sufficient so that even though a limited operational life is envisioned, significant hazards will be identified and appropriate controls implemented accordingly. It is also important to recognize and anticipate that the ideal may not be realized. That is, especially in the case of transition surveillance and maintenance, the time interval that a facility may be in that mode may extend many years beyond "short." When this may be the case, special attention must be paid to hazards that may develop over the extended period of time.

The contractor must also develop a TSR document as part of the safety basis to satisfy the requirements of 10 CFR 830.205.

DOE G 421.1-2 defines a limited life facility as a facility with an approved deactivation plan calling for cessation of operation within a stated period (5 years or less). The primary rationale for utilizing the BIO approach is that the short remaining operational life of the facility does not justify the increased time and cost required to develop a DSA fully utilizing the DOE-STD-3009-94 methodology.

Maximum advantage should be taken of pertinent existing safety analyses and design information (i.e., requirements and their bases) that are immediately available, or can be retrieved through reasonable efforts. Other information arises from existing sources such as process hazards analyses, fire hazards analyses, explosive safety analyses, HASPs, environmental impact statements, etc. If this information does not exist or must be supplemented, it should be created or supplemented in a manner that is consistent with the limited lifetime expectancy of the facility, so time-consuming approaches should be avoided whenever possible. Analyses should generally be qualitative, but thorough. When adequate information is not available to fully support the DSA, conservative compensatory approaches to assuring adequate safety should be considered.

Deactivation refers to the process of placing the facility in a stable and known condition and the removal of readily removable hazardous and radioactive materials. Deactivation activities include the removal of energy sources, draining and/or de-energizing nonessential systems, removal of stored radioactive and hazardous materials, and related actions. Deactivation should be a short-term process, measured in months, or at most a very few years. The

mission is to remove hazardous material to decrease risk during extended surveillance and maintenance or decontamination and decommissioning.

Transition surveillance and maintenance means activities conducted when a facility is not operating and not during deactivation, decontamination, and decommissioning activities. Ideally, deactivation would precede transition surveillance and maintenance, but often it does not. During this phase, surveillance and maintenance are the primary activities being conducted at the facility. These activities are necessary for satisfactory containment of hazardous materials and protection of workers, the public, and the environment. Surveillance and maintenance activities include providing periodic inspections and maintenance of structures, systems, and equipment necessary for the satisfactory containment of contamination and for protection of workers, the public, and the environment. Maintenance of the facility in a stable and known condition includes actions to prevent the alteration in chemical makeup, physical state, and/or configuration of a hazardous substance or radioactive material.

d. Determine whether aircraft crashes pose an acceptable or unacceptable hazard to safety of nuclear facilities.

DOE-STD-3014-2006 provides methodologies that take into consideration items determined to be important to understanding the risk from aircraft crash into hazardous facilities. These items include number of aircraft operations/flights; crash probabilities; aircraft characteristics; crash kinematics; impacting missiles; local, global, and vibratory structural damage; structure characteristics; source terms; release energy; and meteorological conditions. When applied as a complete approach, the methodologies in this standard will result in a technically justified, conservative analysis of the risk posed by releases resulting from aircraft crash. The risk will be defined at a sufficient level of detail to document the safety of the facility with respect to aircraft crash, and at the same level of detail as would be expected for other types of accident analyses.

The standard allows the analysis to proceed along a series of increasingly complex steps: the results at each step are used to determine whether it is necessary to proceed to the next step or whether sufficient information has been provided and the analysis can be stopped and documented. As one proceeds through the steps, the results will get closer to an actual estimate of the risk, but even after fully implementing this standard, the results will still be more conservative than would be expected from a best-estimate risk assessment. In summary, following this standard will, in the vast majority of cases, provide sufficient information to document facility safety and support sound decision making for addressing the effects of an aircraft crash in the context of facility safety. This is not a criterion-based standard. It does not provide any hard-and-fast rules prescribing the actions that should be taken in response to the results; it does not even prescribe whether any action should be considered. It does provide quantitative guidelines against which the results for each step in the analysis can be measured; however, these are only for the purpose of determining whether further analysis should be performed. Meeting or not meeting these guidelines should not be interpreted as indicating that preventive or mitigative actions either are or are not required.

e. Discuss the phenomena of aircraft crashes as a mechanism for releasing toxic materials.

The following is taken from DOE-STD-3014-2006.

First, the results of the structural analysis are used to describe the level of damage. This description will provide a conservative estimate of the structural damage that has occurred, including the path and location of penetrators; the damage state of walls, barriers, and equipment; the location of the aircraft fuel; and other pertinent information.

Assume that all available fuel burns, as well as any other combustibles that are in the path of the penetrators. Assume also that any high explosive material undergoes a high explosive violent reaction. High explosive material includes materials such as TNT, ion exchange resins, etc., but not highly flammable materials that are subject to burning rather than true explosion (e.g., aircraft fuel, hydrogen gas). This assumption only pertains to combustibles and explosives that are directly affected by the penetrators; that is, they are in areas or compartments that are actually breached by the penetrators.

Evaluate the extent to which secondary effects cause the scenario to spread beyond the area directly damaged by the crash. Consider if there is sufficient combustible material to breach additional barriers and spread further through the facility. Credit can be taken for the existence of fire barriers and breaks if they haven't been damaged by the crash. A characterization of fire duration will almost certainly be required. Credit should not be allowed for functioning fire suppression systems unless an analysis can demonstrate they will remain effective following the crash. An evaluation should include a determination of whether the force of any explosion is capable of causing further barriers to be damaged or destroyed or has the potential to cause additional fires and/or explosions in the facility. Again, credit can be taken for the dissipation of explosive energy by existing barriers, if they have not been damaged by the crash. Credit can also be taken for diversion of the explosive force through breaches caused by the crash, thus reducing the shock to intact barriers.

Based on the prior steps, determine if any of the MAR in the facility can be impacted by a release mechanism (e.g., shock, fire, or explosion) as a result of the scenario. This is likely if there is any material that is not separated from the energy available from the release mechanism by an intact barrier capable of dissipating that energy. Consideration should also be given to the potential for the primary confinement around any of the material to be breached, which can occur if the structural integrity of the primary confinement is degraded below that required under accident conditions and if there is a driving force capable of causing the material to migrate through the breach. Finally, the potential for a direct release to the atmosphere should be determined. This is likely to be the case if there are no intact barriers between the material and the atmosphere, assuming that the primary confinement has failed and there is a driving force capable of causing the material to migrate through the release path.

f. Discuss the application of DOE-STD-1120 and 29 CFR 1910.120 to decommissioning and certain environmental restoration activities, and discuss the content of a safety basis Health and Safety Plan and how it can be used in a dynamic project, including management of hazard controls.

DOE-STD-1120 is identified as a "safe harbor" approach for preparing a DSA for decommissioning and environmental restoration activities. Volume 1 of the standard provides a DOE-approved methodology for preparing a DSA for decommissioning of nuclear facilities, as well as environmental restoration activities that involve work not done within a permanent structure. Contractors may prepare a DSA by using the method described in DOE-STD-1120-2005 and the provisions of 29 CFR 1910.120 or 29 CFR 1926.65, "Hazardous Waste Operations and Emergency Response" (HAZWOPER). HAZWOPER requirements specifically focus on provisions for developing a safety and health program and site-specific health and safety plan. HAZWOPER applies to all worker hazards, including physical hazards posed by deconstruction or environmental restoration work. In the context of subpart B of 10 CFR 830, the scope of HAZWOPER is taken to include those hazards, associated controls, and safety and health programs that must be identified and maintained within a hazard category 1, 2, or 3 facility's safety basis.

Volume 1 of the standard applies to hazard category 2 or 3 environmental restoration activities and decommissioning projects as defined in 10 CFR 830, subpart B. 29 CFR 1910.120 applies to general worker safety by providing requirements to ensure worker health and safety during emergency response for hazardous waste operations, including projects conducted under the Comprehensive Environmental Response, Compensation, and Liability Act. It also provides requirements to ensure worker health and safety during emergency release of hazardous substances wherever they occur. HAZWOPER requires a safety and health program and site-specific safety and health plan for cleanup operations involving hazardous substances; operations involving hazardous wastes conducted at treatment, storage, and disposal facilities; and emergency response operations for releases of, or substantial threats of release of, hazardous substances. Derivation of controls is also necessary for facility decommissioning projects that involve more than "low-level residual fixed radioactivity."

Decommissioning projects that have only low-level residual fixed radioactivity are not expected to have the potential for accidents involving significant radiological consequences. This is reflected in 10 CFR 830.205(c), which states that TSRs are not required for this type of activity. The DSA format for this type of decommissioning activity may exclude topics related to accident analysis, safety SSCs, and TSR derivation.

g. Discuss the phenomena to which packaging is designed to withstand transportation accidents and the relationship to accident severity.

The following is taken from 10 CFR 71.71, "Normal Conditions of Transport."

Evaluation of each package design under normal conditions of transport must include a determination of the effect on that design of the conditions and tests specified in the

following paragraphs. Separate specimens may be used for the free drop test, the compression test, and the penetration test, if each specimen is subjected to the water spray test before being subjected to any of the other tests.

With respect to the initial conditions for these tests, the demonstration of compliance with the requirements of 10 CFR 71.71 must be based on the ambient temperature preceding and following the tests remaining constant at that value between -29 °C (-20 °F) and +38 °C (+100 °F) which is most unfavorable for the feature under consideration. The initial internal pressure within the containment system must be considered to be the maximum normal operating pressure, unless a lower internal pressure consistent with the ambient temperature considered to precede and follow the tests is more unfavorable.

Conditions and Tests

Heat. Packaging must withstand an ambient temperature of 38 °C (100 °F) in still air, and insolation according to table 6.

Table 6. Insolation data

Form and Location of Surface	**Total Insolation for a 12-Hour Period** (g cal/cm^2)
Flat surfaces transported horizontally	
Base	None
Other surfaces	800
Flat surfaces not transported horizontally	200
Curved surfaces	400

Source: 10 CFR 71.71

Cold. An ambient temperature of -40 °C (-40 °F) in still air and shade.

Reduced External Pressure. An external pressure of 25 kilopascals (kPa) (3.5 pound-force per square inch, or 3.5 lbf/in.^{2}) absolute.

Increased External Pressure. An external pressure of 140 kPa (20 lbf/in.^{2}) absolute.

Vibration. Vibration normally incident to transport.

Water Spray. A water spray that simulates exposure to rainfall of approximately 5 cm/h (2 in./h) for at least 1 hour.

Free Drop. Between 1.5 and 2.5 hours after the conclusion of the water spray test, a free drop through the distance specified in table 7 onto a flat, essentially unyielding, horizontal surface, striking the surface in a position for which maximum damage is expected.

Table 7. Criteria for free drop test (weight/distance)

Package Weight		Free Drop Distance	
Kilograms	**Pounds**	**Meters**	**Feet**
Less than 5,000	Less than 11,000	1.2	4
5,000–10,000	11,000–22,000	0.9	3
10,000–15,000	22,000–33,100	0.6	2
More than 15,000	More than 33,100	0.3	1

Source: 10 CFR 71.71

Corner Drop. A free drop onto each corner of the package in succession, or in the case of a cylindrical package onto each quarter of each rim, from a height of 0.3 m (1 ft) onto a flat, essentially unyielding, horizontal surface. This test applies only to fiberboard, wood, or fissile material rectangular packages not exceeding 50 kg (110 lb) and fiberboard, wood, or fissile material cylindrical packages not exceeding 100 kg (220 lb).

Compression. For packages weighing up to 5,000 kg (11,000 lb), the package must be subjected, for a period of 24 hours, to a compressive load applied uniformly to the top and bottom of the package in the position in which the package would normally be transported.

The compressive load must be the greater of the following:

- The equivalent of 5 times the weight of the package or
- The equivalent of 13 kPa (2 lbf/in.^{2}) multiplied by the vertically projected area of the package.

Penetration. Impact of the hemispherical end of a vertical steel cylinder of 3.2 cm (1.25 in.) diameter and 6 kg (13 lb) mass, dropped from a height of 1 m (40 in.) onto the exposed surface of the package that is expected to be most vulnerable to puncture. The long axis of the cylinder must be perpendicular to the package surface.

25. Nuclear safety specialists shall demonstrate a familiarity level knowledge of the Price-Anderson Amendments Act of 1988 and its relationship to Subparts A and B of 10 CFR 830.

The following is taken from DOE-HDBK-1085-95.

a. Describe the purpose of the Price-Anderson Amendment Act.

The purpose of the PAAA of 1988 is to promote protection of the environment, health, and safety of the public and workers. It indemnifies (insures) DOE contractors against public liability due to a nuclear incident. It establishes quality and nuclear safety requirements, and it provides DOE enforcement authority.

b. Discuss the general applicability to the Department's nuclear safety activities.

The PAAA provides indemnification to DOE contractors who manage and conduct nuclear activities in the DOE complex. In a general sense, the government acts as an insurer for these contractors against any findings of liability arising from the nuclear activities of the contractor within the scope of its contract.

In 1988, the PAAA was signed into law to extend the government insurance program that was about to expire. It differed from the original act in two principal ways. First, it made Price-Anderson coverage mandatory for all management and operating (M&O) contractors, subcontractors, and suppliers conducting nuclear activities for DOE. (For the purposes of the statute, "nuclear" includes "radiological.") Second, Congress mandated that DOE change its methods of managing nuclear activities at those sites by requiring DOE to undertake enforcement actions against indemnified contractors for violations of nuclear safety requirements. Thus, indemnification risks would be minimized by minimizing the risk to workers and the public. The benefit of indemnification is accompanied by the availability of sanctions to assure compliance with nuclear safety rules.

c. Describe the general indemnity that DOE offers to contractors.

For all M&O contractors, subcontractors, and suppliers thereto, DOE has the authority to issue notices of violation when noncompliances with nuclear safety requirements are identified. Additionally, for cases involving for-profit contractors, DOE has the authority to issue fines for violations of nuclear safety rules up to $100,000 per day per occurrence. Civil penalties are not applicable to individual employees or to contractors specifically exempted by section 234A (d) of the Atomic Energy Act (AEA) of 1954 (as amended).

d. Discuss the requirements associated with the topics below:

- **QA**
- **Safety basis**

Quality Assurance

Per 10 CFR 830, subpart A, contractors conducting activities, including providing items or services, that affect, or may affect, the nuclear safety of DOE nuclear facilities must conduct work in accordance with the QA criteria in 10 CFR 830.122. The intent of the PAAA is to provide incentives and enforcement policy to ensure all work under the scope of the act is accomplished with established quality and nuclear safety requirements set out in the contracts. These requirements include 10 CFR 830. The enforcement provisions of the Act are intended to ensure that contractors understand and implement nuclear safety

requirements, critically self-assess activities, promptly identify, report, and correct non-compliances, conduct work activities in compliance with applicable procedures, and assure the subcontractor's performance meets requirements.

Safety Basis

Per 10 CFR 830.201, subpart B, "a contractor must perform work in accordance with the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility and, in particular, with the hazard controls that ensure adequate protection of workers, the public, and the environment." The PAAA provides incentives and enforcement policy to ensure all work under the scope of the act is accomplished per 10 CFR 830, subpart B.

e. Discuss the role of the Department's NSSs with respect to implementing the requirements of the Price-Anderson Amendment Act.

The following is taken from 10 CFR 820 and DOE-STD-1183-2007.

The nuclear safety specialist ensures that all aspects of 10 CFR 830 are implemented at any given site. The nuclear safety specialist performs independent reviews and audits to determine that the contractor is implementing all aspects of the applicable Nuclear Safety Requirements. Per 10 CFR 820, appendix A, "the DOE goal in the compliance area [associated with the PAAA] is to enhance and protect the radiological health and safety of the public and worker at DOE facilities by fostering a culture among both the DOE line organizations and the contractors that actively seeks to attain and sustain compliance with DOE Nuclear Safety Requirements. A reasonable exercise of enforcement authority will be facilitated by the appropriate application of safety requirements to nuclear facilities and by promoting and coordinating the proper contractor and DOE safety compliance attitude toward these requirements." These goals and those of the nuclear safety specialist are consistent.

26. Nuclear safety specialists shall demonstrate a working level knowledge of the requirements in DOE technical standard DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis, and DOE-STD-3010-94, Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities.**

[Notes: *This is the title of DOE-STD-3009-94 as listed on the Approved DOE Technical Standards Web page; however, on the cover page the title is Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses. **Presumably DOE-HDBK-3010-94 is meant instead of DOE STD-3010-94.]

a. Discuss the conceptual basis and process for preparation of a facility/activity DSA.

The following is taken from DOE-STD-3009-94.

DOE-STD-3009-94 incorporates and integrates many different approaches regarding DSA format and content. To ensure a consistent application of this standard among users, the following guiding principles are provided:

- The focus of this standard is primarily on hazard category 2 and hazard category 3 facilities.

- Hazard analysis and accident analysis are merged into one chapter (chapter 3) to ensure that the proper emphasis is placed on identification and analysis of hazards. The hazard analysis distinguishes when accident analysis is required as a function of potential offsite consequence. Guidance for hazard and accident analysis is not based on PRA.

- Defense in depth, worker safety, and environmental issues are identified.

- Defense in depth, as discussed in this standard, consists of two components:
  1. Equipment and administrative features providing preventive or mitigative functions so that multiple features are relied on for prevention or mitigation to a degree proportional to the hazard potential, and
  2. Integrated safety management programs that control and discipline operation.

- Guidance is provided for evaluating the safety of a facility for which documentable, deterministic DBAs do not exist in order to establish bounding accidents (derivative DBAs) that envelope the safety of existing facilities. Guidance is also provided on the treatment of beyond DBAs.

- Distinction is made between "safety-class SSCs" and "safety-significant SSCs," and the balance of facility SSCs. Safety-class SSCs are related to public protection and are defined by comparison with the numerical EG. Safety-significant SSCs are identified for specific aspects of defense in depth and worker safety as determined by the hazard analysis.

- Guidance is provided identifying administrative controls that are major contributors to defense in depth, which are designated as specific administrative controls. This standard, along with DOE-STD-1186-2004, *Specific Administrative Controls*, provides guidance applicable to these types of controls. SACs provide preventive and/or mitigative functions for specific potential accident scenarios, which also have safety importance equivalent to engineered controls that would be classified as SC or SS if the engineered controls were available and selected.

- Consequences from normal operations are addressed in the radiation protection, hazardous material protection, and waste management chapters.

- Guidance is provided in each chapter on the application of the graded approach.

- A common DSA format (chapter, title, and organization) for all nonreactor nuclear facilities is desirable but not essential. A table is to be provided by the preparer that indicates where the DSA requirements of 10 CFR 830 are addressed. Content needs to be flexible to allow for different facility types, hazard categories, and other grading factors.

- Facility descriptive material is intentionally split to emphasize SSCs of major significance:
  - Chapter 2, "Facility Description," provides a brief, integrated overview of the facility SSCs.
  - Chapter 4, "Safety Structures, Systems, and Components," provides detailed information only for those SSCs that are SC and SS. This application of the graded approach will provide for a significant reduction of DSA volume, while maintaining a focus on safety.

- The programmatic chapters, including chapters 6–17, provide a summary description of the key features of the various safety programs as they related to the facility being analyzed. These chapters are not meant for the determination of the adequacy of these programs.

b. Discuss the following in relation to the preparation of the DSA:
- **Worker safety**
- **Defense-in-depth**
- **Programmatic commitments**
- **TSRs**
- **SSCs**
- **Hazard analysis**
- **Accident analysis**
- **Application of the graded approach**
- **Safe harbor methods**

The following is taken from DOE-STD-3009-94.

Worker Safety

Workers, typically those in close proximity to operations, are the population principally at risk from potential consequences associated with hazard category 2 and 3 facilities. The DOE recognizes, via 10 CFR 830, the importance of including worker safety in safety analyses by specifically noting the worker as a population of concern. Developing a conceptual basis for the methodology used in DOE-STD-3009-94 requires answering the fundamental question of how worker safety is most appropriately addressed in the DSA.

The Occupational Safety and Health Administration has published 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals." OSHA defines the purpose of this regulation in summary fashion as, "Employees have been and continue to be exposed to the hazards of toxicity, fires, and explosions from catastrophic releases of highly hazardous chemicals in their workplaces. The requirements in this standard are intended to

eliminate or mitigate the consequences of such releases." Many of the topics requiring coverage in this Federal regulation, such as design codes and standards, process hazard analysis, human factors, training, etc., are directly parallel to the requirements in 10 CFR 830.

DOE O 440.1B and 10 CFR 851 address the issue of worker safety from process accidents by requiring the performance of hazards analyses for processes (exclusive of standard industrial hazards) in conjunction with implementation of basic safety programs that discipline operations and ensure judgments made in hazard analyses are supported by actual operating conditions. These requirements effectively integrate programs and analyses into an overall safety management structure without requiring quantitative risk assessment. This integration and the basic concepts of process safety management (PSM) described by OSHA regulations and the manuals and codes of practice described in 10 CFR 851 and DOE O 440.1B are philosophically accepted as appropriate for DSAs. This standard effectively merges PSM principles with traditional DSA precepts.

Defense in Depth

Defense in depth as an approach to facility safety has extensive precedent in nuclear safety philosophy. It builds in layers of defense against release of hazardous materials so that no one layer by itself, no matter how good, is completely relied upon. To compensate for potential human and mechanical failures, defense in depth is based on several layers of protection with successive barriers to prevent the release of hazardous material to the environment. This approach includes protection of the barriers to avert damage to the plant and to the barriers themselves. It includes further measures to protect the public, workers, and the environment from harm in case these barriers are not fully effective.

The defense-in-depth philosophy is a fundamental approach to hazard control for nonreactor nuclear facilities even though they do not possess the catastrophic accident potential associated with nuclear power plants. In keeping with the graded-approach concept, no requirement to demonstrate a generic, minimum number of layers of defense-in-depth is imposed. However, defining defense in depth as it exists at a given facility is crucial for determining a safety basis. Operators of DOE facilities need to use the rigorous application of defense-in-depth thinking in their designs and operations. Such an approach is representative of industrial operations with an effective commitment to public and worker safety and the minimization of environmental releases.

For high hazard operations, there are typically multiple layers of defense-in-depth. The inner layer of defense in depth relies upon a high level of design quality so that important systems, structures, and components will perform their required functions with high reliability and high tolerance against degradation. The inner layer also relies on competent operating personnel who are well trained in operations and maintenance procedures. Competent personnel translate into fewer malfunctions, failures, or errors and, thus, minimize challenges to the next layer of defense.

In the event that the inner layer of defense in depth is compromised from either equipment malfunction (from whatever cause) or operator error and there is a progression from the normal to an abnormal range of operation, the next layer of defense in depth is relied upon.

Mitigation of the consequences of accidents is provided in the outer layer of defense in depth. Passive, automatically or manually activated features (e.g., containment or confinement system, deluge systems, filtered exhaust), and/or safety management programs (i.e., emergency response) minimize consequences in the event that all other layers have been breached. The contribution of emergency response actions to minimizing consequences of a given accident cannot be neglected as they represent a truly final measure of protection for releases that cannot be prevented.

Structures, systems, or components that are major contributors to defense in depth are designated as safety-significant SSCs. Additionally, the safety management programs (e.g., radiation protection, hazardous material protection, maintenance, procedures, training) that a facility must commit to in order to establish an adequate safety basis go beyond merely supporting the assumptions identified in the hazard analysis and are an integral part of defense in depth.

Administrative controls that are major contributors to defense in depth are designated as SACs that are required for safety because they are the basis for validity of the hazard or accident analyses, or they provide the main mechanisms for hazard control. This standard, along with DOE-STD-1186-2004, *Specific Administrative Controls*, provides guidance applicable to these types of controls. SACs provide preventive and/or mitigative functions for specific potential accident scenarios, which also have safety importance equivalent to engineered controls that would be classified as safety-class or safety-significant if the engineered controls were available and selected. The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs be preferable to ACs or SACs due to the inherent uncertainty of human performance. SACs may be used to help implement a specific aspect of a program AC that is credited in the safety analysis and therefore has a higher level of importance.

In accordance with nuclear safety precepts, a special level of control is provided through use of TSRs. The safety items identified in the hazard analysis are examined against those criteria to identify a subset of the most significant controls that prevent uncontrolled release of hazardous materials and nuclear criticality. These TSR controls may be captured in operational limits or in administrative controls, including those on safety management programs. This collection of TSRs formally acknowledges features that are of major significance to defense in depth.

Programmatic Commitments

Sections 10 CFR 830.204(b)(5) and 830.204(b)(6) of the Rule require that the DSA define the characteristics of the safety management programs necessary to ensure the safe operation of the facility. Program commitments (e.g., radiation protection, maintenance, QA) encompass a large number of details that are more appropriately covered in specific program documents (e.g., plans and procedures) external to the DSA.

The cumulative effect of these details, however, are recognized as being important to facility safety, which is the rationale for a top-level program commitment becoming part of the safety basis.

As appropriate to the hazard, the safety basis may identify specific controls (e.g., hazardous material inventory limits) that are required for safety. These controls should be considered for designation as an SAC as discussed in this standard and DOE-STD-1186-2004.

The importance of the program commitments, which can be incorporated in TSRs as administrative controls, cannot be overestimated. The safety basis, however, includes only the top-level summary of program elements, not the details of the program or its governing documents. Inspection discrepancies in a program would not constitute violation of the safety basis unless the discrepancies were so gross as to render premises of the summary invalid.

By virtue of application of the graded approach, the majority of the engineered features in a facility will not be identified in the categories of safety-class or safety-significant SSCs even though they may perform some safety functions. However, such controls noted as a barrier or preventive or mitigative feature in the hazard and accident analyses must not be ignored in managing operations. Such a gross discrepancy would violate the safety basis documented in the DSA even if the controls are not designated safety-class or safety-significant, because programmatic commitments extend to these SSCs as well. For example, the commitment to a maintenance program means that the preventive and mitigative equipment noted as such in the DSA hazard analysis is included in the facility maintenance program. As a minimum, all aspects of defense in depth identified must be covered within the relevant safety management programs (e.g., maintenance, QA) committed to in the DSA. The details of that coverage, however, are developed in the maintenance program documentation, not in the DSA.

An overall commitment made in a DSA is that the contractor will not change the facility configuration underlying the documented safety basis without implementing and completing the USQ process. However, situations do occur where a USQ process is not necessary. For example, a stipulation to have a radiation protection program in the administrative control section of the TSR is a commitment; however, changes to specific program provisions do not require going through the USQ process. Further clarification of such interpretations can be found in DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements*.

TSRs and SSCs

In order to comply with 10 CFR 830, specific safety controls are to be developed in the DSA. In keeping with the graded-approach principle, distinctions are made to avoid wasting effort by providing detailed descriptions of all facility SSCs. While a basic descriptive model of the facility and its equipment must be provided in chapter 2, “Facility Description,” highly detailed descriptions are reserved for two categories of SSCs comprising the most crucial aspects of facility safety. These two categories are safety-class SSCs and safety-significant SSCs.

Detailed descriptions are provided for safety-class and safety-significant SSCs and SACs in chapter 4 of the DSA because of the importance of their safety functions. Descriptions result in the definition of functional requirements and associated performance criteria used to derive TSRs. TSRs are safety controls developed in accordance with the precepts of 10 CFR 830. TSR and SSC commitments encompass the following:

Technical Safety Requirements

TSRs comprise (1) SLs, (2) operational limits consisting of limiting control settings and LCOs and associated SRs, (3) ACs, (4) SACs, (5) use and application provisions, (6) design features, and (7) "Bases" appendix. Based on the results of hazard and accident analysis, TSRs are designated for (1) safety-class SSCs and controls established on the basis of application of the EG (2) safety-significant SSCs; (3) defense-in-depth in accordance with the screening criteria of DOE G 423.1-1; and (4) safety management programs for defense in depth or worker safety. The "Bases" appendix provides the linkage to the DSA.

It is important to develop TSRs judiciously. TSRs should not be used as a vehicle to cover the many procedural and programmatic controls inherent in any operation. Excessive use of TSR limits to manage operations will result in distortion of the regulatory structure DOE is attempting to develop and will dilute the emphasis intended for the most critical controls.

SLs should be limited in number and designated with caution. In accordance with table 4 of appendix A to subpart B of 10 CFR 830, SLs are generally reserved for limits on process variables associated with those safety-class physical barriers, generally passive, that are necessary for the intended facility function and that are required to guard against the uncontrolled release of radioactive materials. The associated OLs apply to active SSCs that prevent exceeding SLs. The only candidates for SLs should be safety-class SSCs and any non-SSC controls established on the basis of the application of the EG. Nuclear industry precedent is that only a limited subset of safety-class SSCs, if any, requires the definition of associated SLs, which are intended to prevent significant accidents as opposed to mitigating their effects.

TSRs assigned for defense in depth or safety-significant SSCs do not have SLs and are not required to use operational limits (i.e., LCSs, LCOs). They should, however, receive coverage in the administrative control section of TSRs as a minimum.

Judgment should be used to determine what controls warrant use of operational limits. When TSR administrative controls are used for purposes other than generic coverage of safety management programs (e.g., SAC), descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why. Beyond safety-significant SSCs designated for worker safety and their associated TSR coverage, additional worker safety issues should be covered in TSRs only by administrative controls on overall safety management programs.

Safety-Class Structures, Systems, and Components

The Rule defines safety-class designation for SSCs that are established on the basis of application of the EG. This designation carries with it the most stringent requirements (e.g., enhanced inspection, testing and maintenance, and special instrumentation and control systems). Appendix A of 10 CFR 830 provides guidance for implementing the EG to classify SSCs as safety-class SSCs.

Safety-Significant Structures, Systems, and Components

This category of SSCs is provided to ensure that important SSCs will be given adequate attention in the DSA and facility operations programs. Safety-significant SSCs are those of particular importance to defense in depth or worker safety as determined in hazard analysis. Control of such SSCs does not require meeting the level of stringency associated with safety-class SSCs.

The EG is not used for designating safety-significant SSCs. Safety-class SSCs are designated to address public risk, which makes a dose guideline at the site boundary a useful tool. Safety-significant SSCs address risk for all individuals within the site boundary as well as additional defense in depth for the public, making a dose guideline at any one point an artificial distinction distorting the process of systematically evaluating SSCs. TSRs covering SSCs ensuring defense in depth should generally correlate with safety-significant SSC designation for defense in depth, but exact one-to-one correlation is not required.

Specific Administrative Controls

This category of ACs is provided to ensure that controls important to safety that are needed to prevent or mitigate an accident scenario will be given equivalent attention in the safety basis documents had that safety function been provided by a safety-class or safety-significant SSC. Safety analyses shall establish the identification and functions of SACs and the significance to safety of the functions of the SAC. The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs be preferable to ACs or SACs due to the inherent uncertainty of human performance.

Hazard Analysis

The initial analytical effort for all facilities is a hazard analysis that systematically identifies facility hazards and accident potentials through hazard identification and hazard evaluation. The focus of the hazard analysis is on thoroughness and requires evaluation of the complete spectrum of hazards and accidents. This largely qualitative effort forms the basis for the entire safety analysis effort, including specifically addressing defense in depth and protection of workers and the environment. Basic industrial methods for hazard analysis, its interface with more structured quantitative evaluations, and the basis for both have been described in references such as the American Institute of Chemical Engineers *Guidelines for Hazard Evaluation Procedures* (1992). OSHA has accepted these guidelines as the standard for analytical adequacy in characterizing commercial chemical processes that perform the same type of unit operations conducted at DOE nonreactor nuclear facilities. Appropriately

applied, they help fulfill the requirements of DSAs for hazard category 2 and 3 facilities as specified in 10 CFR 830.

The largely qualitative techniques described in the above reference on hazard analysis provide methodologies for comprehensive definition of the accident spectrum for workers and the public. The basic identification of hazards inherent in the process provides a broad, initial basis for identification of safety programs needed (e.g., radiation protection, hazardous chemical protection). The hazard analysis then moves beyond basic hazard identification to evaluation of the expected consequences and estimation of likelihood of accidents, an activity that in no way connotes the level of effort of a probabilistic or quantitative risk assessment.

Throughout the evaluation process, preventive and mitigative SSCs, and SACs and pertinent elements of programmatic controls are identified. This identification also establishes functional requirements, which will subsequently delineate the technical information (i.e., response parameters) needed to establish performance criteria. The DSA summarizes these requirements and criteria for safety-class and safety-significant SSCs and SACs only. Refinement of the information obtained in hazard evaluation leads to overall definition of defense in depth, worker safety, and environmental protection.

The most significant aspects of defense in depth and worker safety are subject to designation as safety-significant SSCs and coverage by TSRs. Other items noted are encompassed by the details of safety management programs (e.g., procedures, training, maintenance, QA), which can be captured in top-level fashion in TSR administrative controls. However, programmatic administrative controls should not be used to provide preventive or mitigative functions for accident scenarios identified in the safety basis where the safety function has importance similar to, or the same as the safety function of safety-class or safety-significant SSCs. The classification of SAC was specifically created for this safety function. The hazard evaluation conducted to assess the accident spectrum associated with hazards germane to the DSA indicates the adequacy of programmatic efforts and provides input to programmatic activities whose discipline provides a significant margin of safety.

The process outlined above is self-grading for analytical effort. Analytical effort can be limited to a simple, resource efficient hazard analysis geared to facility needs, unless events are noted that are of sufficient complexity to require more detailed, quantitative evaluations to understand the basis for safety assurance. Implicit in this methodology is the statement of DOE-STD-1027-92 that the largely qualitative level of effort in hazard analysis is appropriate and sufficient for accident analysis of hazard category 3 facilities.

The hazard analysis effort is not a quantitative risk assessment. Preparers (and reviewers) cannot expect the level of detail associated with a quantitative risk assessment in a hazard analysis, as the hazard analysis is focused on systematically assessing what can go wrong in a facility as opposed to deriving mathematical expressions of risk.

The final purpose of hazard analysis is to identify a limited subset of accidents to be carried forward to accident analysis.

Accident Analysis

The complete spectrum of accidents is examined in hazard analysis. A limited subset of accidents, (i.e., DBAs and derivative DBAs) that bound "the envelope of accident conditions to which the operation could be subjected" are carried forward to accident analysis where safety-class SSCs are designated by comparison of accident consequences to the EG. Identification of DBAs in safety analysis and use of DBAs is appropriate in defining a facility safety basis. DBAs are accidents that are utilized to provide the design parameters for release barriers and mitigating systems. DBAs are a "front-end" device for designing individual equipment or systems to meet functional requirements, as evidenced by use of the phrase "utilized to provide the design parameters." An accident can be defined as a DBA if relevant SSCs were specifically designed to function during that accident and appropriate documentation of this fact exists.

The range of accident scenarios analyzed in a DSA should be such that a complete set of bounding conditions to define the envelope of accident conditions to which the operation could be subjected are evaluated and documented. This necessitates the consideration of accidents other than DBAs for two cardinal reasons. First, even if DBAs exist, they may not adequately cover "the range of accident scenarios" needed to establish the facility safety basis. Second, DBAs may not cover a "complete set of bounding conditions." Either of these conditions may arise for a number of reasons, such as the original design not being related to bounding conditions, the criteria for determining facility safety basis having significantly changed, operations or types of hazards having changed, or magnitude of hazards having increased. Any one of these reasons may make the DBA inadequate for determining a facility safety basis.

The most obvious and extreme reason for examining accidents other than DBAs for existing facilities is a lack of design documentation. If appropriate design documentation is not available, postulated accidents are not DBAs. The front-end purpose of a DBA (i.e., "to provide the design parameters") cannot be meaningfully addressed even if existing design parameters are estimated and used to develop an accident scenario. The reconstructed accident would not determine design parameters. It would be determined by them. The need to analyze a range of scenarios that bound conditions would not clearly be met by such an exercise. This potential lack of relevance is one of the reasons that the DSA is not the proper vehicle for formally filling gaps in existing design documentation.

Where DBAs do not exist, or do not adequately cover the range of scenarios or bounding conditions, surrogate evaluation bases are needed. These derivative DBAs are used to estimate the response of SSCs to "the range of accident scenarios" and stresses that bound "the envelope of accident conditions to which the facility could be subjected" in order to evaluate accident consequences. The derivative DBAs should take maximum advantage of the pertinent existing design information (i.e., requirements and bases) that is immediately available or can be retrieved through reasonable efforts. To the extent necessary, this information can be supplemented by testing, extrapolation, and engineering judgments.

Existing facilities, like all industrial facilities, were generally built with standard process and utility SSCs with a high consideration for basic safety. For the majority of these facilities, adequate facility design and process information exists that, while not of the quality and detail expected for current conceptual design, is typical of many commercial processing operations, which comprise the majority of industrial practices. This information can be used in estimating SSC response to derivative DBAs whose evaluation will satisfy the requirements of safety analysis.

For operational accidents, a derivative DBA is defined based on the physical possibility of phenomena as defined in the hazard analysis. Use of a lower binning threshold such as 10^{-6}/yr is generally appropriate, but should not be used as an absolute cutoff for dismissing physically credible low probability operational accidents (e.g., red oil explosions) without any evaluation of preventive and mitigative features in hazard analysis. This distinction is made to prevent "pencil sharpening" at the expense of objective evaluation of hazards. Examples of a candidate derivative DBA would be an ion exchange column or a red oil explosion at a facility where the phenomena is physically possible, and documentation is not available substantiating ventilation and building confinement systems were specifically designed for such an occurrence. For natural phenomena accidents, derivative DBAs are defined by a frequency of initiator based on DOE O 420.1B, *Facility Safety*, and its associated implementation standards. For external man-made accidents, derivative DBAs are assumed if the event can occur with a frequency $>10^{-6}$/yr as conservatively estimated, or $>10^{-7}$/yr as realistically estimated. Use of a frequency cutoff for external events represents a unique case for external events only, based on established NRC precedents.

Application of the Graded Approach

Title 10 CFR 830 prescribes the use of a graded approach for the effort expended in safety analysis and the level of detail presented in associated documentation. The graded approach applied to DSA preparation and updates is intended to produce cost-efficient safety analyses and DSA content that provide adequate assurance to the DOE that a facility has acceptable safety provisions without providing unnecessary information. As described in 10 CFR 830, the graded approach adjusts the magnitude of the preparation effort to the characteristics of the subject facility based on seven factors:

1. The relative importance to safety, safeguards, and security;
2. The magnitude of any hazard involved;
3. The life cycle stage of a facility;
4. The programmatic mission of a facility;
5. The particular characteristics of a facility;
6. The relative importance of radiological and nonradiological hazards; and
7. Any other relevant factor.

The Rule provides for developing the DSA based on judgment of the facility in relation to these seven factors. For example, simple hazard category 3 facilities or facilities that have a short operational life may only require a limited but adequate analysis documented to a level less than that required for a hazard category 2 facility. Additionally, facilities with short operational lives (or other compelling circumstances) should consider the appropriateness of

using DOE-STD-3011-2002 to meet the requirements of 10 CFR 830. On the opposite end of the spectrum, a complex hazard category 1 facility that is just going into operation requires extensive analysis and highly detailed documentation.

The application of the graded approach may allow for much simpler analysis and documentation for some of these facilities. For facilities of little hazard, or hazards at the hazard category 3 level, for which only a modest reduction of risk is required, the DSA may be simple and short. In such cases all of the topics for the DSA listed in DOE-STD-3009-94 may not be necessary, and with proper technical bases some topics may be omitted or reduced in the detail that would otherwise be required of hazard category 1 or 2 facilities.

Thus, with application of the graded approach, DSAs for hazard category 3 facilities or facilities with short operational lives will normally require more simplified documented safety analysis and documentation. Specific minimum levels of detail for these facilities are given in options 3 and 8 in table 2 of appendix A to 10 CFR 830, subpart B. As a minimum, a DSA would be found acceptable for a simple hazard category 3 facility if it used the methods in chapters 2, 3, 4, and 5 of DOE-STD-3009-94 to address in a simplified fashion

- the basic description of the facility and its operations, including SSCs;
- a qualitative hazards analysis; and
- the hazard controls (consisting primarily of inventory limits and safety management programs) and their bases.

Safe Harbor Methods

Table 8. Safe harbor methods

The contractor responsible for * * *	May prepare its documented safety analyses by * * *
(1) A DOE reactor.....	Using the method in U.S. Nuclear Regulatory Commission Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, or successor document.
(2) A DOE nonreactor nuclear facility……	Using the method in DOE-STD- 3009, Change Notice No. 1, January 2000, Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports, July 1994, or successor document.
(3) A DOE nuclear facility with a limited operational life.	Using the method in either: (1) DOE-STD-3009-, Change Notice No. 1, January 2000, or successor document, or (2) DOE-STD-3011-94, Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans, November 1994, or successor document.
(4) The deactivation or the transition surveillance and maintenance of a DOE nuclear facility.	Using the method in either: (1) DOE-STD-3009, Change Notice No. 1, January 2000, or successor document, or (2) DOE-STD-3011-94 or successor document.
(5) The decommissioning of a DOE nuclear facility.	(1) Using the method in DOE-STD- 1120-98, Integration of Environment, Safety, and Health into Facility Disposition Activities, May 1998, or successor document; (2) Using the provisions in 29 CFR 1910.120 (or 29 CFR 1926.65 for construction activities) for developing Safety and Health Programs, Work Plans, Health and Safety Plans, and Emergency Response Plans to address public safety, as well as worker safety; and (3) Deriving hazard controls based on the Safety and Health Programs, the Work Plans, the Health and Safety Plans, and the Emergency Response Plans.
(6) A DOE environmental restoration activity that involves either work not done within a permanent structure or the decommissioning of a facility with	(1) Using the method in DOE-STD-1120-98 or successor document, and (2) Using the provisions in 29 CFR 1910.120 (or 29 CFR 1926.65 for construction activities) for developing a Safety and Health Program and a

The contractor responsible for * * *	May prepare its documented safety analyses by * * *
only low-level residual fixed radioactivity.	site-specific Health and Safety Plan (including elements for Emergency Response Plans, conduct of operations, training and qualifications, and maintenance management).
(7) A DOE nuclear explosive facility and the nuclear explosive operations conducted therein.	Developing its documented safety analysis in two pieces: (1) A Safety Analysis Report for the nuclear facility that considers the generic nuclear explosive operations and is prepared in accordance with DOE-STD-3009, Change Notice No. 1, January 2000, or successor document, and (2) A Hazard Analysis Report for the specific nuclear explosive operations prepared in accordance with DOE-STD- 3016-99, Hazards Analysis Reports for Nuclear Explosive Operations, February 1999, or successor document.
(8) A DOE hazard category 3 nonreactor nuclear facility....	Using the methods in Chapters 2, 3, 4, and 5 of DOE-STD- 3009, Change Notice No. 1, January 2000, or successor document to address in a simplified fashion: (1) The basic description of the facility/activity and its operations, including safety structures, systems, and components; (2) A qualitative hazards analysis; and (3) The hazard controls (consisting primarily of inventory limits and safety management programs) and their bases.
(9) Transportation activities.....	(1) Preparing a Safety Analysis Report for Packaging in accordance with DOE-O-460.1A, Packaging and Transportation Safety, October 2, 1996, or successor document and (2) Preparing a Transportation Safety Document in accordance with DOE-G-460.1-1, Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety, June 5, 1997, or successor document.
(10) Transportation and onsite transfer of nuclear explosives, nuclear components, Naval nuclear fuel elements, Category I and Category II special nuclear materials, special assemblies, and other materials of national security.	(1) Preparing a Safety Analysis Report for Packaging in accordance with DOE-O-461.1, Packaging and Transportation of Materials of National Security Interest, September 29, 2000, or successor document and (2) Preparing a Transportation Safety Document in accordance with DOE-M-461.1-1, Packaging and Transfer of Materials of National Security Interest Manual, September 29, 2000, or successor document.

Source: DOE G 421.1-2 and 10 CFR 830

c. Discuss the relationship between the safe harbor methods for a DSA in 10 CFR 830 Appendix A with regard to completeness.

The DSA for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility

- describe the facility (including the design of safety structures, systems and components) and the work to be performed;
- provide a systematic identification of both natural and man-made hazards associated with the facility;
- evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility;
- derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use;
- define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) QA, procedures,

maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection; and

- with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a CSP that
  - ensures that operations with fissionable material remain sub-critical under all normal and credible abnormal conditions,
  - identifies applicable nuclear criticality safety standards, and
  - describes how the program meets applicable nuclear criticality safety standards.

d. Describe the objectives of requiring accident analyses in safety basis documents.

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 implementing DOE-STD-3009-94, 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 EG to identify safety-class structures, systems, and components.

e. Identify and discuss the use of the source term five-factor formula in accident analyses.

The following is taken from DOE-HDBK-3010-94.

The source term is the MAR (as derived from the hazard identification), the release fraction or rate, and the overall facility leak path factors that determine the fraction of material released external to the facility.

The airborne pathway is of primary interest for nonreactor nuclear facilities. DOE-STD-1027-92 states, "for all materials of greatest interest for fuel cycle and other radioactive material licenses, the dose from the inhalation pathway will dominate the (overall) dose."

The airborne source term is typically estimated by the following five-factor equation:

$$\text{Source term} = \text{MAR} \times \text{DR} \times \text{ARF} \times \text{RF} \times \text{LPF}$$

where
MAR = material at risk (curies or grams)
DR = damage ratio
ARF = airborne release fraction (or airborne release rate] for continuous release)
RF = respirable fraction
LPF = leak path factor.

The initial source term and initial respirable source term are products of the first three factors and first four factors respectively. A depleted source term after a subsequent stage of

deposition or filtration is a product of the initial source term multiplied by the leak path factor of the specific stage.

DOE-HDBK-3010-94 provides ARF and RF values for sources of airborne material generated from accidents involving gases, liquids, solids, and surface contamination. All of the above factors may need to be determined for particulate releases. Some of them, however, will collapse to values of one for special cases (e.g., gaseous releases).

Material at Risk (MAR)

The MAR is the amount of radionuclides (in grams or curies of activity for each radionuclide) available to be acted on by a given physical stress. For facilities, processes, and activities, the MAR is a value representing some maximum quantity of radionuclide present or reasonably anticipated for the process or structure being analyzed. Different MAR values may be assigned for different accidents, as it is only necessary to define the material in those discrete physical locations that are exposed to a given stress. For example, a spill may involve only the contents of a tank in one glovebox. Conversely, a seismic event may involve all of the MAR in a building.

Damage Ratio (DR)

The DR is the fraction of the MAR actually impacted by the accident conditions. A degree of interdependence exists between the definitions of MAR and DR. If it is predetermined that certain types of material would not be affected by a given accident, some analysts will exclude this material from the MAR. The DR is estimated based upon engineering analysis of the response of structural materials and materials of construction for containment to the type and level of stress/force generated by the event. Standard engineering approximations are typically used. These approximations often include a degree of conservatism due to simplification of phenomena to obtain a useable model, but the purpose of the approximation is to obtain, to the degree possible, a realistic understanding of potential effects.

Airborne Release Fraction (ARF)

The ARF is the coefficient used to estimate the amount of radioactive material suspended in air as an aerosol and thus available for transport due to physical stresses from a specific accident. For discrete events, the ARF is a fraction of the material affected. For mechanisms that continuously act to suspend radionuclides (e.g., aerodynamic entrainment/resuspension), a release rate is required to estimate the potential airborne release from postulated accident conditions. Generally, accident release rates are based upon measurements over some extended period to encompass most release situations for a particular mechanism. The rates are average rates for the broad spectrum of situations and, as such, the most typically meaningful time unit to reflect average conditions is 1 hour. There is evidence that in some situations (e.g., aerodynamic entrainment of sparse powder deposits on a heterogeneous surface), the rate of release is not uniform with time. Even in the situations where the rates are relatively uniform, the source is depleted by the removal of particles from the surface by aerodynamic forces, and the amount of material airborne decreases with time unless the source is continuously replenished. The ARFs are based primarily upon experimentally measured values for the specific material (e.g., plutonium, uranium, mixed fission products)

or surrogates subjected to the particular type of stress under controlled conditions. Attention is given to the parameters, if known, that may have a significant influence upon suspension by the specific mechanism and the uncertainty in the measurement as indicated by the variability of the results.

Respirable Fraction (RF)

The RF is the fraction of airborne radionuclides as particles that can be transported through air and inhaled into the human respiratory system and is commonly assumed to include particles 10-µm AED and less. Other definitions of "respirable particles" have been presented by various groups at different times. Use of a 10-µm AED cut-size for respirable particles is considered conservative and may even be overly conservative, since the mass is a cube function of particle diameter.

Leak Path Factor (LPF)

The LPF is the fraction of the radionuclide in the aerosol transported through some confinement deposition or filtration mechanism. There can be many LPFs for some accident conditions (e.g., the fraction transported from the package, such as a shipping container, to the cell or enclosure; the fraction leaked from the enclosure, cell, or glovebox to the operating area around the enclosure or room; the fraction leaked from the room to the building-atmosphere interface). Where multiple leak paths are involved, their cumulative effect is often expressed as one value that is the product of all leak path multiples. The LPF is a calculated or standard value based upon (1) established relationships between the size of the particulate material, airborne transport mechanisms, and losses by deposition mechanisms, or (2) specified filtration efficiencies.

f. Given an accident scenario, determine a reasonably bounding estimate of the Airborne Release Fraction (ARF) and Respirable Fraction (RF), Material At Risk (MAR), Leak Path Factor (LPF), and Damage Ratio (DR) to determine the product (MAR × ARF × RF × DR × LPF).

Element f is performance based. The Qualifying Official will evaluate its completion. The information provided in element e of this competency may be helpful.

g. Identify and discuss the methods, conventions, and data sources used in developing estimates of the five factors for use in accident analyses.

See element e of this competency for a discussion of the methods, conventions, and data sources used in developing estimates of the five factors for use in accident analyses.

h. Identify and discuss methods/codes used to determine the environmental dispersion and delivered doses from accidental releases of hazardous materials.

The following is taken from DOE-STD-3009-94.

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 EG.

The method used should be consistent with the statistical treatment of calculated X/Q values described in regulatory position 3 of 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 outline in position 1.2 of Regulatory Guide 1.145. NRC Regulatory Guide 1.23 describes 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. 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 wind speed 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. 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 EG.

i. Discuss the effect of prevailing weather, building wake effects, and plume buoyancy upon the magnitude and distribution of doses from hazardous releases into the atmosphere.

The following is taken from EPA, *Air Toxics Risk Assessment Reference Library,* volume 1, *Technical Resource Manual,* chapter 8, "Quantification of Exposure: Dispersion, Transport, and Fate of Air Toxics in the Atmosphere."

EPA and others have developed several air "dispersion" models to predict the often-complex behavior of air pollution releases. Most air dispersion models take into account a number of characteristics of the source and pollutants released. The most common of these characteristics are described below.

Release Rate and Volume

The rate of release (exit velocity) strongly influences the behavior of the pollutant plume as it moves through the atmosphere. In the case of stack and vent releases, sources can release pollutants as pure vapors, as dilute solutions of vapor in air or other gases, or as suspended particles. Large volumes are often released at a relatively high velocity from stacks or vents,

which can also serve to drive pollutants higher in the atmosphere. Air quality models often calculate volume from data on exit area and exit velocity. In the case of fugitive releases or volatilization, the "volume" of release has less meaning, and often does not receive explicit consideration in fate and transport modeling.

Concentration

Concentration (the mass of pollutant per unit volume of released gases) is the other half of the equation that determines the amount (mass) of pollutant released. Pollutants at higher concentrations may also be more likely to condense onto particles or liquid droplets.

Temperature

The temperature of a plume emitted from a stack or vent influences the dispersion and transport of pollutants. A plume that is warmer than the surrounding air will generally rise, which tends to increase the distance over which pollutants will be transported. The temperature and the vertical velocity of stack emissions combine to affect the height to which the plume will rise and the layer of the atmosphere in which it will initially be transported. As with concentration, the temperature of the plume also affects the physical form of pollutants, with less volatile pollutants condensing faster from cooler plumes.

Height

Pollutants may also be released into the atmosphere at different heights, and the height of release can strongly affect dispersion and transport. Greater release heights generally result in increased pollutant dilution in the atmosphere, lower ground-level concentrations, and a greater distance to peak ground-level concentrations. Release height also is important in evaluating local effects on air transport, such as building downwash. While power generation or industrial activities may release combustion products from stacks that are hundreds of feet tall, volatilization releases or suspension of particulate pollutants often occur at or near the ground surface.

Timing and Duration

Multiplying the release duration by the release rate produces the total mass of pollutant released. The timing of release relative to specific meteorological conditions determines the particular dispersion and transport of pollutants. Unfortunately, only total annual or average daily release data are available for most sources, making it difficult to fully characterize time varying releases. Fortunately, chronic exposure assessments usually focus on the average long-term (annual) concentrations. Acute exposure assessments, however, usually focus on the maximum short-term (24 hours or less) concentration. Acute exposures are derived from conservative meteorological factors that lead to the highest short-term peak values for a screening exercise; for a more detailed exercise, the actual meteorology should determine the short-term peaks.

Physical Form

The physical form of pollutant releases greatly affects the dispersion, transport, and chemical reactions that pollutants undergo. Generally, pollutants are characterized as being vapors (not

bound to particles, but existing as single molecules or very small aggregates "dissolved" in air—also called gaseous), particle-bound (reversibly absorbed or condensed onto the surface of particles), or particulate (irreversibly incorporated into airborne particles). The distribution of pollutants in these three "phases" is known as partitioning. Partitioning is a function of the chemical and physical properties of the pollutants and the temperature and pressure of the atmosphere into which the chemicals have been released (e.g., the partitioning behavior of pollutants can vary greatly with temperature). As noted above, sources can emit chemical pollutants in the vapor phase at relatively high temperatures, and these pollutants can condense into or onto particulates as the emitted gases cool in the atmosphere. Sources generally emit most metals (with the important exception of mercury) as particles in the atmosphere.

Particle Size

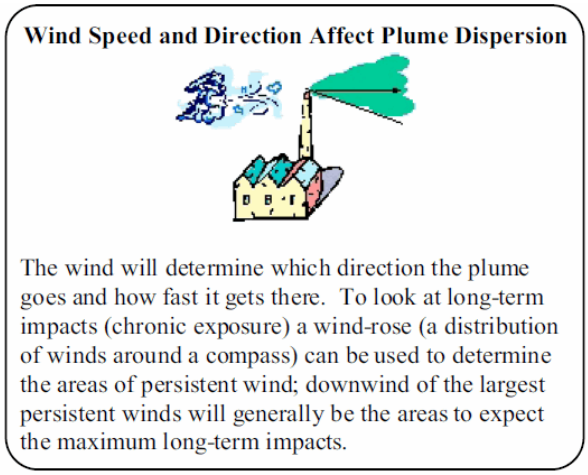
When sources release pollutants as particles (or if released as gases, if these pollutants condense into particles or absorb onto the surface of existing particles), the rate of pollutant removal from the atmosphere to surfaces (e.g., plants, soils, surface water) depends upon particle size. The typical size of particles that different activities and processes emit into the air can vary by many orders of magnitude (powers of ten). As the size of particles increases, the rate at which particles fall due to gravity (the settling velocity) increases. Thus, fine particles (approximate diameter less than a few microns) may remain suspended in air indefinitely, but particles larger than about 20 microns in diameter settle rapidly and may not transport far from sources of release.

Particles less than 10 microns in diameter are of primary concern because they are small enough to be taken into and deposited in the lung after inhalation. These particles are divided into two size ranges: "fine" particles less than 2.5 micrometers in size ($PM_{2.5}$, where "PM" is the abbreviation for particulate matter), and "coarse" particles covering the range from 2.5 to 10 micrometers in diameter (PM_{10}). (Thus, monitoring analyses for metals in particulates, for example, would commonly collect particulate samples of $PM_{2.5}$ and PM_{10} for analysis, not total suspended particulate, because such samples contain particles that are too large to be effectively respired—thereby leading assessors to overestimate inhalation risk). Particles emitted from combustion and high-temperature chemical processes can be very fine, on the order of 0.01 to 1.0 microns in diameter. Such fine particles tend to condense to form larger aggregates up to the limit of perhaps a few microns, and participate in a wide range of chemical reactions.

Chemical Form

Chemical form is generally more of a concern for inorganic pollutants, because organic chemicals tend to have well-defined chemical compositions and properties. The most important chemical properties of inorganic metal compounds, for example, include the oxidation or valence state of the cationic metal, the identity of the anionic counterion, and the chemical and physical properties of the compound comprising the cation and the anion. As an example of the importance of valence state, consider the metal chromium. When emitted in the hexavalent form (with six positive charges—Cr^{6+}), chromium is highly reactive chemically and is readily reduced under certain conditions to the trivalent form, which is

Cr^{3+}. Hexavalent chromium can cause respiratory irritation and cancer in humans. Trivalent chromium, on the other hand, is much more stable, is much less toxic to humans and animals (and is actually an essential mineral), and is not thought to cause cancer.



Source: EPA, *Air Toxics Risk Assessment Reference Library*

Figure 43. Wind speed and direction affect plume dispersion

The following is taken from chapter 8, "Quantification of Exposure: Dispersion, Transport, and Fate of Air Toxics in the Atmosphere," in volume 1, *Technical Resource Manual,* of the EPA's Air Toxics Risk Assessment Reference Library.

The following paragraphs describe some of the most important physical and meteorological factors that affect the movement of air pollutants after their release. Although this section focuses on releases from stationary point sources (i.e., stacks), most of the factors may apply to releases from other source types as well. Stacks come in all sizes, from a small vent on a roof to stacks hundreds of feet in height. The function of a stack is to remove pollution of high concentration and to discharge it to the atmosphere for dispersion and transport. Stacks release pollutants high enough above the earth's surface that pollutants can sufficiently disperse in the atmosphere before reaching ground level. All else being equal, taller stacks disperse pollutants more effectively than shorter stacks because the pollutants release into higher wind speeds and travel through a greater depth of the atmosphere before reaching ground level.

The air space the stack pollutant occupies can be described as a plume. As the plume travels, it spreads and disperses, reducing ambient pollutant concentrations even though the cross sectional mass of the plume remains the same. Eventually, the plume may intercept the ground. The combination of emission velocity, emission temperature, vertical air movement and horizontal airflow all influences how high a plume will rise and how fast and far it travels. Another factor is wind meander (i.e., changes in wind direction during light wind speed conditions), which can cause the plume to deviate in the horizontal direction due to turbulence and wind fluctuation.

As the gases exit the stack, they mix with ambient air. This mixing of ambient air into the plume is called entrainment. The plume grows in volume as it entrains ambient air and travels downwind. Because stack gases are often warmer than the ambient outdoor air, the gases may be less dense than the outdoor air and are therefore buoyant (like a helium filled balloon). Gases that stacks emit are often pushed out by fans giving the gas momentum as it enters the atmosphere. The combination of this momentum and the buoyancy of the stack gases that are warmer than the ambient air cause the gas to rise.

This plume rise allows air toxics emitted in this stack stream to be lofted higher in the atmosphere. Since the plume is higher in the atmosphere where the winds are generally stronger, the plume will generally disperse more before it reaches ground level. Plume rise depends on the stack's physical characteristics and on the effluent's exit temperature and velocity.

The condition of the atmosphere (i.e., the vertical profile of the winds and temperature) along the path of the plume also determines how far the plume rises in the atmosphere. An inversion layer (formed when a layer of warm air "traps" a layer of cold air beneath) may act as a barrier to vertical mixing. The height of a stack in relation to the height of the inversion layer may often influence ground-level pollutant concentrations.

The initial velocity of the plume (stack exit velocity) reduces quickly as the plume entrains ambient air and acquires horizontal momentum from the wind. This momentum causes the plume to bend over. The greater the wind speed, the more horizontal momentum the plume acquires. Wind speed usually increases with height above the earth's surface. Therefore, as the plume continues upward the stronger winds tilt the plume even further. This process continues until the plume may appear to be horizontal to the ground. The point where the plume looks level may be a considerable distance downwind from the stack.

Due to configuration of the stack or adjacent buildings, the plume may not rise freely into the atmosphere. The way in which the wind moves around adjacent buildings and the stack can force the plume toward the ground instead of allowing it to rise in the atmosphere. Stack-tip downwash can occur where the ratio of the stack exit velocity to horizontal wind speed is small. In this case, low pressure in the wake of the stack may cause the plume to draw downward behind the stack. Pollutant plume rise reduces when this occurs and elevates pollutant concentrations immediately downwind of the source. As air moves over and around buildings and other structures, it forms turbulent wakes. Depending upon the stack height, it may be possible for the plume to be pulled down into this wake area. The reduction in plume height is known as aerodynamic or building downwash.

Once air toxics have equilibrated with ambient conditions (e.g., temperature, velocity), atmospheric and meteorologic factors primarily influence dispersion and transport of air toxics. In particular, the rate of dispersion is influenced by both the thermal structure of the atmosphere and mechanical agitation of the air as it moves over the different surface features of the earth.

j. Identify and discuss the treatment of uncertainty and the realistic effects in accident analyses.

The following is taken from DOE-HDBK-3010-94.

Airborne release fractions are based primarily on experimentally measured values for the specific material (e.g., plutonium, uranium, mixed fission products) or surrogates subjected to the particular type of stress under controlled conditions. Attention is given to the parameters, if known, that may have a significant influence upon suspension by the specific mechanism and the uncertainty in the measurement as indicated by the variability of the results. Those applying the data must be aware of the range of stress represented by the measured ARFs, and seek to define the accident conditions to determine, in a gross sense, whether or not the stresses induced by the postulated events are bounded by the experimental parameters.

No attempt is made to precisely characterize total airborne material in terms of individual mechanisms acting within an overall given release. To obtain useful data outside the immediate physical chaos of the stress-inducing event itself, the experimental apparatus almost uniformly rely on designs to channel air to some contamination collection mechanism a short distance from the point of generation. The need to keep this distance small to avoid introducing new distortion in the form of aerosol deposition effects is one of the reasons for the relatively small scale of many experiments.

In keeping with this experimental design, the interpretation of experimental data does not consider material momentarily airborne from substrate mass ejection due to physical stresses acting on the substrate mass as an aerosol suspended in air. For example, in fire and boiling experiments, fuel mass and volumes of solution were observed to splatter or launch from the experimental substrate and land on surfaces in the local vicinity. The radioactive contamination carried with this material that deposits and is measured on the adjacent surfaces is not an aerosol suspended in air, and does not travel on air currents. It represents a source of highly localized migration that is not amenable to meaningful prediction and is not relevant to the issue of how much material might be expected to escape the immediate area and disperse in air.

Measured experimental data for RFs are much more limited but are from the same general sources used for the ARFs. To keep RFs at a reasonable bounding rather than an ultraconservative level, the RF associated with the measured bounding ARF is generally selected rather than the highest RF value measured. The highest RF values are often associated with the smallest ARFs, and when used in conjunction with the bounding ARF, result in ultraconservative estimates of the respirable fraction released. When no measured RF is associated with the maximum measured ARF, but other measured RFs are available for the experimental set, the greatest RFs are generally used. In some cases where significant uncertainty may exist, RFs are arbitrarily set to a value of 1.0 for conservatism.

There appear to be very large differences in suspension rates under experimental test conditions as well as an order of magnitude uncertainty in measurements for individual conditions. On this basis, conservative values are applied.

k. Identify the purpose and relationship between Chapters 3, 4, and 5 and the TSRs of the DSA.

The following is taken from DOE-STD-3009-94.

Section 3.4.2.X.5 identifies the safety-class SSCs (or equivalent SAC) and assumptions judged to require TSR coverage. Any TSR assumption not directly related to exceeding of the EG should be defined in section 3.3.2.3.2, "Defense in Depth."

Sections 4.3.X.5 and 4.5.X.5 identify those assumptions requiring TSRs to ensure performance of the safety function. SACs are implemented in TSRs generally by either of two forms, as identified below:

1. LCO/SR—SACs can often be written in the format of an LCO.
2. Specific "directive action" administrative control—A specific "directive action" administrative control TSR can be in the administrative controls section of the TSRs.

Section 4 of DOE-STD-1186-2004, *Specific Administrative Controls,* discusses the treatment of SACs in TSRs.

Chapter 5 builds upon the control functions determined to be essential in chapter 3, "Hazard and Accident Analyses," and chapter 4, "Safety Structures, Systems, and Components," to derive TSRs. This chapter is meant to support and provide the information necessary for the separate TSR document required by 10 CFR 830.205.

Derivation of TSRs consists of summaries and references to pertinent sections of the DSA in which design (i.e., SSCs) and administrative features (i.e., non-SSCs) are needed to prevent or mitigate the consequences of accidents. Design and administrative features addressed include ones that (1) provide significant defense in depth; (2) provide for significant worker safety; or (3) provide for the protection of the public. Expected products of this chapter, as applicable based on the graded approach, include

- information with sufficient basis from which to derive, as appropriate, any of the following TSR parameters for individual TSRs:
  - SLs,
  - LCSs,
  - LCOs,
  - SRs;
- information with sufficient basis from which to derive TSR administrative controls for specific control features or to specify programs necessary to perform institutional safety functions;
- identification of passive design features addressed in the DSA;
- identification of TSRs from other facilities that affect the facility's safety basis.

l. Complete a review of a hazards analysis including walking down the scope of the work area.

Element l is performance based. The Qualifying Official will evaluate its completion.

Mandatory Performance Activities:

a. Participate on a combination of at least two (2) safety basis documents or amendment reviews and/or review of safety basis documents whose scope includes evaluation of the development of a source term or radiological dose consequences.

Mandatory performance activities are performance based. The Qualifying Official will evaluate the completion of this competency.

27. Nuclear safety specialists shall demonstrate a working level knowledge of DOE-STD-1186-2004, Specific Administrative Controls, with respect to its impact on the Department's nuclear safety.

The information related to all of the elements in this competency was taken from DOE-STD-1186-2004.

a. Describe the relationship of DOE-STD-1186-2004 to 10 CFR 830, DOE G 423.1-1, and DOE G 421.1-2.

Subpart B of 10 CFR 830, "Safety Basis Requirements," requires contractors responsible for hazard category 1, 2, and 3 nuclear facilities to develop safety bases for those facilities. The safety bases consist of DSAs and hazard controls in TSRs derived from the DSA hazard analyses. Various guides and technical standards, such as DOE-STD-1186-2004, provide guidance to help interpret and implement requirements, including the DSA safe harbor methodologies listed in table 2 of appendix A to 10 CFR part 830. Table 2 is reproduced in table 8 of this guide.

The methodology in DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, is an acceptable method for preparation of a DSA for nonreactor nuclear facilities. DOE-STD-3009-94 provides detailed guidance for preparation of DSAs, including the derivation of TSRs. The general guidance of DOE-STD-3009-94 in methodologies for hazard analysis and specification of hazard controls and their classification is applicable to all the safe harbor methodologies (see DOE G 421.1-2, section 5.3), as is the guidance for SACs in DOE-STD-1186-2004.

Dispositioning activities such as decommissioning and environmental restoration provide unique challenges. In these types of activities, it is common that the hazards and the hazard control sets change as the work progresses. More application-specific guidance for dispositioning activities can be found in DOE-STD-1120-2002, *Integration of Environment, Safety, and Health into Facility Dispositioning Activities.*

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

DOE G 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements*, provides detailed guidance for developing TSR content, including ACs. Section 4.10.7 of the guide recognizes that ACs may be applied for risk reduction of individual accident scenarios. When ACs specifically state a limit or specific requirement rather than a generic programmatic reliance, failure to meet such statements can result in a TSR violation. In contrast, a TSR violation of a safety management program can only result from a gross program failure, significant enough to render the DSA assumptions invalid.

DOE G 423.1-1 and DOE STD-3009-94 continue to provide relevant guidance on the application of ACs as part of the DSA-required controls. However, DOE-STD-1186-2004 provides additional amplification and clarification for the appropriate development and implementation of ACs.

b. Define and discuss how SACs are identified.

To focus attention on the unique issues associated with this type of AC, DOE-STD-1186-2004 introduces a classification of AC known as a specific AC (SAC). An SAC exists when an AC

- is identified in the DSA as a control needed to prevent or mitigate an accident scenario, and
- has a safety function that would be SS or SC if the function were provided by an SSC.

c. Discuss the position of SACs in the preferred hierarchy of hazard controls.

When selecting hazard controls, it is preferable to choose engineering controls over ACs due to the inherent uncertainty of human performance. When choosing engineering controls, it is preferable to choose passive SSCs over active SSCs. When ACs are selected over engineering controls, and the AC meets the criteria for an SAC as provided in DOE-1186-2004, the AC shall be designated as an SAC.

d. Describe how SACs are treated in DSAs and TSRs.

DSAs

The provisions in 10 CFR 830.204 require a DSA to "Derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use."

All hazard controls are identified and characterized in support of the DSA. Judgments must be made regarding what constitutes appropriate controls. These judgments should consider the level of the hazard and potential consequences, the practicality and effectiveness of possible control options, the importance of the mission of the facility, and other relevant factors, if any. These are all elements of the graded approach.

Hazard controls in the DSA are selected to reduce the risks of hazardous activities. Controls are classified by comparison to an EG in the case of SC SSCs for protection of the public, and by criteria described in DOE-STD-3009-94 for SS SSCs for worker protection and defense-in-depth. SC and SS SSCs are expected to be addressed in TSRs.

Specific administrative controls may be acceptable for ensuring safe operation. They must be evaluated carefully when choosing safety measures for long-term hazardous activities because of their generally lower reliability compared with engineered controls. The actual design and selection process should consider the ensemble of controls used to address a hazard, such as cost, availability, required reliability, and consequence of mechanical or human failure for each potential control. SACs have elevated safety significance, and have more stringent implementation and verification requirements to ensure their effectiveness and dependability, as described in DOE-STD-1186-2004.

Controls identified as part of a safety management program (e.g., fire, criticality, radiation protection, etc.) may or may not end up as controls that need to have enhanced dependability, as is the case with SACs, based on the designations derived from the hazards and accident analyses in the DSA. Hazard controls should be identified on a case-by-case basis and should be graded according to the guidance in DOE G 421.1-2, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*; DOE-STD-3009-94; and DOE-STD-1186-2004, with regard to the classification of hazard controls.

For site-wide safety management programs (e.g., radiation protection), the DSA should explain the features of those programs that are important to the facility safety basis and can refer to the site-wide program documentation for the details. As appropriate to the hazard, the DSA may identify specific controls (e.g., hazardous material inventory limits) that are required for safety. These controls should be considered for designation as an SAC as discussed in DOE-STD-1186-2004.

TSRs

A clear distinction is made between programmatic ACs and SACs. Most ACs in the TSRs are designed to provide broad programmatic support for safety management programs supporting defense in depth, or worker safety. Failure to maintain all aspects of one of these programs will not result in a safety basis violation unless there is a gross failure significant enough to render the DSA assumptions invalid (i.e., a programmatic breakdown). These ACs are classified as programmatic ACs. Programmatic ACs should not be used to provide specific or mitigative functions for accident scenarios identified in DSAs where the safety function has importance similar to, or the same as, the safety function of SC or SS SSCs. The classification of SAC, as defined in DOE-STD-1186-2004, was specifically created for this safety function. ACs meeting the criteria in DOE-STD-1186-2004 for selection as SACs

should be formulated, implemented, and maintained in accordance with the guidance in DOE-STD-1186-2004.

e. Discuss how the concepts of validation and verification apply to SACs.

The concepts of validation and verification are important to the formulation of SACs. These concepts, as they apply to SACs, are discussed below.

Validation

The functional requirements and performance criteria for safety SSCs are identified to support the safety functions identified in the DSA and to support subsequent derivation of TSRs. The formulation of SACs should include a similar process that validates plant operators can perform the task(s) called for in an SAC within the timeframes assumed in the DSA. If SACs require operator action and perform a function similar to a safety SSC, assurance should be provided that the operators can adequately perform their required tasks by analyzing the following human performance factors at a minimum:

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

Formal engineering calculations may be necessary to ensure that plant operators have the appropriate time and resources to carry out the required tasks. For example, if it is assumed that operators will take actions to detect and isolate a leak, flow rate calculations will need to be performed to substantiate the available time interval necessary to accomplish the task. Consequences of incorrect implementation of the control should be evaluated, and measures to prevent control failure should be factored into the control formulation.

If SACs require operator action and perform a function similar to a SC SSC, a human reliability assessment (HRA) should be performed as part of the SAC formulation.

The HRA validates the dependability of an SAC and can identify weaknesses in the proposed procedures to implement an SAC and suggest additional measures to improve the overall dependability.

Verification

SACs implemented by TSRs must be initially (prior to operation) and periodically verified to perform their intended safety function. In the context of SACs, this may involve “dry runs,” procedure walk-downs, tabletop exercises, or actual hazard/casualty exercises. Additionally, the verification process should be performed by knowledgeable individuals who were not part of the formulation of the control to assure an unbiased assessment of the effectiveness of the control. In addition, the control should be formulated so that it is easily and readily verifiable through appropriate and ongoing testing, examination, or surveillance activities. Periodic re-verification that SACs are performing, or capable of performing, their intended

safety function should be addressed through LCOs, SRs for SACs written as LCOs, or through facility operations and maintenance procedures if the SAC is incorporated into the AC section of the TSRs.

f. Discuss how SACs are implemented and maintained.

SACs are generally procedures. These procedures should include specifications for implementation such as qualifications of involved personnel, steps involved, verification of identified limits, frequency of verification, requirements for any independent verifications, interfaces with measuring equipment, the required accuracy of the equipment, etc. TSRs are the formal requirements that implement those procedures and recovery actions in the case of breakdown of the control. SACs are addressed through the TSRs generally by two forms as identified below.

1. LCO/SR—SAC TSRs can often be written in the format of an LCO.
2. Directive action SAC—A directive action SAC TSR can be in the administrative controls section of the TSRs.

These are discussed in section 4 of DOE-STD-1186-2004.

g. Describe measures used to ensure the dependability of SACs.

The measures to ensure the dependability of SACs are discussed below.

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

Human actions, either taken in response to an event or taken proactively to establish desired conditions, are subject to errors of omission or commission. Experience shows that ACs are prone to common cause failure. Attributes should be developed and used to improve worker performance in utilizing ACs and should be carefully evaluated for improving the dependability of SACs. DOE Order 5480.19, *Conduct of Operations Requirements for DOE Facilities*, and DOE-STD-1186-2004 provide guidance for improving the dependability of SACs based on the safety function performed by the SAC.

Conduct of Operations

The dependability of all hazard controls, including SACs, is improved by implementing the facility-appropriate sections of the guidelines for conduct of operations provided in DOE Order 5480.19. Proper conduct of operations is a key safety management program and should be addressed in the facility DSA as such. The guidelines in DOE Order 5480.19 form a compendium of good practices and describe key elements of programs that support operations at DOE facilities. These may be applied to improve the dependability of SACs.

Two key elements of a proper conduct of operations program that can improve the dependability of SACs are independent verification and lockouts/tagouts. Detailed guidance is provided in DOE Order 5480.19 for each of these program elements. The following discussion provides guidance relative to improving the dependability of SACs.

Independent Verification

SACs that require operation of components, or verification of components condition or position, should be included in the facility's independent verification program. As such, these verifications should be identified explicitly in facility procedures or other official documents.

Lockouts and Tagouts

A lockout/tagout program as described in DOE Order 5480.19 should be used to support implementation of SACs where the SACs require that equipment, components, or equipment controls be placed in a specific position or condition during operations to support the safety basis. Use of this program to support an SAC further ensures that the requirements of the SAC are implemented using detailed administrative procedures, training of personnel, and uniquely identifiable tags.

Instrumentation, Controls and Support Equipment for SACs

Operators often must rely on effective instrumentation and controls and support equipment to implement SACs. For this reason, instrumentation and controls and equipment that support a SAC should meet performance requirements consistent with the importance of the safety function of the SAC.

Training and Qualification for SACs

Training requirements for contractor personnel are generally stated under the QA requirements of 10 CFR 830 and in DOE Order 5480.20A, *Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities*. These requirements are applicable to all contractor personnel involved with nuclear facilities, including management and supervisory personnel, technical staff, and operations personnel. As a minimum, hazard analysts, personnel involved with formulation of SACs, and TSR writers should receive training on the guidance of DOE-STD-1186-2004. Training on TSRs for operations personnel should include specific training on attributes of the SACs as identified in the safety basis. Training should also include training on the implementing procedures for SACs.

Establishing a Safety Culture

There are many aspects, both organizationally and operationally, to establishing a safety culture in facilities involving hazardous operations. The Institute of Nuclear Power Operations (INPO) *Excellence in Human Performance Initiative 2001* identified the key principles in developing an appropriate safety culture to improve human performance.

h. Discuss SAC violation reporting requirements.

Violations of SACs in the TSRs must be reported to DOE in accordance with DOE O 231.1A*, Environment, Safety, and Health Reporting*, and DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*.

DOE G 231.1-2, *Occurrence Reporting Causal Analysis Guide*, provides guidance on how to determine the apparent cause(s) of specific reportable occurrences, including TSR violations,

and to explain the structure and nodes of the causal analysis tree for use in occurrence reporting and failure analysis.

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

TSR violations, including SAC violations, that may occur during operation of the facility, must be investigated to determine their specific or generic cause(s) and generic implications, corrective actions recommended, and those violations reported to the DOE as required by 10 CFR 830.205, DOE O 231.1A, and DOE M 231.1-2.

MANAGEMENT, ASSESSMENT, AND OVERSIGHT

28. Nuclear safety specialists shall demonstrate a working level knowledge of assessment techniques (such as the planning and use of observations, interviews, and document reviews) to assess facility performance, report results of assessments, and follow up on actions taken as the result of assessments.

a. Describe the role of NSSs in the assessment of Government-Owned, Contractor-Operated (GOCO) facilities.

The following is taken from DOE-STD-1183-2007.

Role of NSSs

- Oversee implementation of nuclear safety requirements and programs, including
  - Participate in the oversight of contractor implementation of the Nuclear Safety Management Rule (10 CFR 830, subpart B) e.g., preparation, review, and/or recommendation for approval of nuclear safety documents: DSAs, TSRs, USQs, and SERs. Oversight also includes assessments of the contractor's procedures and program documents that implement the requirements of 10 CFR 830, subpart B.
  - Evaluate implementation of ISM: identification, surveillance, and maintenance of SSCs, safety-related QA, selection and implementation of safety-related standards, and related nuclear safety management programs.
  - Evaluate the nuclear safety of nuclear facilities and operations for PAAA compliance, contract performance, operational readiness reviews, readiness assessments, and other periodic assessments. Participate in enforcement of PAAA requirements.
  - Participate in nuclear facility design reviews and safety system status monitoring.

- Evaluate design and analysis uncertainties with the functionalities of systems as described in the DSA.

- Communicate nuclear safety issues to DOE and contractor management and other stakeholders and assist in the resolution these issues.
- Participate in the development, review, approval, and interpretation of nuclear safety rules, Orders, policies, standards, guides, and documents.
- Participate in DOE self-assessments in the area of nuclear safety.
- Participate in nuclear facility accident/incident investigations.
- Participate in emergency response activities.
- Maintain and increase professional knowledge and expertise related to the field of nuclear safety.
- With respect to independent assessment, especially performance based, the NSS is an SME for the safety basis. This is the area (and areas related to 10 CFR 830 implementation) where the NSS contributes most effectively to an assessment program.

b. Describe the assessment requirements and limitations associated with the interface with contractor employees.

The following is taken from NNSA/Service Center, Environment, Safety and Health Department, *Assessment Handbook*, June 2006.

The assessor must be independent of the particular area being assessed with respect to the contractor. The assessor must not have a vested interest in the outcome of an assessment with respect to his or her area of the assessment.

The assessor has no line management oversight over the contractor and particular assessment area and is not in any way a supervisor over those contractors with whom he/she interfaces during the course of the assessment. If a contractor fails to give the assessor information or documents requested, the issue should be turned over to the team leader who will then "interface" with appropriate DOE/NNSA line management and their contractor counterparts.

The assessment results are a government work product. Aside from the contractor response during factual accuracy processing, the results are not subject to negotiation by the contractor.

c. Discuss the essential elements of a performance-based assessment including:
- **Investigation**
- **Fact finding**
- **Exit interview**
- **Reporting**
- **Follow-up**
- **Closure**

The following is taken from DOE G 414.1-1B.

Investigation

An investigation is an examination or inquiry into something, especially a detailed one that is undertaken officially, or the act of undertaking an examination. Its purpose is to collect facts that, when taken as a coherent whole, enable the assessor to come to a conclusion.

The assessment itself is an investigation. The assessor's responsibilities within an assessment should include the following, according to DOE G 414.1-2A:

- Evaluate work performance and process effectiveness.
- Evaluate quality of work products.
- Evaluate compliance with management system requirements.
- Identify abnormal performance and potential problems.
- Identify opportunities for improvement.
- Document and report results.

Fact Finding

This is a process leading toward a goal—collection and analysis of relevant facts. DOE G 414.1-1B reports five basic techniques for fact finding. The guide refers to these five techniques as independent assessment techniques:

1. Document review
2. Interviews
3. Observations
4. Inspections
5. Performance testing

Inspections are performed to verify the adequacy and condition of physical facilities, systems, equipment, and components. Usually, inspections are used to obtain additional information concerning other items evaluated during the assessment, such as equipment labeling, configuration control, the status of system lineups, adequacy of construction, or material storage. Inspections may also be performed to gain information and data for interviews and/or work observation. While on these inspections, the assessor must heed all security and safety requirements. It is always a good practice to be accompanied by someone familiar with the facility.

Performance testing is used to observe the response of personnel or equipment by creating a specific situation and noting performance. This technique is especially useful when activities of interest would not normally occur during an assessment visit. It is also used when timeliness and appropriateness of the response are critical to an organization (e.g., emergency responses).

Exit Interview

This meeting is used primarily by the assessment team to present the assessment summary. Reasonable time should be allowed to discuss any concerns, but this meeting should not be used to argue the assessment findings or methodology. There should be no surprises during

the exit meeting since the assessment team should have taken every effort possible during the conduct of the assessment to ensure that the assessed organization was aware of the team's findings and concerns. Prior to the exit meeting the assessment team should consider combining related findings into a small number of well-supported findings to help focus management's opportunities for improvement.

Reporting

Assessment reports are required for documentation of assessment results. Assessment team leaders have the overall responsibility for preparing the report and obtaining appropriate approval for its release as applicable. The report may be formal (e.g., distributed by memorandum) or informal (e.g., letter to file or email), depending on the level of assessment performed, but should provide a clear picture of the results in terms of the programs, systems, and processes assessed. The assessment report should be clear, concise, accurate, and easy to understand, and should include only facts that directly relate to assessment observations and results. It should include sufficient information to enable the assessed organization to develop and implement appropriate improvement plans.

Follow-Up

A follow-up assessment with special focus may be performed and should be completed in accordance with applicable corrective action documents. Particularly, this follow-up assessment should evaluate the effectiveness of corrective actions. A reasonable subset of corrective actions should be reviewed for effectiveness.

Closure

DOE O 425.1C, *Startup and Restart of Nuclear Facilities,* and DOE-STD-3006-2000, *Planning and Conduct of Operational Readiness Reviews (ORR),* give some information regarding closure of findings. All assessments have results that may include findings that must be addressed by the contractor. Once the final report of the assessment has been submitted and follow-up of the corrective actions has occurred, the DOE mechanism for closure of findings includes the following:

- Development of plans of action approved by DOE to correct the findings. Action plans must provide evaluation of any overall programmatic deficiencies and root causes.
- Documentation of completion of actions responding to the findings in a closure package. Closure packages must include a brief description of actual corrective actions taken and reasons for concluding that closure has been achieved.
- DOE verification of closure of pre-start findings (for some assessments this may require closure of all findings). The organization verifying the closure will be designated by the authorization authority (usually DOE).

Some assessments require lessons learned to be addressed in the final report to be used by DOE and the contractor to improve the assessment process. Lessons learned provide information concerning problems encountered by the review team, adequacies or inadequacies concerning the review, design and implementation, expertise, or any other relevant factors or information that may be used by future review teams.

d. Describe the following assessment methods and the advantages or limitations of each method:
- **Document review**
- **Observation**
- **Interview**

The following is taken from DOE G 414.1-1B.

Document Review

Document reviews provide the objective evidence to substantiate compliance with applicable requirements. A drawback is that the accuracy of the records cannot be ascertained by review alone. This technique should be combined with interviews, observation, inspection, and/or performance testing to complete the performance picture. Records and documents should be selected carefully to ensure that they adequately characterize the program, system, or process being assessed.

Observation

Observation, the viewing of actual work activities, is often considered the most effective technique for determining whether performance is in accordance with requirements. Assessors should understand the effect their presence has on the person being observed and convey an attitude that is helpful, constructive, positive, and unbiased. The primary goal during observation is to obtain the most complete picture possible of the performance, which should then be put into perspective relative to the overall program, system, or process.

Interview

Interviews provide the means of verifying the results of observation, document review, inspection, and performance testing; allow the responsible person to explain and clarify those results; help to eliminate misunderstandings about program implementation; and provide a venue where apparent conflicts or recent changes can be discussed and organization and program expectations can be described.

e. Describe the action to be taken if the contractor challenges the assessment findings, and explain how such challenges can be avoided.

The following is taken from NNSA/Service Center Environment, Safety, and Health Department, *Assessment Handbook*, June 2006.

All reports of assessment results must be reviewed for factual accuracy. The contractor being assessed must concur that the reported results are factual, or detailed objective evidence must be assembled to provide indisputable evidence that reported information is factual. Factual accuracy review can be performed in parallel with assessment performance, or a period of time following completion of the data-gathering portion of the assessment may be allotted to the contractor to provide formal comments. Comments should be restricted to those of a technical nature. The contractor being assessed must provide documented objective evidence to address discrepancies documented within the report. Inclusion of a disputed non-discrepancy within the report is solely at the discretion of the Team Leader. It is very

important that the review plan identify the process to be used for factual accuracy verification, and that the process is clearly understood by the contractor and site office. Failure to adequately verify factual accuracy of information contained within the final report often results in corrective action weaknesses, and greatly reduces the effectiveness of any type of assessment.

Since the goal of any assessment is to identify and implement actions to improve the assessed activity, the contractor being assessed must fully understand any identified problems, and must agree that the problem identification was based upon valid information. It is not necessary that the assessed contractor agree that the problem identified is valid, since requiring this agreement can result in contentious relations between the contractor and the team.

29. Nuclear safety specialists shall demonstrate a working level knowledge of the DOE facility contract provisions necessary to provide oversight of a contractor's operations.

a. Describe the role of NSSs in contractor oversight.

The following is taken from 10 CFR 830 and DOE-STD-1183-2007.

In general, an NSS, as a representative of a DOE/NNSA site office's line management, is to ensure that

- government nuclear facilities are operated safely and efficiently;
- the M&O management system is effectively controlling its conduct of operations (within the NSS's area of expertise);
- effective lines of communication between the DOE/NNSA site office and the M&O are maintained regarding operational matters within the NSS's area of expertise.

The NSS role is to ensure that the site contractor has developed an up-to-date, comprehensive, compliant, documented nuclear facility safety basis and associated implementing mechanisms and procedures for all required nuclear facilities and activities pursuant to 10 CFR 830, subpart B.

The NSS should determine whether or not the following elements have been incorporated into the contractor's safety basis:

- Requirements for developing and implementing a nuclear facility safety basis are included in contract documents and include all applicable requirements in 10 CFR 830, subpart B
- Identification and categorization of all nuclear facilities and activities (category 1, category 2, category 3, and below hazard category 3) per 10 CFR 830, subpart B, using the current version of DOE-STD-1027-92
- Preparation of an authorization agreement that identifies all nuclear facilities/activities and the approved safety basis for these facilities/activities and its submittal to the appropriate DOE/NNSA site office

- Preparation and submission for approval of a DSA for each nuclear facility/activity that complies with the requirements of 10 CFR 830, subpart B
- Preparation and submission for approval of TSRs for each nuclear facility/activity that complies with the requirements of 10 CFR 830, subpart B
- Submission of a compliant USQ process that meets the requirements of 10 CFR 830, subpart B
- The contractor has a process in place to develop a DSA for each nuclear facility/activity that complies with the requirements of 10 CFR 830, subpart B, and DOE/NNSA-directed standards
- A process in place to ensure safety basis documentation is updated in accordance with the requirements of 10 CFR 830, subpart B and NNSA-directives and standards

b. Compare and contrast the following:
- **DOE's expectations of a contractor**
- **A contractor's expectations of the DOE**

The following is taken from 10 CFR 830 and DOE-STD-1183-2007.

DOE's Expectations of a Contractor

The M&O contractor's statement of work and supporting documentation (e.g., work smart standards, etc.) will convey the mutual agreement between DOE and the M&O.

DOE expectations are furthermore communicated by means of a performance evaluation plan (PEP) or similar document. PEPs should delineate clearly and communicate effectively appropriate milestones and performance objectives for upcoming rating periods. The award-fee criteria for each contract must reflect DOE's objectives, priorities, and focused initiatives. The criteria must be meaningful and must contain challenging objectives that are prioritized and weighted in importance as appropriate. Goals and objectives that result from the corrective action plans of various assessments, investigations, etc., must be incorporated into the award-fee criteria.

A Contractor's Expectations of the DOE

The M&O contractor's statement of work and supporting documentation (e.g., work smart standards, etc.) will convey the mutual agreement between DOE and the M&O.

c. Identify the key elements and features of an effective DOE and contractor relationship.

The following is from DOE Order 5480.19.

An effective relationship between DOE/NNSA and the M&O contractor should be based on the site's conduct of operations. An effective DOE/NNSA and M&O contractor relationship should incorporate the following key elements:
- High operating standards established in writing by M&O management through effective implementation and control of operations activities
- Communication of those operating standards to the working levels

- Sufficient resources provided to operations
- Guarantee that personnel at all levels are well trained according to the requirements of their duties
- Close monitoring of performance in operations—i.e., performance assessments
- Accountability of workers and supervisors for performance in conducting duties and responsibilities

d. Describe the responsibility NSSs have associated with contractor compliance under the Price-Anderson Amendments Act.

The following is taken from 10 CFR 820 and DOE-STD-1183-2007.

The PAAA of 1988 added section 234A to the AEA to give DOE the authority to assess civil penalties for violations of rules, regulations, or Orders that related to nuclear safety by contractors and subcontractors who are indemnified by DOE pursuant to the AEA, section 170.

Any risks that are indemnified are not considered as risk to the contractor. The net result of the PAAA is to provide for greater accountability of contractors, subcontractors, and suppliers in the performance of their duties under contract with DOE for indemnified nuclear activities. The availability and careful exercise of this authority by DOE management and its SME professionals can reduce the likelihood of serious nuclear incidents. For the contractor, there are opportunities as well to identify improvements to existing operations and facilities, and modifications in practices that can improve the health and safety of workers, the public, and the environment.

To achieve the above the NSS should

- provide oversight and direction to the M&O contractor for the development and approval of the safety basis for nuclear facilities under the cognizance of the contractor,
- monitor M&O contractor conformance with required regulations, DOE Orders, standards, etc., pursuant to agreements in the DOE-M&O contract,
- identify potential PAAA non-compliance actions and activities to one's supervisor and/or the PAAA coordinator,
- assist in determinations of the M&O contractor's liability and penalty (civil and/or criminal) for a PAAA-relevant violation.

e. Describe the role of NSSs in the cost-plus-award fee process.

The following is taken from 48 CFR 916 and DOE-STD-1183-2007.

A cost-plus-award-fee contract is a cost-reimbursement contract that provides for a fee consisting of a base amount fixed at inception of the contract and an award amount that the contractor may earn in whole or in part during performance and that is sufficient to provide motivation for excellence in such areas as quality, timeliness, technical ingenuity, and cost-effective management. The amount of the award fee to be paid is determined by the

government's judgmental evaluation of the contractor's performance in terms of the criteria stated in the contract. This determination and the methodology for determining the award fee are unilateral decisions made solely at the discretion of the government.

The cost-plus-award-fee contract is suitable for use when

- the work to be performed is such that it is neither feasible nor effective to devise predetermined, objective incentive targets applicable to cost, technical performance, or schedule;
- the likelihood of meeting acquisition objectives will be enhanced by using a contract that effectively motivates the contractor toward exceptional performance and provides the government with the flexibility to evaluate both actual performance and the conditions under which it was achieved;
- any additional administrative effort and cost required to monitor and evaluate performance are justified by the expected benefits.

The number of evaluation criteria and the requirements they represent will differ widely among contracts. The criteria and rating plan should motivate the contractor to improve performance in the areas rated, but not at the expense of at least minimum acceptable performance in all other areas.

Cost-plus-award-fee contracts should provide for evaluation at stated intervals during performance so that the contractor will periodically be informed of the quality of its performance and the areas in which improvement is expected. Partial payment of the fee should generally correspond to the evaluation periods. This makes effective the incentive that the award fee can create by inducing the contractor to improve poor performance or to continue good performance. The advantage to the contractor is monetary in nature. The disadvantage to the contractor is that the award fee amount is subject to a judgmental evaluation by the purchasing organization. The contractor faces the possibility of earning a reduced award fee or no award fee if the contractor's performance ranges from marginal to unacceptable. The advantage to DOE is that the contractor is more motivated to perform well. The disadvantage to DOE is increased cost if the award is actually earned.

Basically, the NSS should assist the contracting officer and the contracting officer's representative in evaluating the contractor's safety programs—vis-à-vis nuclear safety—for the cost-plus-award-fee process. This role should help ensure that

- competitive sources are solicited, evaluated, and selected;
- quality standards are prescribed and met;
- performance and delivery are timely;
- prices, estimated costs, and fees are reasonable;
- files are documented to substantiate the judgments, decisions, and actions taken.

f. Explain the responsibilities of NSSs for DOE O 442.1A, Department of Energy Employee Concerns Program, and the identification, reporting, reviewing, and documentation of employee concerns.

The NSS should

- support the effective implementation of the DOE Employee Concerns Program;
- assist line management in the resolution of employee concerns in a manner that protects the health and safety of employees and the public and ensures the effective and efficient operation of DOE/NNSA-related activities under the NSS's cognizance;
- report concerns related to environment, safety, and health to one's supervisor and/or the appropriate NNSA site office manager or official;
- assist in assessments used to verify that corrective actions as applicable and pursuant to an employee's concerns minimize, correct, or prevent the recurrence of the situation that precipitated an employee's valid concern.

g. Describe the differing professional opinions process used in your office.

Element g is site specific. The local Qualifying Official will evaluate its completion.

30. Nuclear safety specialists shall demonstrate a familiarity level knowledge of problem analysis principles and the techniques necessary to identify problems, potential causes, and corrective action(s) associated with nuclear safety issues at DOE nuclear facilities.

a. Describe and explain the application of problem analysis techniques, including the following:
- **Root cause analysis**
- **Causal factor analysis**
- **Change analysis**
- **Barrier analysis**
- **Management oversight risk tree analysis**

The following is taken from DOE-NE-STD-1004-94.

Root Cause Analysis

DOE O 225.1A, *Accident Investigations,* defines "root cause" as the causal factor(s) that, if corrected, would prevent recurrence of the accident. DOE G 225.1A-1, *Implementation Guide for Use with DOE O 225.1A, Accident Investigations,* states that a root cause analysis should be conducted for each accident investigation. The methodology used is not as important as the results.

Causal Factor Analysis

DOE G 433.1-1, *Nuclear Facility Maintenance Management Program Guide for Use with DOE O 433.1*, states that causal factor charting uses a block diagram to depict cause and effect. This technique is most effective for solving complicated problems because it provides a means to organize the data, provides a concise summary of what is known and unknown about the event, and results in a detailed sequence of facts and activities. The first block on the chart is the primary effect. For each effect, there is a cause that becomes the effect in the next block to the right. For each cause (effect), two reasons that are known to be true are listed in a block just below the cause (effect). If only one reason is known or the reason is uncertain, then all possible causes should be evaluated as potential causes. When this process

gets to the point where a cause can be corrected to prevent recurrence of the event, the root cause has been found.

Change Analysis

Change analysis is used when the problem is obvious. It is generally used for a single event and looks at a problem by analyzing the discrepancy between what is expected and what actually happened. The evaluator essentially asks what differences occurred in this task or activity to make its outcome different this time from all other times. This technique consists of asking What? When? Where? Who? How? The answers should provide direction toward answering the root-cause-determination question, Why?

Barrier Analysis

Barrier analysis is a systematic questioning process that can be used when the problem appears to be programmatic. It identifies physical, administrative, and procedural controls, or barriers that should have prevented an event from happening. This technique should be used to assess why existing barriers, both physical and administrative, failed and what additional barriers are needed to prevent recurrence. Secondary questions in this technique ask Why? and How do you know?

Management Oversight Risk Tree Analysis

A management oversight risk tree analysis is used to identify causal factors related to inadequacies in barriers/controls, specific barrier and support functions, and management functions.

DOE G 231.1-2, *Occurrence Reporting Causal Analysis Guide*, and DOE G 225.1A-1, *Implementation Guide for Use with DOE O 225.1, Accident Investigations*, provide detailed descriptions of each technique.

b. Describe the following types of investigations and discuss an example of the application of each:
- **Type A**
- **Type B**

DOE O 225.1A, *Accident Investigations*, states that DOE field elements shall categorize the type of an investigation in accordance with the algorithm in attachment 2 of DOE O 225.1A to determine if a Type A or Type B investigation is required. Categorization of all Type A and Type B accident investigations should be reported in a timely manner to the Office of the Deputy Assistant Secretary for Oversight. Categorization should be made expeditiously, taking into account that timeliness is crucial to conducting an accurate investigation, preserving the accident scene and evidence, and identifying causal factors. A Type A investigation is conducted for the more serious accidents and is appointed and managed by the Office of the Assistant Secretary for Environment, Safety, and Health. A Type B investigation is appointed and managed at the field level. However, the elements of the investigation and the report format are the same.

Type A and Type B accidents reflect similar types of effects, but are distinctly different regarding the severity of these effects. For comparison purposes, those effects are depicted in DOE G 225.1A-1.

There is one area of commonality regarding Type A and Type B investigations—cost estimating. When the cost of an accident is estimated, the methods in DOE G 430.1-1, chapter 15, "Estimating Methods," should be used.

c. Compare and contrast immediate, short term, and long term actions taken as the result of problem identification or an occurrence.

According to DOE G 231.1-2, *Occurrence Reporting Causal Analysis Guide*, corrective actions should be identified to remedy the problem (immediate actions), prevent recurrence of the specific problem (short-term actions), and preclude occurrence of similar problems (long-term actions). INPO has developed a list of error precursors that are useful in preventing events from occurring. These error precursors are listed in attachment 5 of DOE G 231.1-2. It provides extensive information on the development, implementation, and follow-up of corrective action programs. The guidance may be considered and applied using a graded approach based on the significance, criticality, sensitivity, risk, and/or impact of each finding to the mission, safety, and security of the site, the public, and regulatory requirements. The guidance may assist managers and contractors during the course of ongoing work activities, operational events, informal and formal individual and organizational self-assessments, internal and external oversight, investigations, regulatory actions, audits, inspections, worker safety concerns, design reviews, analyses, and other types of incidents or assessments.

d. Given a nuclear safety event and/or occurrence data, apply problem analysis techniques and identify the problems and how they might have been avoided.

Element d is performance based. The Qualifying Official will evaluate its completion.

e. Describe various data gathering techniques and the use of trending/history when analyzing problems.

The processes found in DOE Order 5480.26 are identified in three main categories. These are performance indicators (PIs), trending and analysis, and reportable performance indicators. Each category is discussed below, as found in the Order.

Performance Indicators

For all DOE facilities included in the DOE PI program, contractors shall provide their PI report addressing the specified list of PIs, provided in DOE Order 5480.26, to the cognizant PSO, through the cognizant field organization, on a quarterly basis. For those facilities identified in appendix 1 of DOE-STD-1048-92, which do not report to a field office, their quarterly report should be sent directly to the cognizant PSO.

Departmental elements not included in the formal DOE PI Program shall internally establish and track operations using PIs appropriate to their organizations but are excluded from formal reporting requirements defined in DOE-STD-1048-92.

PIs are designed to be reportable as numerical values on a consistent basis so that they are readily usable in trending analysis. For each facility included in the DOE PI program, the contractor shall gather, analyze, and report the PI data, including narrative data, according to the requirements of DOE Order 5480.26 and the guidance provided in DOE-STD-1048-92.

The contractor, field office, and PSO quarterly performance indicator reports shall follow the format and content provided in DOE-STD-1048-92.

The detailed schedule for submittal of PI data and all quarterly PI reports is provided in DOE-STD-1048-92.

Trending and Analysis

Contractors for each facility, group of facilities, or site shall review and assess their PIs and other operations information, such as reportable occurrences.

Facility managers shall assess their facility operating information for trends and indications of deteriorating/improving conditions and identify lessons-learned and good practices that should be used in their facilities to prevent occurrences or to improve safety and/or operations.

Each level of DOE line management shall adopt the use of trending and analysis of PIs and other operations information, such as reportable occurrences, at all levels of operations to provide ongoing feedback to operators, support personnel, and managers of the condition and performance of their operations with the intent of identifying deficiencies/good practices and opportunities for improvement in safety and performance of their operations.

Reportable Performance Indicators

The PIs delineated in DOE-STD-1048-92 are the minimum required to be reported for each facility. For some facilities, certain information may not be applicable and, therefore, need not be reported. However, the report should so indicate. It is also expected that DOE line management may request additional PIs to be reported which they may determine to be relevant to their facilities.

Detailed definitions and information concerning these PIs can be found in DOE-STD-1048-92.

31. Nuclear safety specialists shall demonstrate a familiarity level knowledge of DOE Policy 450.4, Safety Management System Policy; Policy 226.1A, Department of Energy Oversight Policy; and DOE O 226.1, Implementation of Department of Energy Oversight Policy, as applied to nuclear safety.

a. Discuss the fundamentals of ISM and its direct application to nuclear safety.

The following is taken from DOE P 450.4.

The Department is committed to conducting work efficiently and in a manner that ensures protection of workers, the public, and the environment. It is Department policy that safety management systems described herein shall be used to systematically integrate safety into management and work practices at all levels so that missions are accomplished while protecting the public, the worker, and the environment. Direct involvement of workers during the development and implementation of safety management systems is essential for their success.

The DOE ISMS establishes a hierarchy of components to facilitate the orderly development and implementation of safety management throughout the DOE complex. The safety management system consists of six components: (1) the objective, (2) guiding principles, (3) core functions, (4) mechanisms, (5) responsibilities, and (6) implementation. The objective, guiding principles, and core functions of safety management identified below shall be used consistently in implementing safety management throughout the DOE complex. The mechanisms, responsibilities, and implementation components are established for all work and will vary based on the nature and hazard of the work being performed.

Component 1—Objective of Integrated Safety Management

The Department and contractors must systematically integrate safety into management and work practices at all levels so that missions are accomplished while protecting the public, the worker, and the environment. This is to be accomplished through effective integration of safety management into all facets of work planning and execution. In other words, the overall management of safety functions and activities becomes an integral part of mission accomplishment.

Component 2—Guiding Principles for Integrated Safety Management

The guiding principles are the fundamental policies that guide Department and contractor actions, from development of safety directives to performance of work.

Line Management Responsibility for Safety—Line management is directly responsible for the protection of the public, the workers, and the environment. As a complement to line management, the Department's Office of Environment, Safety, and Health provides safety policy, enforcement, and independent oversight functions.

Clear Roles and Responsibilities—Clear and unambiguous lines of authority and responsibility for ensuring safety shall be established and maintained at all organizational levels within the Department and its contractors.

Competence Commensurate with Responsibilities—Personnel shall possess the experience, knowledge, skills, and abilities that are necessary to discharge their responsibilities.

Balanced Priorities—Resources shall be effectively allocated to address safety, programmatic, and operational considerations. Protecting the public, the workers, and the environment shall be a priority whenever activities are planned and performed.

Identification of Safety Standards and Requirements—Before work is performed, the associated hazards shall be evaluated, and an agreed-upon set of safety standards and requirements shall be established which, if properly implemented, will provide adequate assurance that the public, the workers, and the environment are protected from adverse consequences.

Hazard Controls Tailored to Work Being Performed—Administrative and engineering controls to prevent and mitigate hazards shall be tailored to the work being performed and associated hazards.

For nuclear facilities, the hazard analysis should be based on the direction in 10 CFR 830 for identification of the safety-class and the safety-significant structures, systems, and components. This level of hazard analysis is then used as the foundation for more detailed analysis at the facility level, which in turn is used as the basis for the activity or task level hazard analysis.

DOE has promulgated a number of directives (policies, regulations, orders, notices, standards, and guides) that may be used for hazard analysis and hazard categorization. Such directives, when incorporated into a contract, establish the processes and expectations for contractor performance of hazards analyses. Note that, in addition, DOE has developed proposed regulations that correspond to existing DOE nuclear safety Orders. These proposed rules remain compatible with the ISMS and provide for implementation into ISMSs.

Operations Authorization—The conditions and requirements to be satisfied for operations to be initiated and conducted shall be clearly established and agreed-upon.

Component 3—Core Functions for Integrated Safety Management

These five core safety management functions provide the necessary structure for any work activity that could potentially affect the public, the workers, and the environment. The functions are applied as a continuous cycle with the degree of rigor appropriate to address the type of work activity and the hazards involved.

1. Define the Scope of Work—Missions are translated into work, expectations are set, tasks are identified and prioritized, and resources are allocated.
2. Analyze the Hazards—Hazards associated with the work are identified, analyzed, and categorized.
3. Develop and Implement Hazard Controls—Applicable standards and requirements are identified and agreed-upon, controls to prevent/mitigate hazards are identified, the safety envelope is established, and controls are implemented.

4. Perform Work within Controls—Readiness is confirmed, and work is performed safely.
5. Provide Feedback and Continuous Improvement—Feedback information on the adequacy of controls is gathered, opportunities for improving the definition and planning of work are identified and implemented, line and independent oversight is conducted, and, if necessary, regulatory enforcement actions occur.

Component 4—Integrated Safety Management: Mechanisms

Safety mechanisms define how the core safety management functions are performed. The mechanisms may vary from facility to facility and from activity to activity based on the hazards and the work being performed and may include

- departmental expectations expressed through directives (policy, rules, orders, notices, standards, and guidance) and contract clauses
- directives on identifying and analyzing hazards and performing safety analyses
- directives that establish processes to be used in setting safety standards
- contractor policies, procedures, and documents (e.g., health and safety plans, safety analysis reports, chemical hygiene plans, process hazard analyses) established to implement safety management and fulfill commitments made to the Department

Component 5—Responsibilities for Integrated Safety Management

Responsibilities must be clearly defined in documents appropriate to the activity. DOE responsibilities are defined in Department directives. Contractor responsibilities are detailed in contracts, regulations, and contractor-specific procedures. For each management mechanism employed to satisfy a safety management principle or function, the associated approval authority needs to be established. The review and approval levels may vary commensurate with the type of work and the hazards involved.

Component 6—Implementation of Integrated Safety Management

Implementation involves specific instances of work definition and planning, hazard identification and analysis, definition and implementation of hazard controls, performance of work, developing and implementing operating procedures, and monitoring and assessing performance for improvement.

b. Describe the key elements of an effective contractor self-assessment nuclear safety program.

The following is taken from DOE O 226.1A and DOE G 450.4-1B.

A rigorous and credible assessment program is the cornerstone of effective, efficient management of programs such as environment, safety, and health; safeguards and security, cyber security; emergency management; and business processes.

Contractors will be responsible for developing, implementing, and performing comprehensive assessments for all facilities, systems, and organizational elements, including subcontractors, on a recurring basis. The scope and frequency of assessments must be

specified in site plans and program documents and must meet or exceed the requirements of applicable DOE directives. External peers or SMEs may be utilized to support assessment activities.

Self-assessment is used to evaluate performance at all levels periodically and to determine the effectiveness of policies, requirements, and standards and the implementation status.

- Management self-assessments are performed by contractor management, and are developed (scope and review criteria) based on the nature of the facility/activity being assessed and the hazards and risks to be controlled.
- Self-assessments, which focus on hands-on work and the implementation of administrative processes, involve workers, supervisors, and managers to encourage identification and resolution of deficiencies at the lowest level practicable.
- Support organizations will perform self-assessments of their performance and the adequacy of their processes.
- Contractors, at all levels, will assess the implementation and adequacy of their processes, including analysis of the collective results of lower-level self-assessments.
- Self-assessment results will be documented commensurate with the significance of and risks associated with activities being evaluated.

A robust, rigorous, and credible contractor self-assessment program linked to the DOE safety management system includes elements that address the following:

- Performance measures and PIs
- Line and independent evaluations
- Compliance with applicable requirements (rules, regulatory standards, contract terms)
- Data collection, analysis, and corrective actions
- Continuous feedback and performance improvement

c. Discuss the following nuclear safety assessments/surveillance activities:

- **Determination of assessment/surveillance requirements**
- **Operation/area/site office and contractor notification**
- **Assessment/surveillance agenda**

The following is taken from DOE O 226.1A.

Determination of Assessment/Surveillance Requirements

DOE line management must establish and implement assessment programs to determine contractor compliance with requirements. DOE line management assessments will be planned and scheduled based on requirements, analysis of hazards and risks, past performance, and effectiveness of contractor assurance systems for organizations, facilities, operations, and programs. In addition to scheduled assessments, “for cause” reviews will be performed when circumstances warrant (e.g., when events indicate degradation of a system). Assessments will be performed in support of facility startup and restart or review and will review and approve required program documents. Assessments must include reviews of site qualification standard programs, training programs, and individual training and qualifications as they relate to environment, safety, and health.

Operation/Area/Site Office and Contractor Notification

Assessment results, including findings, must be documented and provided to the contractor for timely resolution. Deficiencies identified by DOE assessments or other DOE reviews must be addressed in a structured issues management process. DOE verifies that contractor corrective actions are complete and effective in addressing deficiencies before they are closed out in the issues management system. DOE line management must maintain a baseline assessment program that provides assurance that DOE managers have an accurate picture of the status and effectiveness of site programs and that deficiencies are identified in a timely manner.

Assessment/Surveillance Agenda

DOE oversight programs and assurance systems will evaluate performance against requirements and performance objectives, including laws, regulations, national standards, DOE directives, DOE-approved plans and program documents, site-specific procedures/manuals, criteria review and approach documents, other contractually mandated requirements, and contractual performance objectives. Requirements and performance objectives are established and interpreted through approved processes so that they are relevant to the site and mission.

SELECTED BIBLIOGRAPHY AND SUGGESTED READING

Code of Federal Regulations (CFR)

10 CFR 20, "Standards for Protection Against Radiation." January 1, 2008.
10 CFR 50.120, "Training and Qualification of Nuclear Power Plant Personnel," appendix K, "ECCS Evaluation Models." January 1, 2008.
10 CFR 71.71, "Normal Conditions of Transport." January 1, 2008.
10 CFR 820, "Procedural Rules for DOE Nuclear Activities." January 1, 2008.
10 CFR 830, "Nuclear Safety Management." January 1, 2008.
10 CFR 830.3, "Definitions." January 1, 2008.
10 CFR 830.122, "Quality Assurance Criteria." January 1, 2008.
10 CFR 830, subpart B, "Safety Basis Requirements." January 1, 2008.
10 CFR 830.201, "Performance of Work." January 1, 2008.
10 CFR 830.202, "Safety Basis." January 1, 2008.
10 CFR 830.203, "Unreviewed Safety Question Process." January 1, 2008.
10 CFR 830.204, "Documented Safety Analysis." January 1, 2008.
10 CFR 830.205, "Technical Safety Requirements." January 2008.
10 CFR 830.206, "Preliminary Documented Safety Analysis." January 1, 2008.
10 CFR 830.207, "DOE Approval of Safety Basis." January 1, 2008.
10 CFR 835, "Occupational Radiation Protection." January 1, 2008.
10 CFR 835.403, "Air Monitoring." January 1, 2008.
10 CFR 851, "Worker Safety and Health Program." January 1, 2008.
29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals." July 1, 2007.
29 CFR 1910.120, "Hazardous Waste Operations and Emergency Response." July 1, 2007.
29 CFR 1910.1200, "Hazard Communication." July 1, 2007.
29 CFR 1910.1450, "Occupational Exposure to Hazardous Chemicals in Laboratories." July 1, 2007.
29 CFR 1926.65, "Hazardous Waste Operations and Emergency Response." July 1, 2007.
40 CFR 302, "Designation, Reportable Quantities, and Notification." July 1, 2004.
40 CFR 355, "Emergency Planning and Notification," appendix A, "The List of Extremely Hazardous Substances and Their Threshold Planning Quantities." July 1, 2007.
48 CFR 916, "Types of Contracts." October 1, 2007.
48 CFR 970.5223-1, "Integration of Environment, Safety, and Health into Work Planning and Execution." October 1, 2007.
49 CFR 173.469, "Tests for Special Form Class 7 (Radioactive) Materials." October 1, 2007.

American Industrial Hygiene Association. *Emergency Response Planning Guidelines.* 2008.

American Institute of Chemical Engineers. *Guidelines for Hazard Evaluation Procedures*. 1992.

American National Standards Institute (ANSI)/American Nuclear Society (ANS)

ANSI/ANS-8.1-1998, R2007 (R = reaffirmed), *Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors.* 1998.

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

ANSI/ANS-8.5-1996, R2002, R2007, *Use of Borosilicate-Glass Raschig Rings as a Neutron Absorber in Solutions of Fissile Material.* 1996.

ANSI/ANS-8.7-1975, R1982, R1987, W1997 (W=withdrawn), *Guide for Nuclear Criticality Safety in the Storage of Fissile Materials.* 1975.

ANSI/ANS-8.15-1981, R1987, R1995, R2005, *Nuclear Criticality Control of Special Actinide Elements*. 1981.

ANSI/ANS-8.19-2005, *Administrative Practices for Nuclear Criticality Safety*. 2005.

American National Standards Institute (ANSI)

ANSI N43.6, *Sealed Radioactive Source Classification.* 1997.

ANSI N317, *American National Standard Performance Criteria for Instrumentation Used for Inplant Plutonium Monitoring*. 1980.

American Society of Civil Engineers.

ASCE 4-98, *Seismic Analysis of Safety-Related Nuclear Structures and Commentary*. 1998.

ASCE 7-05, *Minimum Design Loads for Buildings and Other Structures*. 2006.

American Society of Heating, Refrigerating, and Air-Conditioning Engineers. ASHRAE/ANSI 62-2001, *Ventilation for Acceptable Indoor Air Quality.* 2001.

American Society of Mechanical Engineers. ASME NQA-1-2004, *Quality Assurance Requirements for Nuclear Facility Applications*. 2004.

Bureau of Radiological Health and the Training Institute, Environmental Control Administration. Washington, D. C.: Government Printing Office. *Radiological Health Handbook*. 1970.

Burton, D. Jeff. *Industrial Ventilation Workbook.* Bountiful, UT: IVE Inc. 2003.

Cember, Herman. *Introduction to Health Physics.* McGraw Hill Companies Inc. 1996.

Executive Order 12699, "Seismic Safety of Federal and Federally Assisted or Regulated New Building Construction." January 5, 1990.

Institute of Electrical and Electronics Engineers. IEEE-Std-603-1991, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.* 1991. This document has been superseded by 603-1998.

International Commission on Radiological Protection (ICRP)

ICRP Publication 26*, Recommendations of the International Commission on Radiological Protection.* 1977. Superseded by ICRP 60.

ICRP Publication 30, *Limits for Intake of Radionuclides by Workers: Part 4 (An Addendum).* 1989.

ICRP Publication 56, *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 1*. 1990.

ICRP Publication 60, *1990 Recommendations of the International Commission on Radiological Protection.* 1991.

ICRP Publication 61, *Annual Limits on Intake of Radionuclides by Workers Based on the 1990 Recommendations*. 1991.

ICRP Publication 66, *Human Respiratory Tract Model for Radiological Protection*. 1995.

ICRP Publication 67, *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 2, Ingestion Dose Coefficients*. 1994.

ICRP Publication 68, *Dose Coefficients for Intakes of Radionuclides by Workers*. 1995.

ICRP Publication 69, *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 3, Ingestion Dose Coefficients*. 1995.

ICRP Publication 71, *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 4, Inhalation Dose Coefficients.* 1996.

ICRP Publication 72, *Age-Dependent Doses to the Members of the Public from Intake of Radionuclides: Part 5, Compilation of Ingestion and Inhalation Coefficients*. 1996.

Knief, Ronald Allen. *Nuclear Criticality Safety: Theory and Practice*. La Grange Park, Illinois: American Nuclear Society. 1998.

Los Alamos National Laboratory (LANL)

LANL Master Specification, Section 11 5311.10, "Glovebox Fabrication." January 6, 2006.

LANL Master Specification, Section 23 3816, "Fume Hoods." January 6, 2006.

LANL SG-ENG-25082, R0 VA, Course Number 25082, Nuclear Science Self-Study Guide. September 2002.

National Aeronautics and Space Administration. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. Ver. 1.1. August 2002.

National Fire Protection Association. NFPA 704, *Standard System for the Identification of the Hazards of Materials for Emergency Response.* 2007.

National Institute for Occupational Safety and Health. *A Comparative Evaluation of the Differential-Pressure-Based Respirable Dust Dosimeter with the Personal Gravimetric Respirable Dust Sampler in Underground Coal Mines*. January 2001.

National Institute for Standards and Technology. NIST Special Report 1026, *CFAST—Consolidated Model of Fire Growth and Smoke Transport, Version 6, Technical Reference Guide.* December 2005.

Terrauniversal.com. http://terrauniversal.com/products/measuring/magphotohelic.php.

U.S. Congress

Atomic Energy Act of 1954.

Comprehensive Environmental Response, Compensation, and Liability Act of 1980.

Price-Anderson Amendments Act of 1988.

U.S. Department of Energy (DOE)

DOE/EH-0173T, *Environmental Regulatory Guide for Radiological Effluent Monitoring and Environmental Surveillance*. 1991.

DOE/EH-0340, *Example Process Hazard Analysis of a Department of Energy Water Chlorination Process.* September 1993.

DOE/EH-0711, *Gap Analysis for IMBA and DOE Safety Software Central Registry Recommendation.* http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/IMBA/IMBAGapAnalysisFinal20060831.pdf. August 2006.

DOE-EH-4.2.1.2-Criteria, *Software Quality Assurance Plan and Criteria for the Safety Analysis Toolbox Codes*, https://hss.energy.gov/CSA/CSP/sqa/central_registry/SQA_Plan_Criteria_113003.pdf. November 2003.

DOE-EH-4.2.1.3-ALOHA-Gap Analysis, *Software Quality Assurance Improvement Plan: ALOHA Gap Analysis.* http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/ALOHA/Final_ALOHA_Gap_Analysis_Report050304.pdf. May 2004.

DOE-EH-4.2.1.3-CFAST-Gap Analysis, *Software Quality Assurance Improvement Plan: CFAST Gap Analysis, http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/CFAST/Final_CFAST_Gap_Analysis_Report050304.pdf.* May 2004.

DOE-EH-4.2.1.3-EPIcode-Gap Analysis, *Software Quality Assurance Improvement Plan: EPIcode Gap Analysis,* http://www.hss.energy.gov/csa/csp/sqa/central_registry/EPICode/Final_EPICode_Gap_Analysis_Report050304.pdf. May 2004.

DOE-EH-4.2.1.3-GENII-Gap Analysis, *Software Quality Assurance Improvement Plan: GENII Gap Analysis*, http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/Genii/Final_GENll_Gap_Analysis_Report050304.pdf. May 2004.

DOE-EH-4.2.1.3-MACCS2-Gap Analysis, *Software Quality Assurance Improvement Plan: MACCS2 Gap Analysis,* http://www.hss.energy.gov/csa/csp/sqa/central_registry/MACCS2/Final_MACCS2_Gap_Analysis_Report050304.pdf. May 2004.

DOE-EH-4.2.1.3-MELCOR-Gap Analysis, *Software Quality Assurance Improvement Plan: MELCOR Gap Analysis,* http://www.hss.energy.gov/CSA/CSP/sqa/central_registry/MELCOR/Final_MELCOR_Gap_Analysis_Report050304.pdf. May 2004.

DOE/EIS-0120, *Final Environmental Impact Statement, Wetland Assessment for the F- and H-Area Groundwater Remediation Project at the Savannah River Site.* March 2004.

Energy Efficiency and Renewable Energy. *A Consumer's Guide to Energy Efficiency and Renewable Energy. Whole-House Supply Ventilation Systems.* September 19, 2005.
National Nuclear Security Administration. Service Center. Environment, Safety and Health Department. *Assessment Handbook*. June 2006.
Office of Health, Safety, and Security. Protective Action Criteria (PAC) with AEGLs, ERPGs, & TEELs: Rev. 23 for Chemicals of Concern Web site. August 2007.
Safety Analysis Software Group. Technical Report, *Selection of Computer Codes for DOE Safety Analysis Applications*. August 2002.

U.S. Department of Energy Directives (Guides, Manuals, Notices, Orders, Policies, and Secretary of Energy Notices)

DOE Guide 200.1-1, *Software Engineering Methodology,* chap. 4*, "*Requirements Definition Stage*."* May 21, 1997.
DOE Guide 225.1A-1, *Implementation Guide for Use with DOE O 225.1, Accident Investigations.* November 26, 1997.
DOE Guide 231.1-2*, Occurrence Reporting Causal Analysis Guide.* August 20, 2003.
DOE Guide 414.1-1B, *Management and Independent Assessments Guide for Use with 10 CFR, Part 830, Subpart A, and DOE O 414.1C, Quality Assurance; DOE M 450.4-1, Integrated Safety Management System Manual; and DOE O 226.1A, Implementation of Department of Energy Oversight Policy.* September 27, 2007.
DOE Guide 414.1-2A, *Quality Assurance Management System Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance.* June 17, 2005.
DOE Guide 414.1-4, *Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance.* June 17, 2005.
DOE Guide 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE O 420.1, Facility Safety.* March 28, 2000.
DOE Guide 420.1-2, *Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Nonnuclear Facilities.* March 28, 2000.
DOE Guide 420.1-3, *Implementation Guide for DOE Fire Protection and Emergency Services Programs for Use with DOE O 420.1B, Facility Safety.* September 27, 2007.
DOE Guide 421.1-X draft, *Accident Analysis Guidebook for Interim Use and Comment.* 2003.
DOE Guide 421.1-1, *DOE Good Practices Guide: Criticality Safety Good Practices Program Guide for DOE Nonreactor Nuclear Facilities.* August 25, 1999.
DOE Guide 421.1-2, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830.* October 24, 2001.
DOE Guide 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements.* October 24, 2001.
DOE Guide 424.1-1A, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements.* July 24, 2006.
DOE Guide 430.1-1, (*Cost Estimating Guide)*, *Chapter 15, Estimating Methods*. March 28, 1997.
DOE Guide 433.1-1, *Nuclear Facility Maintenance Management Program Guide for Use with DOE O 433.1.* September 5, 2001.

DOE Guide 440.1-8, *Implementation Guide for Use with 10 CFR 851, Worker Safety and Health Program.* December 27, 2006.
DOE Guide 450.4-1B, *Integrated Safety Management System Guide*. Vol. 1 and 2. March 1, 2001.
DOE Guide 460.1-1, *Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety*. June 5, 1997.

DOE Manual 231.1-2, *Occurrence Reporting and Processing of Operations Information*. August 19, 2003.
DOE Manual 411.1-1C, *Safety Management Functions, Responsibilities, and Authorities Manual*. December 31, 2003.
DOE Manual 461.1-1, *Packaging and Transfer of Materials of National Security Interest Manual.* July 26, 2005.

DOE Notice 5400.9, *Sealed Radioactive Source Accountability.* December 24, 1991.

DOE Order 225.1A, *Accident Investigations*. November 26, 1997.
DOE Order 226.1A, *Implementation of Department of Energy Oversight Policy*. July 31, 2007.
DOE Order 231.1A, *Environment, Safety, and Health Reporting.* June 3, 2004.
DOE Order 413.3A, *Program and Project Management for the Acquisition of Capital Assets.* July 28, 2006.
DOE Order 414.1C, *Quality Assurance*. June 17, 2005.
DOE Order 420.1B, *Facility Safety*. December 22, 2005.
DOE Order 425.1C, *Startup and Restart of Nuclear Facilities.* March 13, 2003.
DOE Order 440.1B, *Worker Protection Program for DOE (Including the National Nuclear Security Administration) Federal Employees*. May 17, 2007.
DOE Order 442.1A, *Department of Energy Employee Concerns Program*. June 6, 2001.
DOE Order 460.1B, *Packaging and Transportation Safety*. April 4, 2003.
DOE Order 461.1A, *Packaging and Transfer or Transportation of Materials of National Security Interest*. April 26, 2004.
DOE Order 5400.5, *Radiation Protection of the Public and the Environment*. January 7, 1993.
DOE Order 5480.19, *Conduct of Operations for DOE Nuclear Facilities*. October 23, 2001.
DOE Order 5480.20A, *Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities.* July 12, 2001.
DOE Order 5480.22, *Technical Safety Requirements*. January 23, 1996. (Archive)
DOE Order 5480.23, *Nuclear Safety Analysis Reports*. March 10, 1994. (Archive)
DOE Order 5480.26, *Trending and Analysis of Operations Information Using Performance Indicators.* January 15, 1993. (Archive)
DOE Order 5480.30, *Nuclear Reactor Safety Design Criteria*. March 14, 2001.

DOE Policy 226.1A, *Department of Energy Oversight Policy.* May 25, 2007.
DOE Policy 450.4, *Safety Management System Policy*. October 15, 1996.

DOE Secretary of Energy Notice SEN-35-91, *Nuclear Safety Policy.* September 9, 1991.

U.S. Department of Energy Handbooks and Standards

DOE HDBK-1011/1 [through 4] -92, *DOE Fundamentals Handbook: Electrical Science*. Vol. 1 through 4. June 1992.

DOE-HDBK-1013/1 [and 2] -92, *DOE Fundamentals Handbook: Instrumentation and Control*. Vol. 1 and 2. June 1992.

DOE-HDBK-1014/2-92, *DOE Fundamentals Handbook: Mathematics*. Vol. 2. June 1992.

DOE-HDBK-1016/1 [and 2] -93, *DOE Fundamentals Handbook: Engineering Symbology, Prints, and Drawings*. Vol. 1 and 2. January 1993.

DOE-HDBK-1019/1 [and 2] -93, *DOE Fundamentals Handbook: Nuclear Physics and Reactor Theory*. Vol. 1 and 2. January 1993.

DOE-HDBK-1079-94, *Primer on Tritium Safe Handling Practices*. December 1994.

DOE-HDBK-1085-95, *DOE Enforcement Program Roles and Responsibilities*. August 1995.

DOE-HDBK-1100-2004, *DOE Handbook: Chemical Process Hazards Analysis*. February 1996.

DOE-HDBK-1101-2004, *DOE Handbook: Process Safety Management for Highly Hazardous Chemicals*. August 2004.

DOE-HDBK-1108-2002, *DOE Handbook: Radiological Safety Training for Accelerator Facilities.* January 2007.

DOE-HDBK-1122-99, *DOE Handbook: Radiological Control Technician Training*. June 1999.

DOE-HDBK-1130-2007, *DOE Handbook: Radiological Worker Training*. February 2005.

DOE-HDBK-1132-99, *DOE Handbook: Design Considerations*. April 1999.

DOE-HDBK-1141-2001, *DOE Handbook: Radiological Assessor Training*. January 2007.

DOE-HDBK-1163-2003, *DOE Handbook: Integration of Multiple Hazard Analysis Requirements and Activities.* October 2003.

DOE-HDBK-1169-2003, *DOE Handbook: Nuclear Air Cleaning Handbook*. November 2003.

DOE-HDBK-3010-94*, DOE Handbook: Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities*. Vol. 1 and 2, December 1994. Vol. 1, change notice 1, March 2000.

DOE-NA-STD-3016-2006, *DOE Limited Standard: Hazard Analysis Reports for Nuclear Explosive Operations*. May 2006.

DOE-STD-1020-2002, *DOE Standard: Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*. January 2002.

DOE-STD-1021-93, *DOE Standard: Natural Phenomena Hazards Performance Categorization Guidelines for Structures, Systems, and Components.* January 1996.

DOE-STD-1022-94, *DOE Standard: Natural Phenomena Hazards Site Characterization Criteria.* January 1996.

DOE-STD-1023-95, *DOE Standard*: *Natural Phenomena Hazards Assessment Criteria.* January 1996.

DOE-STD-1027-92, *DOE Standard: Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports.* September 1997.
DOE-STD-1048-92, *DOE Performance Indicator Guidance Document.* December 1992.
DOE-STD-1098-99, *DOE Standard*: *Radiological Control.* March 2005.
DOE-STD-1104-96, *DOE Standard: Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements).* December 2005.
DOE-STD-1120-2005, *DOE Standard: Integration of Environment, Safety, and Health into Facility Disposition Activities*. Vol. 1 and 2. April 2005.
DOE-STD-1134-99, *DOE Standard*: *Review Guide for Criticality Safety Evaluations.* September 1999.
DOE-STD-1135-99, *DOE Standard: Guidance for Nuclear Criticality Safety Engineer Training and Qualification*. September 1999.
DOE-STD-1158-2002, *DOE Standard: Self-Assessment Standard for DOE Contractor Criticality Safety Programs.* November 2002.
DOE-STD-1172-2003, *DOE Standard: Safety Software Quality Assurance Functional Area Qualification Standard*. December 2003.
DOE-STD-1183-2007, *DOE Standard: Nuclear Safety Specialist Functional Area Qualification Standard*. November 2007.
DOE-STD-1186-2004, *DOE Standard*: *Specific Administrative Controls.* August 2004.
DOE-STD-1189-2008, *DOE Standard*: *Integration of Safety into the Design Process.* March 2008.
DOE-STD-3006-2000, *DOE Standard*: *Planning and Conduct of Operational Readiness Reviews (ORR)*. June 2000.
DOE-STD-3007-2007, *DOE Standard*: *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*. February 2007.
DOE-STD-3009-94, *DOE Standard*: *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. March 2006.
DOE-STD-3011-2002, *DOE Standard: Guidance for Preparation of Basis for Interim Operation (BIO) Documents*. December 2002.
DOE-STD-3014-2006, *DOE Standard: Accident Analysis for Aircraft Crash into Hazardous Facilities*. October 1996.
DOE-STD-3020-2005, *DOE Technical Standard: Specification for HEPA Filters Used by DOE Contractors.* December 2005.

U.S. Department of Health and Human Services. Centers for Disease Control and Prevention. *Acute Radiation Syndrome: A Fact Sheet for Physicians.* March 2005.

U.S. Department of Health, Education, and Welfare. Public Health Service. *Radiological Health Handbook*. Revised edition. January 1970.

U.S. Environmental Protection Agency (EPA)

EPA. *Acute Exposure Guideline Levels*. April 25, 2007.
EPA. Office of Underground Storage Tanks. EPA 510-R-04-002, *How to Evaluate Alternative Cleanup Technologies for Underground Storage Tank Sites: A Guide for*

Corrective Action Plan Reviewers, "Appendix: Abbreviations and Definitions." http://www.epa.gov/OUST/pubs/tum_appx.pdf. May 2004.

EPA. Basic Concepts in Environmental Sciences: Pressure, Web site; Glossary feature. March 1, 2006.

EPA. Federal Guidance Report No. 11, *Limiting Values of Radionuclide Intake and Air Concentration and Dose Conversion Factors for Inhalation, Submersion, and Ingestion*. 1988.

EPA. Federal Guidance Report No. 13, *Cancer Risk Coefficients for Environmental Exposure to Radionuclides*. September 1999.

EPA. Risk Assessment and Modeling—Air Toxics Risk Assessment Reference Library. Vol. 1, *Technical Resource Manual*. Chap. 8, "Quantification of Exposure: Dispersion, Transport, and Fate of Air Toxics in the Atmosphere." April 2004.

EPA. *Technical Guidance for Hazards Analysis: Emergency Planning for Extremely Hazardous Substances.* December 1987.

U.S. Nuclear Regulatory Commission (NRC)

NRC. NUREG/CR-6751, *The Human Performance Evaluation Process: A Resource for Reviewing the Identification and Resolution of Human Performance Problems*. September 2001.

NRC. Regulatory Guide 1.145, *Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants*. February 1983. Available at Agency-wide Documents Access and Management System (NRC ADAMS), accession number ML003740205.

NRC. Regulatory Guide 1.23, *Meteorological Monitoring Programs for Nuclear Power Plants*. March 2007.

NRC. Regulatory Guide 1.7, *Control of Combustible Gas Concentrations in Containment.* March 2007.

NRC. Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports of Nuclear Power Plants*. November 1978. Available at Agency-wide Documents Access and Management System (NRC ADAMS), in 3 parts with accession numbers ML011340072, ML011340108, and ML011340116.

Nuclear Safety Specialist
Qualification Standard
Reference Guide
AUGUST 2008