ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

SYSTEM DESIGN DESCRIPTIONS

Main Category:	Project Management
Sub Category:	-
Course #:	PRJ-121
Course Content:	46 pgs
PDH/CE Hours:	3

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM
TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)
SUPPORT@ENGINEERING-PDH.COM

PRJ-121 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. According to the reference material, SDD data shall be housed in only an approved data system, such as an "enterprise" system (ES) that meets the site's configuration management requirements.
    a. True
    b. False
2. The FDD may be the only document needed for less than Hazard Category _ facilities. For more complex or important systems within a larger facility, the FDD should refer to individual SDDs for more detailed information.
    a. 4
    b. 3
    c. 2
    d. 1
3. According to the reference material, the SDD should collect and provide more detail than would normally be included in safety basis documents but less detail than in engineering design documents.
    a. True
    b. False
4. According to APPENDIX C of the reference material, which of the following codes/standards outlines the guidelines for quality assurance?
    a. 10 CFR part 830
    b. DOE-STD-1189-2008
    c. DOE G 420.1-1
    d. DOE O 414.1D

5. Requirements should be classified with regard to their importance to ensure appropriate consideration in system operation, maintenance, performance evaluations, and evaluation of system changes. According to the hierarchy used in the reference material, which of the requirements ranks 3rd in the list?
    a. General Requirements
    b. Environmental Requirements
    c. Mission-Critical Requirements
    d. Safety Requirements
6. The useful life of the completed SDD should be long enough to make it worth the resources expended to develop the SDD. If the remaining lifetime of the facility is less than ___ years, development of SDDs may not be considered worthwhile.
    a. 5
    b. 10
    c. 15
    d. 20
7. According to the reference material, the manufacturer and model number for components in the current system configuration should be recorded in a controlled document for several reasons including to facilitate identifying the applicable information in vendor-supplied documents.
    a. True
    b. False
8. Field experience in both the commercial nuclear industry and the DOE nuclear complex indicates that some virtually new facilities have already "lost" important design information that once existed, and that many "existing" facilities, including those dating back to the ____, have design information still on hand or reasonably retrievable.
    a. 1930s
    b. 1940s
    c. 1950s
    d. 1960s
9. The FDD should be a lower level document than the SDDs and, in many cases, should contain details on overall facility functions, facility systems that support process systems (e.g., electrical distribution system) in lieu of placing this information in SDDs.
    a. True
    b. False
10. _____ has been developed to show how project management, engineering design, and safety analyses can interact to successfully integrate safety into the design of a new facility or major modification of an existing facility early in the project.
    a. DOE-STD-1027
    b. DOE-STD-1073
    c. DOE-STD-1189
    d. DOE-STD-3009

CONTENTS

FOREWORD

This Department of Energy (DOE) standard is approved for use by all Departmental organizational units and contractors of the Department.

This Standard provides criteria and guidance for the development of a System Design Description (SDD). An SDD identifies the requirements associated with structures, systems, and components (SSCs); explains why those requirements exist (that is, provides the bases for the requirements); and describes the features of the system design provided to meet those requirements. The SDD helps ensure consistency among the engineering requirements for systems, the actual installed physical configuration, and the associated documentation.

This Standard is referenced in DOE Order (O) 420.1B, *Facility Safety*, as a source of guidance on the identification of key design documents supporting facility safety basis development and documentation.

Like National consensus standards, the DOE Technical Standards Program generally expects its standards to be applied voluntarily. Sometimes, a standard is mandated by a higher authority or a regulatory agency, and hence the standard becomes mandatory. To distinguish the requirements contained in this Standard from its recommendations, the term “shall” has been used to designate requirements and “should” to designate recommendations within the standard. Compliance with a standard is achieved by adherence to its requirements and consideration of its recommendations.

Beneficial comments for improvements of this Standard (additions, deletions, or other changes) and any pertinent information should be addressed to Ms. Ashley Ruocco, U. S. Department of Energy, 19901 Germantown Road, Germantown, Maryland 20874-1290; or e-mailed at ashley.ruocco@hq.doe.gov. Commenters are encouraged to use the form DOE F 1300.3, *Document Improvement Proposal.*

1. PURPOSE

This Standard provides criteria and guidance for the technical content and organizational structure of system design descriptions (SDDs) at Department of Energy (DOE) facilities.

2. APPLICABILITY

This Standard should be used to develop an SDD for all active safety class (SC) and safety significant (SS) systems for nuclear facilities. On a case-by-case basis, it may be beneficial to create SDDs for complex or unique passive SC or SS systems, or for complex and unique process safety and general service systems. Examples of such passive system structures and components (SSCs) include an especially complex shielding system, a natural convection (passive) ventilation system, or a complex containment structure. Application of this Standard should be considered for systems, including those in other than Hazard Category 1, 2 or 3 nuclear facilities, because SDDs can support cost-effective operation of systems.

3. OVERVIEW OF STANDARD

The main body of this Standard describes the objective of SDDs and provides higher level criteria and guidance for SDD development (Section 4 and 5).

Appendices A through C provide the following general supporting and background information:

Appendix A – Glossary
Appendix B – Abbreviations and Acronyms
Appendix C – Developmental Resources

Appendices D through H provide the following details supporting SDD development:

Appendix D – Format of SDDs
Appendix E – Technical Content Criteria and Guidance
Appendix F – Compiling Technical Information for the Development of SDDs
Appendix G – Application of the Graded Approach to the Development of SDDs
Appendix H – Preparation of Facility Design Descriptions

4. OBJECTIVE OF SYSTEM DESIGN DESCRIPTIONS

4.1 General

A major purpose of the SDD is to collect system information to facilitate efficient design, maintenance, operation, and training (because personnel will not have to review multiple documents in an effort to locate pertinent information). An SDD identifies the requirements associated with SSCs, explains why those requirements exist (that is, provides the bases for the requirements), and describes the features of the system design provided to meet those requirements. The SDD helps ensure consistency among the engineering requirements for systems, the actual installed physical configuration, and the associated documentation. The SDD often serves as the central coordination link among the engineering documents, facility safety basis, and procurement and construction documents. SDDs also provide a key reference to facilitate design reviews when integrated early in

the design. An SDD does not generate requirements or basis information, but rather collects that information into a usable form.

4.2 Development as Part of Facility and Project Design

DOE Standard (STD) 1189, *Integration of Safety into the Design Process*, has been developed to show how project management, engineering design, and safety analyses can interact to successfully integrate safety into the design of a new facility or major modification of an existing facility early in the project. One of the design outputs of the safety-in-design process is an initial SDD developed during conceptual design to capture the functional and performance requirements of facility systems as they relate to the facility-level design basis accidents that provide necessary input to the identification and classification of important safety functions. The iterative and evolutionary nature of safety-in-design requires engagement of project operations, maintenance, engineering, and safety personnel throughout the process and design output (e.g., drawings, SDDs) to support project milestones and critical decisions through final design and to reflect as-built configurations.

4.3 Users of System Design Descriptions

The intended users of SDDs vary depending on the facility and system covered. Normally, the Cognizant System Engineer assigned to the system is responsible for the development and maintenance of this document. Intended users include those involved in the facility safety analysis, engineering, operations, training, and procedures staff, as well as oversight staff such as DOE Safety System Oversight personnel or Facility Representatives.

An SDD does not generate a system's design, requirements, or basis information, but rather collects such information from multiple sources, such as original technical documents (e.g., safety basis documents, drawings, specifications, vendor technical manuals, etc.) into a conveniently usable vehicle for accessing this information. Since an SDD author cannot anticipate or address all needs, uses, or vintages in a system's evolution for which specific information is sought, it cannot reliably serve as, and therefore should not be used as, a primary source or basis for actual design, operations, maintenance, testing, or other technical activities. Such activities should always be based on original primary documentation sources, where available, in order to minimize the potential for information loss or misinterpretation in the translation, and to assure that *all* information that the user may find pertinent, but that may not have been recognized as such by the SDD author and therefore not included in the SDD, may be appropriately considered. Though not a primary source, the SDD has been proven to be a valuable tool for staff to obtain information and as a pointer to more detailed design information.

5. CRITERIA AND GUIDANCE FOR SDDS

5.1 SDD Physical Form/Location

SDD data shall be housed either in a physical document or in an approved data system, such as an "enterprise" system (ES) that meets the site's configuration management requirements. Either approach should provide the reader a single point of reference rather than requiring access to different documents to obtain pertinent information or interpreting details in vendor technical manuals and engineering documents. Where an ES is used in lieu of a hard copy document, the ES shall provide the same type and level of information in a configuration controlled, accessible manner that meets both the facility configuration management requirements and provides equal or greater functionality to the end-users in supporting their ability to find information.

5.2 SDD Level of Detail

The SDD should collect and provide more detail than would normally be included in safety basis documents but less detail than in engineering design documents. Early in a project's development, this can assist procedure writers in determining what procedures are needed. Later, it can benefit the training staff and new technical staff. When an enterprise system is used, the SDD's references can become links, allowing rapid access to needed procedures and information.

5.3 Procedure Identification

The SDD should identify procedures for facility operations, testing, and maintenance related to the system being described, and point the reader to those specific documents in their proper context.

5.4 Performance Criteria

The SDD shall include information on the functionality and requirements (performance criteria) for evaluating the performance of the system. Performance evaluation may include assessing overall facility operational effectiveness and efficiency, compliance with regulatory requirements, the possible need for improvements to increase system reliability, and the possible need for system design modifications to meet changing programmatic mission needs and demands. SDDs should identify which performance characteristics of the system are the most important.

5.5 Facility Design Descriptions

SDDs may be developed in conjunction with Facility Design Descriptions (FDDs). In an FDD, all the systems in a facility can be addressed with their top-level functions and requirements. Using a graded approach, an FDD can provide a mechanism for addressing simple, less important systems, without requiring a separate SDD. The FDD may be the only document needed for less than Hazard Category 2 facilities. For more complex or important systems within a larger facility, the FDD should refer to individual SDDs for more detailed information. For simple systems that do not implement safety requirements, a separate SDD should not be required if the FDD provides sufficient information. Similarly, for a facility with limited systems, an FDD may not be necessary if an SDD provides necessary information. For guidance on preparing FDDs, see Appendix H.

5.6 Design Information

The SDD shall contain all information about features of the design that demonstrate how the design satisfies the safety criteria in the safety basis documents.

5.7 SDDs and Safety Basis

An SDD shall support the safety basis and help ensure that the operation of the system will be consistent with the safety basis. Even though the SDD may precede the development of the Documented Safety Analysis (DSA), it should not serve as a source of information for the safety basis, since the SDD is not a part of the safety basis. DOE does not rely upon information found uniquely in the SDD to make decisions regarding the safety of the facility. In addition to engineering and safety requirements, the SDD should contain requirements that are derived from programmatic needs.

5.8 Non-Safety Information

While a primary focus of the SDD is on system safety features, the SDD should also address other important features provided to accomplish the programmatic mission, maintain system reliability, and promote effectiveness, efficiency, and flexibility in operations and maintenance.

5.9 SDD Evolution

For a new facility or system, the SDD scope and level of detail may change throughout design and construction. Initially [at conceptual design, either Critical Decision-1 (CD-1) or early CD-2 stage], the SDD may include information on primary system functions and boundaries. It may contain preliminary data and indicators of "to be determined" (TBD) that should be refined as the design matures. It shall serve as the vehicle for collecting and conveying the system requirements, their bases, and how the system meets the requirements to support integration of system design and the safety functions and requirements development during the safety analysis process.

5.10 Documenting Design Changes

The SDD may be used for documenting changes as the design evolves from conceptual design through the preliminary and final design. The development of the SDD shall be coordinated with the engineering design process and with the safety analysis development. During design, updates will iterate between the design and development of the safety basis. To assure that the development of the SDD proceeds as planned, it is recommended that the Safety Design Strategy, per DOE-STD-1189, specifically address the configuration control and development strategy of the SDD parallel with the Preliminary Documented Safety Analysis and hazard analysis development.

During design, construction and commissioning the data needs are different than for operations. The enterprise systems are particularly beneficial to support this process. For example, the ability to have different, custom reports or data presentation is particularly beneficial during design, procurement, construction, and commissioning. The data can be presented from an enterprise system for each group in a different format. The data itself is what is important and shall be configuration controlled and managed in a manner that all data required for operations shall be available when the facility is started up.

For an existing facility or system, where the development and approval of the safety basis have preceded the development of the SDD, the SDD shall contain requirements and descriptions of all relevant features of safety SSCs contained in safety basis documents that are needed to meet the safety functions. The SDD is not a safety basis document. The SDD has proven to be an excellent source for documenting requirements and system characteristics in a facility that has had multiple changes and safety documents (and often contractors) over its operating life.

5.11 SDD Change Control

After the facility is in operations, the SDD shall be a controlled document, or controlled SDD data maintained in an approved data system. It shall be maintained as an authoritative, up-to-date source of technical information on the system. Prior to starting operations, the configuration management approach should be defined in the design strategy.

When a change to the system is proposed, the SDD should be consulted to identify the pertinent requirements and the referenced engineering source documents. The results of the change should be

reflected back into the SDD. Changes to the SDD itself are within the purview of the DOE contractor within an appropriate change control process.

5.12 Distinguishing Mandatory Versus Optional Requirements

An SDD shall distinguish between the items that are mandatory requirements that the system shall meet and those additional characteristics that are optional/desirable. If the format recommended in this Standard is followed, Section 3 shall contain only the requirements on the system (and their bases) necessary to fulfill the system function statements, and not the extra, non-mandatory performance capabilities that might exist in the actual system design configuration. Section 4 of the SDD describes how the actual system currently is designed and configured to satisfy its requirements, and also describes the full capacity and capabilities of the system beyond the mandatory requirements.

5.13 SDD Use of Source Documents

The information in the SDD is a combination of narrative and index ("road map") approaches. It is not intended that the SDD be a "cut and paste" of sections from the DSA or Technical Safety Requirements (TSRs). Data or information from these higher-level documents should be linked (or road-mapped) to minimize the maintenance of information in the SDD and to reduce the potential for the staff to fail to use the source documents. Including photographs of equipment and arrangements is encouraged, particularly when the equipment/room is inaccessible during operations and/or difficult to access. Photographs and sketches provide valuable information in an SDD.

Engineering judgment should be applied to determine when information might be more detailed than is worthwhile for the intended audience of the SDD. The status of the source document for information (that is, current document or archived historical record) should not be a deciding factor in determining if the information may be needed by the SDD user. The best practice is to provide a summary and a reference to the details. To omit information from an SDD on the basis that the information might need to be revised sometime in the future if a change were to be made is not a valid basis for determining what information to include in the SDD. If the information is important to the overall purposes of an SDD and to the intended audience, it should be included in the SDD.

If not captured in other facility documentation (example: System Health Reports), then the SDD should provide for collecting/capturing operating experience information, including lessons learned from other facilities that have similar systems. This would normally be captured in an Appendix if not retrievable elsewhere.

5.14 SDD Details

All SDD detail areas to be covered are included in the Appendices; if not applicable, the document or enterprise system should so state the non-applicability.

The SDD shall identify by title the "owner" of the SDD and shall define responsibilities and authorities for maintaining the technical content of, and for reviewing changes to, the SDD.

APPENDIX A: GLOSSARY

This glossary explains important terms in this Standard. To the extent practical, standard definitions have been used. The full bibliographical information on these references is given in Appendix C to this Standard. In some cases, the general definitions have been supplemented in order to explain more fully how the term is used in this Standard.

Basis. The basis explains why a requirement exists and why it has been specified in a particular manner or at a particular value during the engineering design process. Basis information is delineated in design input information, design constraints, and intermediate outputs, such as design studies, analyses, and calculations. The basis encompasses consideration of such factors as facility mission, facility availability, facility efficiency, costs, schedule, maintainability, and safety. (10 CFR 830)

Cognizant System Engineer. The engineer designated by the organization to each system to which the System Engineer Program, as defined in DOE O 420.1B, applies. The CSE maintains overall cognizance of the system and is responsible for system engineering support for operations and maintenance. The CSE provides technical assistance in support of line management safety responsibilities and ensures continued system operational readiness. (DOE-STD-1073-2003)

Controlled Documents. Documents whose content is maintained uniform among the copies by an administrative control system. The goal of controlling documents is to ensure that work is performed using approved current information, not obsolete information. Important documents to be controlled are uniquely identified (including revision number, date, and specific copy number), and distribution is formally controlled. Revisions to controlled documents are uniquely tracked and implemented, including mandatory page replacements and receipt acknowledgment. Controlled documents typically include procedures for operations, surveillance, and maintenance, and safety basis documents such as the DSA, TSRs, and hazard and accident analyses. (10 CFR 830)

Design Information. Design information is the combination of the requirements and the corresponding basis information associated with the engineering design process. (DOE-STD-1073-2003)

Engineering Design Process. The technical and management process that begins with the identification of design inputs and constraints (e.g., mission objectives, commitments, applicable codes, standards, regulations, procedures, and methodologies), processes this information, and results in the issuance of requirements and of formal design analyses and design documents from which SSCs are fabricated, constructed, installed, and commissioned. This process defines and documents the inputs; adheres to the constraints; performs and documents analyses, calculations, technical studies and evaluations; and ensures that the outputs of the process (i.e., the requirements that dictate a design that satisfies the inputs and constraints) are documented and complete.

Enterprise System. Enterprise systems (ES) are large-scale, integrated application-software packages that use the computational, data storage, and data transmission power of modern information technology (IT) to support processes, information flows, reporting, and data analytics within and between complex organizations. The integrated content may then be used to provide a configuration management solution throughout the life cycle in relation to the products, assets, processes and requirements of the entity (laboratory, facility, SDD, etc.). Enterprise applications can be described as a means to manage both the content and the configuration (including change control) of the enterprise. Enterprise content management

systems are electronic systems effective in capturing, managing, storing and delivering content across an enterprise, managing the content (e.g., the information and data of an SDD) "in context" with the entire business (facility/national laboratory).

Facility Design Description. A document that defines the facility, its systems and functions.

Requirements. The results of the engineering design process that define what has been required. Requirements are typically defined on design output documents (such as drawings and specifications) that specify the functions, capabilities, capacities, physical dimensions, limits, setpoints, etc. for a structure, system, or component.

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

Safety Basis Documents. Documents providing safety basis information. These typically include, but are not necessarily limited to, the DSA, TSRs, Unreviewed Safety Question (USQ) Process, DOE-issued Safety Evaluation Reports, and DOE Conditions of Approval.

Safety Function Statements. Top-level statements that express the objective of the SSC in preventing or mitigating a given accident scenario. Safety functions should include: 1) situations and any general accident types during which the function is required to be met; 2) specific functional needs that prevent, detect, and mitigate an event; and 3) sufficient description to enable clear functional requirements, design requirements, and acceptance limits to be defined for those SSCs chosen to meet the safety function.

Safety Structures, Systems, and Components (Safety SSCs). The set of safety-class SSCs and safety-significant SSCs for a given facility. (10 CFR 830) The definitions for safety-class SSCs and safety-significant SSCs and associated relevant information are provided in DOE-STD-3009.

Subsystem. A combination of components, modules, devices, or software within a system that can perform a function or an identifiable part of a function. A subsystem may be deemed to exist when specific flow paths or equipment or functional capabilities can be correlated with different parts of the system functions or system requirements. For example, if the system function statement were to say to maintain negative differential pressures in various zones, there might be one flow path that could be correlated with maintaining the negative differential pressure in one of these zones. In another example, a general fire protection system might have one subsystem that detects fire conditions, another subsystem that holds the fire water, and a third subsystem that delivers the fire water to the proper location to suppress the fire. In some systems, programmable software is treated as a subsystem associated with the system.

Support System. A system that provides another system with a supporting service that is necessary for the supported system to be capable of meeting its system requirements. For example, an instrument air system may be needed for a ventilation system to meet its system requirements with regard to certain dampers opening, modulating to maintain a specified negative pressure differential, or closing under specified conditions. In another example, an HVAC system may be required to maintain the temperature of an environment within the limits for which some components are rated. In some designs, components of the system may go to a so-called "fail-safe" condition upon loss of electric power or some other supporting service, but that is a preferred failure mode. Preferred failure modes do not negate the need for the support system.

System. An interrelated set of structures, equipment, subsystems, modules, components, devices, parts, and/or interconnecting items that is capable of performing a specified function or set of functions that fulfill a purpose. Systems usually have defined physical boundaries, and systems often depend upon human interactions. Some aspects of a system might be important to safety or programmatic mission, while others might not. Sometimes a distributed set of individual structural elements may be considered collectively to be a system. Accordingly, the term "system" is used in this Standard to fully encompass structures, systems, and components (SSCs). A system design description may be appropriate even if a particular set of items does not meet this definition.

System Functions. Those functions that the system needs to be capable of performing in order to accomplish its intended purpose in the facility.

APPENDIX B: ABBREVIATIONS AND ACRONYMS

CD	Critical Decision
CM	Configuration Management
CMMS	Computer Maintenance Management System
COTS	Commercial Off-the-Shelf
CSE	Cognizant System Engineer
DSA	Documented Safety Analysis
EIS	Environmental Impact Statement
ES	Enterprise System
FDD	Facility Design Document
FMEA	Failure Modes and Effects Analysis
HVAC	Heating, Ventilation, Air Conditioning system
MEL	Master Equipment List
P&ID	Piping and Instrumentation Diagram
PDL	Project Decision List
PID	Proportional-integral-derivative [controller]
PLC	Programmable Logic Controller
QA	Quality Assurance
SC	Safety Class
SDD	System Design Description
SNM	Special Nuclear Material
SS	Safety Significant
SSC	Structure, System, or Component
TSR	Technical Safety Requirement

APPENDIX C: DEVELOPMENTAL REFERENCES

This Attachment identifies documents that were considered during the development of this Standard, either directly or indirectly.

1. 10 Code of Federal Regulations (CFR) Part 830, *Nuclear Safety Management*
2. 10 Code of Federal Regulations (CFR) Part 835, *Occupational Radiation Protection*
3. DOE O 410.1, *Central Technical Authority Responsibilities Regarding Nuclear Safety Requirements*, 8-28-07
4. DOE O 414.1D, *Quality Assurance*, 4-25-11
5. DOE O 420.1B, *Facility Safety*, 12-22-05, Change 1: 4-19-10
6. DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1, Facility Safety*, 3-28-00
7. DOE O 422.1, *Conduct of Operations*, 6-29-10
8. DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, December 1992, Change 1: September 1997
9. DOE-STD-1073-2003, *Configuration Management*, October 2003
10. DOE-STD-1189-2008, *Integration of Safety into the Design Process*, March 2008
11. DOE-STD-3009-94, *Preparation Guide for U. S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, July 1994, Change 3, March 2006

APPENDIX D: FORMAT OF SYSTEM DESIGN DESCRIPTIONS

SDDs should adhere to the following outline to the extent that it is relevant to the SSC being described. When a section of the outline below is not applicable to the system, the section shall be retained in the SDD with a statement that the section is not applicable. A brief explanation of its non-applicability should also be provided, especially if the reason for the non-applicability might not be immediately obvious to the readers. Conversely, the outline might need to be expanded to address aspects of some systems not covered previously. If an ES is used to capture the SDD information, all aspects recommended by this Standard shall be searchable and, if the data is not applicable, the ES shall capture the non-applicability rather than just not having the information available.

> Note: The outline below is not intended to define minimum content requirement, but rather to provide general guidance. This outline is intentionally exhaustive to encompass important aspects of virtually any system. The content of specific SDDs is expected to vary with the type of physical system being described (e.g., ventilation/confinement systems, electrical power systems, chemical processes). Site format consistency has been shown to assist training and orientation of new staff and/or backup staff, to aid in use by the CSE staff, and to aid in updating and maintaining multiple SDDs for a facility.

1. Chapter 1: Introduction of an SDD
   - 1.1 System Identification
   - 1.2 Limitations of this SDD
   - 1.3 Ownership of this SDD
   - 1.4 Definitions/Glossary
   - 1.5 Acronyms

2. Chapter 2: General Overview
   - 2.1 System Functions/Safety Functions
   - 2.2 System Classification
   - 2.3 Basic Operational Overview

3. Chapter 3: Requirements and Bases
   - 3.1 Requirements
   - 3.2 Bases
   - 3.3 References
   - 3.4 General Requirements
     - 3.4.1 System Functional Requirements
     - 3.4.2 Subsystems and Major Components
     - 3.4.3 Boundaries and Interfaces
     - 3.4.4 Codes, Standards, and Regulations
     - 3.4.5 Operability
     - 3.4.6 Performance Criteria
   - 3.5 Specific Requirements
     - 3.5.1 Radiation and Other Hazards
     - 3.5.2 As Low As Reasonably Achievable
     - 3.5.3 Nuclear Criticality Safety
     - 3.5.4 Industrial Hazards
     - 3.5.5 Operating Environment and Natural Phenomena
     - 3.5.6 Human Interface Requirements

APPENDIX E: TECHNICAL CONTENT CRITERIA AND GUIDANCE

The chapters described in this Appendix provide criteria and guidance for each section of the SDD based on the format recommended in Appendix D.

1. CHAPTER 1: INTRODUCTION OF AN SDD

This section provides limited preliminary information related to the specific SDD such that the SDD can be understood and can be used effectively and efficiently.

1.1 System Identification

This section shall identify the scope of the system being described in the particular SDD. This section should identify the boundaries of the system concisely to explain the physical scope of the system that is covered by the SDD and shall identify the interfacing systems.

1.2 Limitations of this SDD

This section shall explain any limitations that may exist for the SDD. If the scope of the SDD is limited in some way, the reader needs to be made aware of that limitation. For example, the current version may be preliminary and provide basis information for only the safety requirements. Similarly, if certain sections of the SDD have not been fully addressed or developed completely, the reader should be informed of this limitation. This section may contain notes to the user, e.g., known limitations of source document information, missing source documents, or missing source data.

1.3 Ownership of this SDD

This section shall identify by title the owner of the SDD and shall define responsibilities and authorities for maintaining the technical content of, and for reviewing changes to, the SDD. The owner should not be identified by name, because assignments could change. Rather, the SDD should point the reader to a title, place, or document that would identify the specific individual assigned as SDD owner. Normally, the owner is the assigned Cognizant System Engineer for the system described. For some facilities, the Design Authority for the facility is designated as the Approval Authority for changes. Depending on the significance of the system and the maturity of the facility, additional reviewers should be specifically identified in this section.

1.4 Definitions/Glossary

This section should define or explain key terms and phrases necessary for the reader to understand the SDD.

1.5 Acronyms

This section should define the acronyms used in the SDD.

2. CHAPTER 2: GENERAL OVERVIEW

The SDD shall include an overview of the system that includes: 1) statements of the safety functions and other functions assigned to the system; 2) the overall classification of the system; and 3) a basic operational overview of the system, including a simplified system diagram. This general overview section should be limited to information necessary to establish a foundation for understanding the requirements and bases information that follows in the SDD.

2.1 System Functions/Safety Functions

The SDD shall state the functions that the system needs to be capable of performing in order to accomplish its intended purpose in the facility. To the extent applicable to the system being described, the system's function statements should address the areas of safety (protection of onsite and offsite personnel from radiological and other types of hazards), environmental protection, programmatic mission, and general functions. Statements of the functions of the system should be sufficiently specific to the system as to be distinctively different from the functions of other systems. When taken collectively, the functions of all the systems should describe comprehensively how those systems contribute to the overall operation of the facility.

Statements of safety function serve as the key link between the safety basis documents and supporting documents. As discussed in References 14 and 15, the essential constituents of statements of safety function are:

a. The situations and any general accident types during which the system may be called upon to perform its safety function(s).

b. The specific functional needs that prevent, detect, or mitigate undesirable occurrences.

c. Those performance characteristics that have been specifically relied upon in the safety basis, including the hazard analysis and accident analysis (this may include initial conditions or assumptions concerning the system or its operation).

Specific requirements and bases that are derived from the safety functions should be defined in detail in Chapter 3: Requirements and Bases.

Statements of safety functions in the SDD shall be consistent with the corresponding information in the facility safety basis and specific references to the safety basis documents shall be provided. More than one safety function may be assigned to a system. Safety functions may also be assigned to a subsystem when the SDD is for a process system that includes subsystems required to prevent, detect, or mitigate an event involving the process system.

> Note: A fundamental understanding of the functions to be provided by safety SSCs is integral to maintaining the analyzed and approved engineering basis, as well as to operations, testing, surveillance, maintenance, and modification activities. It is important that safety function statements contain sufficient information and clarity to provide the fundamental understanding that supports the development of functional requirements, identification of appropriate design and performance criteria, evaluation of system performance, and evaluation of changes.

2.2 System Classification

The SDD shall state the overall classification that has been assigned to the system. This classification should be based on the highest ranking (most important) requirements identified for the system, using the hierarchy presented in Chapter 3 of this Standard (or the DOE contractor equivalent). For example, if a system were to have safety-significant, mission-critical, and general requirements, but no safety-class (SC) requirements, it would be classified as a "safety-significant" system. If a system were to have mission-critical and general requirements, but no safety or environmental requirements, it would be classified as a "mission-critical" system. This part of the section should be limited to a simple, one-sentence statement such as, "This system is classified as *mission-critical*."

This section shall include a simple positive or negative statement indicating whether or not the system being described (or a subsystem of the system being described, such as a high temperature interlock) is the subject of the facility TSRs.

2.3 Basic Operational Overview

This section should include a simplified system diagram, including boundaries and interfaces. Where subsystems exist, they should be illustrated on the simplified system diagram. Where the safety function(s) are provided by a subsystem(s) (e.g., high temperature interlock safety system associated with an evaporation system), a simplified system diagram for the safety system should be provided. The system boundary shall be consistent with that of the approved safety basis documents. This is particularly important for safety system boundaries. Responsibilities of the Cognizant System Engineer should normally align with the established system boundary, such that one Cognizant System Engineer should typically be responsible for the SDD. The scope should not require multiple CSEs to be responsible for the same document.

This section shall include a brief discussion of how the system operates. This discussion should be limited to those operational aspects necessary to understand the requirements in Chapter 3.

3. CHAPTER 3: REQUIREMENTS AND BASES

This section of the SDD shall identify both the requirements of the system and the bases for those requirements. This section should also present the classification of those requirements with regard to importance, thereby differentiating whether or not each requirement applies to a safety function of the system. The bases should also refer to the source documents from which the requirements and bases were obtained. If the requirements of an applicable standard were tailored, a justification that explains the adequacy of the design with the tailored requirements should be included in the basis, either explicitly or by reference.

Requirements and bases statements should be appropriate, concise, and meaningful. System requirements statements should be clear and specific and should not include basis information. For example, a requirement statement such as, “Redundancy is required to mitigate component failures” would be better stated as, “Full-capacity redundancy is required for the following components: ...” with the explanation for this requirement provided as part of the basis information. In addition, the bases statements should be informative and add value instead of merely re-stating the requirement in different words. Value-added statements may include, for example, a brief explanation/summary of the application of specific subsections of a consensus code and standard with reference to the specific edition (code of record) of the standard and any associated facility engineering design documents.

3.1 Requirements

System requirements build on and logically support the system functions. For example, a system general or overall function statement might say that the system has to function “on a highly reliable basis.” The system requirement statements would then specify those features, such as component quality requirements, redundancy, diversity and environmental requirements that provide the high reliability for the system.

Requirements come from various sources. For example, some requirements might originate from regulatory agencies such as DOE or EPA, from state and local governments (such as release limits or building codes), or from DOE contractor organizations such as site management, design engineering, construction, ES&H, or facility management. Also, requirements should have different levels of importance. Some requirements are part of the DOE safety basis for a facility, and operation of that facility is allowed only if it complies with those requirements (such a requirement can be changed only if prior approval is obtained from DOE). Other requirements may have no bearing on the facility safety basis, and may be changed as deemed appropriate by the design authority (which may be the facility management) without prior approval from DOE.

The requirements and bases that should be included are those related to the system as a whole and those that are specific to individual subsystems and components within the system. Requirements and their bases (using a graded approach) should be included in the SDD, regardless of their source, because the SDD should identify the requirements and bases needed for operations, engineering, and maintenance personnel to have the understanding to operate and maintain the system safely, reliably, and efficiently. Requirements should be stated in such a way as to communicate the information as design output requirements within the context of an operating facility even if the SDD is prepared prior to commencement of operations. These requirements should be maintained throughout the operational life of the facility and updated to reflect changes to the requirements and their sources, typically stemming from facility engineering design change documents (the level at which the change control process for the system is accomplished).

Categorizing requirements by type is useful for identifying information that may be sought quickly for making decisions concerning system operability and compliance with the safety basis. This

categorization is also helpful for routine searches, e.g., finding all seismic requirements for a given system or for the facility overall.

Repetition of requirements should be avoided. However, some requirements could fit into more than one section of the SDD. For example, a requirement might say that certain components shall go to specified positions (open or closed) upon loss of electrical power. This might be considered to be an electrical power engineering requirement (Section 3.3.4), or this same requirement could be viewed as a reliability requirement (Section 3.5.3). In such cases, the information should be presented in only one section of the SDD, with a reference to that section in other sections where the same information becomes pertinent. One approach is to place the requirement in the first section in the SDD in which it becomes relevant. Alternatively, use judgment to select the most fitting section for the requirement.

Requirements should be classified with regard to their importance to ensure appropriate consideration in system operation, maintenance, performance evaluations, and evaluation of system changes. The following hierarchy, or equivalent, should be used. The hierarchy is not intended to define a required format for this information.

1. Safety Requirements
   a. Safety Class
   b. Safety Significant
   c. Other “Important to Safety” Requirements
2. Environmental Requirements
3. Mission-Critical Requirements
4. General Requirements

Requirements classified as safety-class or safety-significant are those identified in safety basis documents to accomplish safety functions, as established by the hazards analysis and safety analysis processes. The “Important to Safety” requirements classification applies to those requirements that, although not classified as safety-class or safety-significant, still perform functions considered important to overall facility safety and are part of worker safety (e.g., standard industrial hazards) or the defense-in-depth safety basis for the facility as defined in the facility’s safety basis.

The safety requirements statements shall be consistent with the corresponding statements of functional requirements and performance criteria in the facility DSA, TSRs, and other safety basis documents, if the safety basis has already been established for the facility. Performance criteria (normally provided in Section 3.16) for the system shall be consistent with the performance criteria specified in the facility DSA. Often, additional performance criteria are needed to meet program or project goals. These should also be provided along with a brief description of the driver/basis for those criteria.

One convenient way to correlate these requirements is to use footnotes. A footnote to a particular requirement statement might say, “This requirement corresponds to Requirement 4.4.3.8 on Page 4.4-12 in the DSA (Reference 3 in Appendix A).” An alternate way to correlate these requirements is with a table (e.g., a requirements matrix) in a separate appendix or attachment to the SDD. The environmental protection category should be considered separately and explicitly in the SDD to assure this important set of requirements is not overlooked and to address requirements related to environmental permits, when applicable.

Mission-critical functions are those that prevent or mitigate substantial interruptions of facility operations or severe cost or other adverse impacts, or satisfy other DOE programmatic mission considerations.

The general category is used for requirements that do not fit into the other categories.

This set of classifications is based on DOE-STD-3009 for Hazard Category 1, 2 or 3 nuclear facilities. This set of classifications, a modified set, or a completely new set of classifications may be used for other than Hazard Category 1, 2 or 3 nuclear facilities.

3.2 Bases

A major function of the SDD is not only to state the engineering requirements of the system, but also to explain the basis for those requirements. Basis information explains why the requirement exists, why it is specified in a particular manner, and why it has a particular value. While documenting the bases for all requirements in the SDD is desirable, the basis information for safety requirements shall be stated in the SDD.

Technical basis information should be included directly in the body of the SDD immediately after the requirement, rather than placing such information in an appendix or referring to another document. However, the basis for a group of related requirements may be provided in one place. The bases for the requirements should be presented in a manner that minimizes the disruption of the reader's flow of thought. The recommended manner for presenting the basis information is to provide it in separate paragraphs that are set off in a special format or font that is clearly discernable. The following example illustrates this approach:

> **Requirement**: The exhaust air high temperature trip setpoint on the ventilation exhaust fan shall be less than or equal to 185°F.
>
> **Basis**: The setpoint is established high enough above the normal operating exhaust air temperature of 140°F to avoid spurious trips of the ventilation exhaust fan, but low enough to provide early detection of hot gases. The safety analysis shows that, in the event of a fire, the consequences to workers from the spread of toxic products of combustion are acceptable if the fan is tripped before exhaust air temperature reaches 200°F (Reference #, Section xyz).

Basis information can take different forms. Specific engineering documents (such as studies, analyses, calculations, and reports) are important basis references. Appropriate and specific references to national codes and standards also should be included in the basis references, when appropriate. Operational experience and standard engineering practices are valid reasons that could justify a requirement. Basis information should be as detailed as possible with controlled document reference to aid future personnel in fully understanding the technical basis, especially when no other information is available.

3.3 References

Specific references are essential to understanding and using the SDD. Reference to source documents from which requirements and basis information has been extracted adds traceability to the SDD and improves its credibility. To the extent that such reference documents are available, the source documents that contain the cited requirements or the bases information should be referenced in the SDD. Even if the supporting reference document contains only the requirement but not the basis information, such as may be the case for a procurement specification, the SDD should include that document as a reference.

If the requirement or basis information is not recorded in a separate document, the documentation no longer exists, or retrieval of such a document is not feasible, the basis should note that a documented reference is not available, so as to avoid potential confusion and wasted effort by other staff who may try to research the basis.

One effective method of referencing the source documents is to provide the bibliographical information on the source documents in an appendix to the SDD (i.e., Appendix A). Footnotes, or an equivalent, can refer to particular source documents and provide specific page references where they are appropriate in the body of the SDD. For example, the footnote for a particular requirement might say: "See Appendix A, Reference 5, pages 12-16." This technique has the advantage that complete bibliographical details do not need to be repeated each time a document is referenced. This technique should also make SDD revisions easier. Such footnotes need not be limited to a single source document. If more than one source document/reference contains pertinent information, they should be included in the footnote.

3.4 General Requirements

3.4.1 System Functional Requirements

This section shall state those functional requirements and their bases, for both safety requirements and non-safety requirements, that fulfill the system function statements. Using a graded approach, emphasis should be placed on ensuring that a comprehensive set of safety functional requirements is identified. If the requirements and bases have already been presented earlier in the SDD (see e.g., item c. in Section 2.1), refer to that section rather than repeating the information.

> Note: Functional requirements relate to how the system functions, performs, behaves, or responds to particular conditions. Non-functional requirements should be addressed in other sections that correspond to the most fitting engineering or topical category, such as those that address reliability features, electrical power needs, testability, or quality assurance provisions.

Functional requirements should address the system or facility situations to which the system is designed to respond. When applicable, this should include the expected ambient operating conditions related to those situations under which the system is required to perform its assigned function(s), and the sequence in which certain actions are to be accomplished. Refer to DOE-STD-3009 for examples of functional requirements.

These requirements statements should include sufficient detail to establish the acceptance criteria or limits against which the actual performance capability of the as-built system can be evaluated. In some situations, such acceptance criteria may be called "Performance Criteria."

3.4.2 Subsystems and Major Components

General requirements and their bases that are unique to subsystems and major components should be identified in this section.

3.4.3 Boundaries and Interfaces

This section should identify requirements and their bases that might exist concerning the boundaries of the system being described, with emphasis on the components at the boundaries such as isolation valves. For example, the boundary with an associated instrument air system may be required to be at the upstream side of a particular check valve. Not all boundaries will have specific requirements;

however, those that do have specific requirements shall be included in this section. Referring to the simplified system diagram in Chapter 2 of the SDD may be useful for this purpose.

The SDD should identify any requirements and their bases relating to interfacing systems, especially "support systems" (see Glossary, page 1-2). For example, if a system requires a support power supply that is to be operated on electric power available only from an uninterruptible power system, that interface should be described. The SDD should also identify those interface requirements and their bases that exist if the system being described provides support to another system, especially if needed for the operation of a safety function of the other system. Not all interfaces will have specific requirements.

3.4.4 Codes, Standards, and Regulations

This section should identify those codes, standards, or portions thereof that have been applied to the system. It should identify codes and standards that have been required either by regulatory organizations or by the DOE contractor.

> Note: Where codes, standards, or portions thereof have been applied at the option of the DOE contractor and compliance is expected by the contractor, they become requirements on the system and hence they need to be included in this section. In contrast, if codes and standards (or similar documents such as handbooks or guides) are intended to be used only as general guidance and compliance is not required, they are not requirements on the system and hence should be addressed in other sections of the SDD and clearly identified as guidance rather than a requirement.

To the extent practical, the bases associated with codes and standards should identify the authority that determined that it was appropriate to apply each of the codes and standards, so that future proposed changes or exceptions in the application of those codes and standards can be referred to the appropriate authority.

The specific codes and standards should be identified, rather than simply the general name of the standards organization. Consideration should also be given to the desirability of identifying the edition (or year of publication) for each identified code or standard, i.e., the code of record, to eliminate confusion as to the specific requirement that is applicable.

> Note: Subsequent editions of some codes or standards might contain requirements that this particular system does not meet and should not have to meet. If the editions of the standards are not specified, it implies an intent to maintain compliance with all subsequent editions. This is a lesson learned by many facilities that leads to a failure to meet requirements "on paper," when management, engineering, etc., do not intend for subsequent revisions to a code and standard to automatically apply.

A system may need to meet a particular section of, but not the entire, code or standard. Identify only those sections with which the system will comply or has complied and for which such compliance will be maintained.

> Note: If the whole standard is identified without any qualifications, it implies an intent to comply with the entire standard.

This section should identify government regulations that are applicable to the system being described. These include: the Code of Federal Regulations (CFRs), DOE nuclear safety directives and

regulations from other Federal agencies such as the EPA, court orders (if applicable), state laws and regulations, and state permit requirements.

3.4.5 Operability

When the system being described is the subject of TSRs that require the system to be operable, this section shall be consistent with that of the safety basis documents. This section shall define system operability; that is, the aspects of this system that are required to be capable of performing as intended in order for this system to be formally considered "Operable." This section may summarize and point to the appropriate safety basis document operability requirements (e.g., TSR LCOs, limiting safety system settings, or TSR design feature requirements), rather than duplicating extensive and complex controls and surveillance requirements within the SDD. To the extent that the facility safety basis, including the TSRs, defines operability specifically for the system, that definition shall be the one stated/identified in the SDD. This section should also identify the facility operating modes or conditions for which the system is required to be operable.

> Note: System compliance with its "Operability" requirements will ensure accomplishment of those safety functions specified by the applicable safety basis documents such as the DSA or TSRs. The general definition of operability is that a system, subsystem, component, or device shall be considered operable or have operability when it is capable of performing its specified function(s), and when all necessary attendant instrumentation and controls, electrical power, cooling water, or other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its function(s) are also capable of performing their related support function(s).

If the system has additional operability requirements established by facility management that go beyond those requirements included in the TSRs, these should also be included in this section in a manner distinctive from the TSR operability requirements.

3.5 Specific Requirements

3.5.1 Radiation and Other Hazards

This section shall address those safety requirements and their bases that have been established for the design of the system in consideration of radiation or other hazards (such as lasers and hazardous chemicals) that are beyond those typically accepted in an industrial workplace covered by OSHA. These requirements pertain to the required level of protection for facility workers, other employees located at the site, and the public. All system functional requirements assumed in facility safety basis documents should be identified if they have not already been presented in the SDD.

This section includes all radiological safety requirements needed to comply with specific numerical exposure limits regardless of cost. Those additional safety features that may be provided on a cost-beneficial basis are generally referred to as "As Low As Reasonably Achievable" (ALARA) and should be addressed in the next section and excluded from this section.

3.5.2 As Low As Reasonably Achievable

This section should identify requirements in the design safety features (such as special shielding) to reduce the radiation exposures to personnel to ALARA. In general, ALARA goals are achieved (or implemented) on a cost-beneficial basis, as contrasted with numerical radiation exposure limits that must be met regardless of cost. This section should also address those requirements (and bases) that

might exist to protect sensitive components from radiation exposure or to minimize radiological contamination. Monitoring equipment and alarms should also be addressed.

This section should include only information that is specifically related to the system being described; general information about the facility radiation control program or ALARA program should not be repeated here.

3.5.3 Nuclear Criticality Safety

This section shall identify those requirements and their bases that might exist related to design features to prevent an inadvertent nuclear criticality. An example would be critical dimensions on the size and shape of pipes, tanks, or other containers. This section also should identify items that intentionally are not present, such as sources of water that have been routed so as not to be overhead or in the immediate vicinity.

Non-design, operational (or administrative) aspects of the nuclear criticality safety program that apply to this system, such as the use of materials/contents placards, should be addressed under Safety Management Programs in Section 4.

3.5.4 Industrial Hazards

This section should identify requirements for safety features for hazards that are typically accepted at commercial industrial workplaces. This section should identify safety and health requirements pertaining to the system being described related to personnel safety and OSHA considerations.

This section is not intended to identify all the features of a piece of equipment that may be related to the safety of personnel operating the equipment. Prominent aspects (such as guards surrounding rotating machinery) or those that were part of the basis for selecting the particular equipment from a vendor should be identified. This section provides the information that would help preclude potential future modifications that might compromise features important to protecting employees.

3.5.5 Operating Environment and Natural Phenomena

This section should identify requirements (and their bases) related to the normal environment under which the system is required to be capable of operating; for example, ambient temperature, humidity, altitude, noise, radiation, electromagnetic or radio frequency interference (EMI/RFI) and vibration. Requirements in this section typically will be unique to the particular system.

This section should also address abnormal and accident environments, consistent with the hazards analysis and accident analysis. This section should be limited to environmental conditions that go beyond typical design requirements such as those found in the International Building Code. This section should address design requirements for protection from natural phenomena such as tornadoes, floods, or seismic events. For example, if the system is required by the Facility Safety Basis to operate during or following an earthquake, the associated acceleration spectra should be identified.

3.5.6 Human Interface Requirements

This section should identify the requirements (and bases) that may exist related to the design of the system to enhance the interface between the system and the human operator. Where appropriate, this should also include human factors or ergonomics requirements.

This section shall identify any design requirements for alarms intended to trigger manual safety actions. The basis for such a requirement should include a summary of the conditions that are intended to generate the alarm (the meaning or significance of the condition) and a brief summary of the actions that need to be taken manually in response to the alarm. Response actions to these alarms are typically summarized in section 4.2 or 4.1.6 of the SDD.

Requirements for alarms that are related to non-safety actions should be similarly described. This section should identify requirements that may exist for the design to distinguish indications and alarms that promote the prompt and effective performance of required operator safety actions from other indications and alarms. Similarly, this section should identify requirements related to features such as shapes, colors, or locations of particular indicators, controls, or displays if the feature is critical to ensure the task can be correctly completed by the operator.

3.5.7 Specific Commitments

This section shall identify unique or special commitments that have been made to the DOE or another regulatory agency such as the EPA and court orders. For example, in the investigation of an operational event at a facility, it might have been determined that a major contributor to the incident was the absence of positive position indication for some critical dampers or valves. As part of the corrective actions to prevent recurrences of that or similar events, the contractor may have made a commitment to DOE that all dampers and valves will have positive position indicators provided. In that case, this commitment would be identified as a requirement for the system, and a reference made to the appropriate document(s) that provide the commitment. Such commitments may be contained in occurrence reports, correspondence, or other documents.

3.6 Engineering Disciplinary Requirements

This section should identify those requirements and their bases that are typically related to particular disciplines of engineering. The focus should be on the requirements needed to meet the system and safety functions; optional capabilities or excess capacities should be discussed in Section 4.

3.6.1 Civil and Structural

This section should identify those civil and structural engineering requirements and their bases related to the system being described. This section should include only the civil or structural requirements for a typical facility such as may be found in the International Building Code. Examples of requirements that should be included are anchorage, bracing, or support requirements for equipment (e.g., to prevent damage to equipment or injury to personnel).

3.6.2 Mechanical and Materials

This section should identify those mechanical or materials engineering requirements and their bases related to the system being described. Such requirements may relate to pumps (e.g., type, net positive suction head, flow capacity, discharge pressure), valves (e.g., type, size, stroke time, location), HVAC system components and flow rates or differential pressures, equipment heat generation limits or cooling system parameters, and parameters relating to compressors, filters, fans, boilers, and other equipment.

3.6.3 Chemical and Process

This section should identify those chemical or process requirements and their bases related to the system being described. Such requirements might include process or engineering limits on physical parameters such as temperature, pressure, concentrations, feed rate, pH, heat transfer rates, and

chemical compositions (e.g., amount or concentration of impurities allowable). Other requirements that might relate to the type of process (e.g., continuous or batch, reactive or non-reactive), waste generation considerations, or process evolutions (e.g., hold times, agitation rates) should be identified.

3.6.4 Electrical Power

This section should identify those electrical power engineering requirements and their bases related to the system being described. In most cases, these will involve the need for electrical power at a particular voltage level, current, frequency, or quality. In some cases, these requirements might involve providing electrical power for other systems. Examples of these later cases would be systems that include diesel generators, motor-generator sets, uninterruptible power supplies, or battery banks. Such systems would typically include the associated electrical distribution system plus automatic and manual transfer features and the associated alternate power paths or circuits.

Examples of requirements are the length of time the system shall be capable of performing its function(s) following the loss of normal utility power, and fail-safe states that equipment shall assume upon loss of power. Another such requirement may be power quality. For example, a component that is critical to the proper functioning of a safety system may be sensitive to voltage or frequency perturbations and thus have a power quality requirement that the component receive regulated power from an uninterruptible power supply with specific output parameters, such as between 118.5 and 121.5 Vac and between 59 and 61 Hz at the input terminal of the device.

3.6.5 Instrumentation and Control

This section should identify those instrumentation and control engineering requirements and their bases related to the system being described. This section is focused primarily on hardware controls; computer hardware and software controls are addressed separately in a later section.

This section should include requirements for manual and automatic actions for system initiation and control, indicators, alarms, and manual controls that are used to operate the system. This section should identify required ranges and accuracies.

This section shall distinctively identify instrumentation that either is (or will be) directly subject to TSR requirements or provides information to verify compliance with TSRs. This section of the SDD should identify the required nominal values of the setpoints associated with the system and ranges of acceptable setpoint values. The basis information should explain any limitations, either administrative, design, or limits important to safety, that may exist on the system or its components.

3.6.6 Computer Hardware and Software

This section should identify those computer hardware and software engineering requirements and their bases related to the system being described. Many of the instrumentation and control topics discussed in section 3.6.5 are also relevant to computer hardware and software. The topics addressed in section 3.6.6 should be those unique to computer hardware and software. Examples include: sample rates, real-time performance, data communications, and provisions for backing up programs and data.

If there are requirements on the design and development process for computer hardware and software aspects of the system being described (e.g., verification and validation, or qualitative reliability goals), they should be described in this section. Key design documentation (such as the Software Requirements Specification) should be referenced.

> Note: The performance of digital systems over the entire range of input conditions cannot be inferred from testing a limited sample of input conditions. Therefore, the design qualification for digital systems is often based on requirements for employing a high-quality development process that incorporates disciplined specification and implementation of design requirements.

If diverse or defense-in-depth features are provided as backup to protect against hardware or software features, these features should be identified in this section.

> Note: Software and hardware are often shared to provide multiple functions to a greater degree than is typical for analog systems. Although this sharing is the basis for many of the advantages of digital systems, it also presents the potential for common mode failures (or common cause failures) that might defeat the redundancy provided within the hardware and software. Sometimes diverse or defense-in-depth features that are not susceptible to the effects of such failures are provided to ensure that their consequences are tolerable. For example, the automatic computer monitoring and alarming for certain facility variables may be backed up by separate hardware indicators or manual surveillances.

If requirements exist related to the reliability of commercial off-the-shelf (COTS) hardware or software, they should be described. Such requirements may include vendor documentation demonstrating high reliability based on a formal program for recording and tracking failures.

> Note: Computer based systems often employ COTS; for example, source code embedded in a programmable logic controller (PLC) or local application programming of commercial software such as database management system software.

Administrative programs that support computer and software activities (such as software configuration management and quality assurance) should be described in the appropriate section of the SDD, which might be in Section 4.

3.6.7 Fire Protection

This section should identify requirements and their bases that might exist for fire protection features within the system, including detection, suppression, and other mitigation features. An example of the information provided in this section would be requirements on ventilation system fire dampers to close at or before a critical temperature is reached, and for the dampers to be rated for preventing the spread of fire for a specific time. This section should also identify special types of fire suppression materials, such as the need to use gaseous fire suppression systems in a particular area rather than a water sprinkler system.

3.7 Testing and Maintenance Requirements

This section should address those aspects of testing and maintenance of the system being described that are related to the design of the system.

3.7.1 Testability

This section should identify those design requirements and their bases that might exist for features that make the system testable, especially those design features that preclude the need to install temporary configurations manually on a frequent basis (e.g., every 12 months). For example, a requirement might exist to provide a test panel, with spring-loaded switches and bypass indicating lights, that eliminates the use of manually installed temporary configurations. Another example

might be a requirement to bring certain electrical connections to external test points to avoid internal electrical hazards and to avoid potential errors in manually installing temporary configurations. Operational (non-design) limitations on the use of temporary configurations are addressed in Section 4.3.1.

3.7.2 TSR-Required Surveillances

A summary of the TSR-required surveillances, with reference to the safety basis documents (e.g., TSRs), should be provided here in lieu of direct duplication of those documents. This section should not contain verbatim restatement of the TSR surveillance requirements. Rather, it should provide additional supportive technical information and explanations of the surveillance requirements such as those features provided in the design to facilitate those performing the testing.

3.7.3 Non-TSR Inspections and Testing

If the system being described is the subject of required inspection, testing, or surveillance requirements (including setpoint verifications or adjustments) that are not due to TSRs, this section should identify them, state how often they are required to be performed, state the acceptance criteria for these activities, and describe any design features necessary to perform those surveillance actions. These items should be clearly distinguished from TSR-required items.

> Note: Where surveillances, inspections, or testing beyond the TSRs have been applied at the option of the DOE contractor and compliance is expected by the contractor, they become requirements on the system and hence they should be included in this section.

> Note: In some cases, an industry code or standard may mandate certain in-service inspection (ISI) or testing (IST) activities. In many cases, the manufacturer recommends certain checks, tests, and calibrations that need to be adhered to (unless an engineering analysis establishes a basis for alternate activities or a modified schedule for those activities).

3.7.4 Maintenance

This section should identify maintenance activities required to comply with the manufacturer's recommendations or otherwise required to ensure continued reliability. Examples include requirements to periodically replace specified components in order to prevent a failure such as seals, lubricants that degrade over time, or certain parts that wear out-of-tolerances after a number of cycles or operations. When maintenance requirements are extensive, it may be beneficial to point to the applicable maintenance documents such as vendor technical manuals for the components of the system that support the intended safety function of the system.

3.8 Other Requirements

3.8.1 Security and Special Nuclear Material Protection

This section shall identify those requirements and their bases that are applicable to the system, related to the general security of the facility or the need to protect special nuclear materials (SNM). For example, the design of a vault to store SNM may be required to include features such as combination locks, weight, size, and seismic capability in order to protect the contents of the vault from certain postulated situations. However, the level of detail should be limited to protect security safeguards information, and simply referencing the applicable security source documents may be appropriate.

3.8.2 Special Installation Requirements

This section shall identify any requirements and their bases that may exist related to special arrangements, locations, or installation of components of the system being described. These might include alignments, shock mounting, lengths of electrical signal cable, special routing requirements for pump net positive suction head considerations, physical separation between redundant equipment, location requirements to minimize equipment interferences, and "free space" requirements for maintenance access.

> Note: Some installation requirements may be specified in the vendor's or manufacturer's technical information that comes with the equipment. For example, equipment may be required to be wall mounted instead of floor mounted, be oriented in a particular direction, maintain a minimum bend radius for interconnecting equipment, or locate certain types of components in a fluid system (liquid or air) a minimum distance from a bend or other flow-perturbing component.

3.8.3 Reliability, Availability, and Preferred Failure Modes

This section should identify requirements and their bases for design provisions that will ensure the system will perform its function(s) by improving system availability, improving reliability by minimizing ways in which it can fail, or minimizing the impact of failures. Such provisions might include equipment redundancy, diversity, physical separation, electrical isolation, features that provide mechanisms for on-line testing, features that avoid frequent use of temporary configurations (such as lifted leads or jumpers) for testing and maintenance, automatic fault detection capability, and preferred failure modes ("fail-safe" states).

3.8.4 Quality Assurance

This section should identify the general category of quality assurance (QA) to be applied to the system as a whole and to the components of the system and should identify any specific QA actions and how the system meets the QA requirements specified in the facility-specific QA plan. When the general QA category provides for options related to specific QA activities, the SDD should identify which options apply to this system. When specific QA requirements, such as witnessing vendor testing, are applicable only to certain components, those requirements should be identified (perhaps in a table) in the SDD. Safety features that should be demonstrated during procurement, startup, and maintenance should be included and uniquely identified.

3.8.5 Miscellaneous Requirements

This part of the system requirements section of the SDD is for requirements and their bases that do not fit conveniently into the other defined sections.

4. CHAPTER 4: SYSTEM DESCRIPTION

The SDD shall include a comprehensive description of the system safety features. It should also include a description of its important non-safety features. The description should emphasize those features provided to meet the requirements of the system. This section should identify the components of the system; describe how those components are laid out physically and interconnected; explain the system flow paths; identify the indicators, controls, and alarms provided; define the acceptable ranges for system performance and setpoints; and explain how the system operates.

The manufacturer and model number for components in the current system configuration should be recorded in a controlled document for several reasons including to facilitate identifying the applicable information in vendor-supplied documents. In some cases, the SDD may be the most appropriate place to record this information. In other cases, the SDD may reference a separate controlled document or ES such as the Computer Maintenance Management System (CMMS or Master Equipment List) or Bill of Materials that contains this configuration information.

The system should be described with specific values, rather than simply a repetition of the requirements. For example, a requirement on a system might be that the centerline of a pump suction line be located more than 8 inches and less than 14 inches above the bottom of a tank. This requirement might have been based on a combination of net positive suction head considerations for the pump and avoiding debris that may be on the bottom of the tank. The system description should not simply repeat the 8 to 14 inches requirement, but rather describe the actual installation more specifically, such as stating that the centerline of the suction pipe is 11.25 inches above the bottom of the tank. In another example, for a requirement that a valve be provided with position indication that is displayed in the control room, the SDD should not simply say that valve indication is provided in the control room. Instead, it should state specifically that valve position limit switches are provided on the valve that indicate on the auxiliary systems panel in the control room when the valve is greater than 90% open (green light) or greater than 90% closed (red light).

In addition, features of the system description that are related to the system requirements should be correlated. One effective method for this correlation is use of footnotes. For example, a footnote to a particular feature, characteristic, or performance capability might say, “This feature is related to System Requirement 3.3.4.15.” Conversely, the requirements in Chapter 3 of the SDD may contain footnotes/notes as to the corresponding description section of Chapter 4.

4.1 Configuration Information

4.1.1 Description of System, Subsystems, and Major Components

A more detailed system diagram than that provided in Chapter 2 of the SDD should identify the components in the system and their interconnections. This diagram should extend sufficiently to identify the interfacing equipment and systems. The boundary between the system being described and the interfacing systems shall be shown on the diagram in a distinctive manner. Similarly, the subsystems that have already been shown in the simplified system diagram in Chapter 2 of the SDD should be identified in a distinctive manner that can be correlated with the earlier diagram. For a very simple system, a single diagram may be used. For complex systems, multiple subsystem diagrams may be needed to describe the system.

A purpose of the system diagram is to illustrate which components are needed to fulfill the system functions. To the extent practical, piping and instrumentation diagrams (P&IDs) should be provided as the system diagram. For a fluid system or a ventilation system, the system diagram might be some form of a flow diagram. A P&ID is a system flow diagram that also shows the location of installed

instrumentation and controls. For an electrical system, the system diagram might take the form of a one-line diagram. For electronic systems that involve components such as transducers, bi-stable voltage comparators, and power supplies, a system functional block diagram might be the most informative. For a computer system, the system diagram might take the form of a combination of a hardware diagram and a summary logic diagram. In many cases, it may be appropriate to provide a reference to the system drawing rather than including it in the SDD.

The system diagram shall encompass at least all the major components provided to meet the requirements of the system. The components shown on the diagram should be identified in the same manner as the equipment is labeled in the field. Pertinent sizing values should be shown on the diagram. For example, a fan may be identified as 10,000 cfm, a pump may be labeled as 250 gpm, and an electrical transformer may be identified as 480V/120V.

This section should also describe any operational or maintenance features that are beyond the design requirements. For example, a ventilation damper position indicator may have been installed in the operations center (in addition to the local position indicator) as an enhancement due to operational problems with that particular damper. These operational problems should be explained in sufficient detail to provide lessons learned. Appendix D, System History, may also be used to provide a synopsis of key maintenance and system changes and the associated lessons learned.

4.1.2 Boundaries and Interfaces

Defining the boundaries of the system is important so that components at or near the boundaries are classified properly and hence receive appropriate attention in activities such as the procurement of replacement parts and maintenance actions.

The precise boundaries of the system shall encompass all components needed for the system to meet all of its requirements. This includes mechanical boundaries, electrical boundaries, other support systems' boundaries, and instrumentation and controls boundaries. Mechanical boundaries should be based on components, and not based on a room location. Such components may be capable of isolating one system from another system. For example, these components might be isolation valves or dampers, fill and drain valves, vent valves, or safety relief valves. The system boundaries should extend out to and include such interface isolation devices.

Heat exchangers are typically assigned to the system from which the heat is being removed when the primary function is to remove heat; or to the system that is being heated when the primary function is to provide heat. Mechanical support components for piping and duct work should be included in the primary system, unless a separate facility system has been defined to address such supports generically.

Electrical boundaries are usually located at circuit breakers. For an electrical power distribution system, those breakers that route power to other distribution points are usually considered to be part of the electrical power system. However, those breakers that provide power uniquely to a particular system are often considered to be part of that system, instead of the electrical power system. For example, if a particular pump motor gets its electrical power from a specific circuit breaker in a panel, the breaker may be assigned with the pump motor to the pump system. In this case, the system boundary for the pump system should be at the input/line/supply side of the circuit breaker, not at the load side of the circuit breaker.

When instrument air is provided to support the functioning of a system, the instrument air components necessary for the system to accomplish its functions should be part of that system.

Where applicable, the boundary of the system should extend out to and include the first upstream isolation valve in the air supply if the system can still function when the isolation valve is closed. Sometimes this may be at a check valve associated with an air accumulator.

The instrumentation and controls (I&C) systems usually are not designated as separate systems but are most often considered integral portions of the system being controlled. The system boundaries should be determined by the interfaces with the supporting electrical power or instrument air necessary to make the I&C portions perform properly.

A separate I&C system may include sensors, controls, and signals to actuated equipment, and alarms. For example, an I&C computer-based system that provides overall operator control for a reactor (or multiple systems) is typically identified as a separate system. Such an I&C system might include flow, pressure, and temperature sensors; signal comparators; and alarm, control, and interlock signals. These signals and controllers may position valves, control motors, provide information and status displays to operators, provide alarm indicators for operators, and support data recording. If the I&C system has been designated as a separate system, the boundaries might be selected at the mechanical output connections to the flow sensor and at the input signal connections to the valve actuator since these components are typically a part of the system that is being controlled.

Interfacing systems should be defined to the level of detail needed to ensure proper functioning and support. The most critical of these interfacing systems are “support systems” because they provide services that are required for the system to perform as described. Electric power (both motive power and control power), steam power, and instrument air are examples. For the current actual configuration of the system, the important characteristics of the support systems should be defined.

The system being described may also provide support that is essential to the performance of another system. For example, a particular control system may be essential for the proper operation of a ventilation system.

4.1.3 Physical Layout and Location

The system diagram, being schematic in nature, does not identify the location of the equipment or physical configuration. This section (or another figure) should explain where the equipment is installed (building, room numbers) and its physical arrangement within each room. Any special features regarding the installation, location or arrangement of the equipment should be explained.

4.1.4 Principles of Operation

This section should describe generally how the system operates with emphasis on how the system accomplishes its required functions. This discussion should also describe other operational features about the system. For ease of understanding, the discussion should use a walk-down approach, referring to and following the system and subsystem flow paths in the diagram.

The description should not be limited to the required performance; rather, it should reflect the full capabilities and capacities of the installed system. Extra optional capabilities of the system design beyond that required, such as extra capabilities beyond the safety margins that were added by the designer or were obtained as part of the procurement process, should be identified to prevent these from being considered as part of the “safety margin” at some time in the future. For example, a particular set of components might have been required to be designed for a 0.20 g earthquake, but the actual equipment was designed and qualified for a 0.35 g earthquake.

The discussion should be appropriate to the intended audience of the SDD (e.g., Cognizant System Engineers, operations, maintenance). This discussion should not be as detailed as an engineering analysis or so simplistic as to not add value. This discussion should be developed in coordination with the discussion of the system operational considerations to be provided in Section 4.2, Operations, to avoid overlap or repetition.

When components of the system are unusual or complicated, the principles of their operation should be explained. For example, if the system contains a proportional-integral-derivative (PID) controller, the SDD should summarize its operation. When a system contains multiple components of similar type (e.g., PID controllers, gamma radiation detectors, sonic level sensors, etc.) a generic description of the operating principles for each type of instrument or component may be more practical.

4.1.5 System Reliability Features

This section should describe any attributes, features, design or operating characteristics, and other information important to the reliability of the system. System design characteristics such as preferred failure modes or "fail-safe" positions or states should be discussed. This section should discuss other known failure modes of the system and their effects on the system and the facility. (The associated compensatory measures and recovery action are addressed in Section 4.2.4.) References should be provided to applicable engineering studies or failure modes and effects analyses (FMEAs), if such reports are known to exist. Features in the system design that make the system testable should be described.

Where the system includes redundant subsystems or components, the SDD description should identify these redundant features. The SDD should describe the capacity and degree of redundancy provided. For example, a particular design might require the operation of two exhaust fans at all times, but four fans are provided in the design. If two fans are required, each might be a 50 percent capacity fan, with two additional 50 percent fans in standby, ready for operation. Also, this section should discuss independence of the redundant features and any technical limitations on their use. For example, although four fans are available for operation, a maximum of only three fans is allowed to be operated at one time to avoid excessive flow rates.

4.1.6 System Control Features

This section should describe the indication, alarm, and control features of the system that are used to operate the system and monitor its performance. Control logic diagrams should be provided directly or via a link or reference.

4.1.6.1 System Monitoring

The instrumentation, indicators, alarms, and other information provided to operations personnel, remote and local, to allow assessment of system status and performance should be described, including types, ranges, and accuracies. This may include indicators, recorders, status lights, computer monitor displayed information, computer printouts, and information automatically stored on disks or tapes. The locations of these items should be identified clearly, such as being mounted directly on the equipment, installed remotely on a nearby control panel, or installed remotely in a central location.

Instrumentation either directly subject to TSRs or that provides information to verify compliance with TSRs should be identified as such.

4.1.6.2 Control Capability and Locations

System, equipment, and component manual operational controls should be described. The locations of these controls and the actions caused by actuating these controls should be identified clearly.

4.1.6.3 Automatic and Manual Actions

The SDD should describe the conditions under which important features are to be activated and whether these features are activated automatically or manually. Where automatic or manual controls are specifically associated with specific instrumentation, the instrumentation and control actions should be correlated in the SDD. For example, the control action might be taken only upon reaching a particular value as detected by a specific instrumentation channel or displayed by a specific indicating device, or an indicator might provide feedback of system response that shall be closely monitored.

Where alarms are provided that are intended to trigger manual safety actions, the SDD should provide an overview of the operator actions that are to be taken and refer to the corresponding operating procedures that govern the operator responses to the alarms. Alarms for non-safety actions (such as those that identify the need for operational adjustments or fine tuning) should be described similarly. Footnotes should be used to point to the particular procedure in the appropriate appendix to the SDD. This discussion should be coordinated with the discussion in Section 4.2, Operations, related to off-normal operations in a manner that avoids overlap and repetition.

4.1.6.4 Setpoints and Ranges

This section of the SDD should identify setpoints associated with the system (including pre-trip alarms) and the purpose of the setpoints. The values of setpoints and other system limitations should be correlated with the system requirements, especially TSR-required setpoints.

> Note: A common practice is including setpoints and limitations information in a set of tables in a stand-alone document that contains such information for numerous systems. When a setpoint entry is made into the table, the entry should identify the adjustment by name, where the adjustment is located physically, where and how the adjusted value is determined, the nominal value of the adjustment, the range of acceptable values for the setpoint, and the bases for the values. The acceptable ranges should be specified in actual values, not as tolerances, percentages, or other approaches that necessitate calculations. The setpoint value should be in terms of the measured value. For example, the requirement for a ventilation system may be in terms of ventilation flow rate (cubic feet per minute) while the actual measured value might be in differential process (psid).

Not repeating setpoint data in the SDD may be advantageous in order to avoid the need to revise the SDD each time a setpoint specification is changed. When complete setpoint data is not provided as part of the SDD, provide a reference to the governing setpoint information.

Internal controls and adjustments that are beyond the domain of operators but within the domain of maintenance personnel should be identified. Not all adjustments need to be identified in the SDD; however, some setpoints affect the limits of performance of the equipment and should be identified in the SDD. For example, a backup diesel generator may have an automatic trip on overspeed or overcurrent. The preferred approach to these setpoints is to identify in the SDD those setpoints that have a direct bearing on the limits of system performance and to present the nominal values of those setpoints. The SDD should also provide a footnote reference to the maintenance procedures or other

information that identifies all the internal setpoints and adjustments and provides the range of acceptable values.

4.1.6.5 Interlocks, Bypasses, and Permissives

This section should identify interlocks, automatic and manual operating bypasses, permissives, and other design constraints or conditions associated with the system being described. For example, the function of a particular safety system may become available automatically after system pressure exceeds a specified value, but be deactivated below this pressure to prevent inadvertent actuation when the system is operating within a pressure range for which the safety function is not needed. Interlocks provided to prevent or permit certain system actions or responses only when specific conditions are met should be listed. This section also should identify and explain provisions for manually disabling, bypassing or otherwise altering system performance, and the conditions and limitations under which they are to be used.

4.2 Operations

When procedures exist, this section should provide an overview of system operations to enable the reader to gain an understanding of the scope and intent of the approved procedures. The system operations should be described in a general manner that will aid the reader in understanding the detailed procedure steps, their required sequence, and how the system operations is integrated with facility operations. This section should identify good practices related to the operation of the system that operations personnel have voluntarily adopted. For example, operations personnel may have assigned equipment nomenclatures and equipment labeling in accordance with a particular good practices guide.

4.2.1 Initial Configuration (Pre-startup)

Some systems are required by their safety basis or other external requirement to be verified (e.g., by system walkdown or status checks) in the proper configuration for system operation prior to those systems being started. When this is the case, the SDD should describe the pre-startup configuration in general terms and provide a reference to the applicable procedure(s).

> Note: As described in previous sections, footnotes should be used to refer to procedures for system operations.

4.2.2 System Startup

This section should summarize the key steps in the startup procedure and refer to the corresponding procedure.

Particular attention should be drawn to the startup sequence, any timing that is involved, and how it is determined that the system is ready for the next step. Finally, this section should describe how to determine if the system was started up successfully or unsuccessfully.

4.2.3 Normal Operations

This section shall identify all the normal operating modes of the system, describe when each mode is appropriate, and explain generally how mode changes are accomplished. A reference should be provided to the procedures that cover system operations, including operational mode changes, to the extent that such procedures exist. A footnote that refers to a particular referenced item in the appropriate appendix to the SDD may be convenient. This section should then focus on and generally describe the most frequently-used mode of operations, including routine checks on system

performance and performance data logging by the operations staff to verify that the system is operating normally, including the key parameters and their nominal values. Those surveillance actions performed by maintenance staff should be identified in Section 4.3.

This section should identify the types of automatic records or logs that are maintained by or for the system in the central control area, including any equipment status changes that are "alarmed" during normal operations.

This section should also briefly address conduct of operations as it applies to this particular system. For example, at shift turnover, certain types of information about how this system is functioning might be appropriate or required. Then a reference should be provided to the specific procedure that provides the details for these aspects of the operation of the system.

4.2.4 Off-Normal Operations

This section shall identify off-normal conditions for or during which the system is intended to operate. Off-normal events range from simple, ordinary events such as the failure of a particular component, to anticipated system upsets (such as loss of cooling or lubrication, excessive leakage, or high radiation levels), to unlikely events such as a fire, explosion, or earthquake. For each off-normal event, this section should identify how the upset would be detected, describe the impact of the event on functional capability of the system, and, to the extent appropriate, describe the impact on the facility.

This section should summarize briefly the recovery actions for each type of off-normal condition. Some facilities use what are called "Alarm Response Procedures" that define pre-planned, reviewed, and approved actions that operators are to take when particular alarms are activated. Typically, such procedures will identify each important alarm that requires action, describe what conditions will cause that alarm to activate, define those few immediate operator actions, and then define the less-urgent, follow-up actions appropriate to that alarm. This section should provide a reference to the appropriate documents for recovery actions.

4.2.5 System Shutdown

If the system must be shut down in a particular sequence or with special timing, those system shutdown actions should be summarized and a reference to the corresponding procedure provided.

4.2.6 Safety Management Programs and Administrative Controls

This section should identify the aspects of safety management programs that apply to the system being described. This discussion should focus on the unique aspects of the application of those programs (such as radiation control and configuration management) and simply reference the general programs that apply to many systems at the facility.

This section should identify administrative controls placed on the system and/or its operation, and reference the associated procedures. If general access to the equipment of the system is restricted in any way, those restrictions should be identified in general terms.

4.3 Testing and Maintenance

When procedures exist, this section should provide an overview of testing and maintenance activities so as to enable the reader to gain an understanding of the scope and intent of the approved procedures. These activities should be described in a general manner that will aid the reader in understanding the

detailed procedure steps, their required sequence, and how system maintenance supports facility operations. This section should identify good practices related to the system that maintenance personnel have voluntarily adopted. For example, maintenance personnel may have decided that all battery testing will be performed in accordance with a particular national standard.

4.3.1 Temporary Configurations

Situations under which temporary configurations are used during surveillance or maintenance should be identified and described in the SDD. The SDD should state the operational limitations on the use of those configurations and should refer to the applicable governing procedures.

Temporary configurations may be needed to conduct surveillance, testing, inspection, and maintenance activities properly. For example, it might be necessary to lift leads temporarily so that the fire deluge system will not be activated during the test of the fire detection system. In most cases, operational limitations on the use of such temporary configurations may impact system availability. For example, redundant sets of equipment might not be allowed to be jumpered out, bypassed, or otherwise rendered out of service at the same time. Another type of limitation might be time constraints on how long lifted leads, jumpers, bypasses, etc., are permitted to be in use, especially where operability is a factor. The SDD should define compensatory measures required during the time the equipment is not operable or is out of service. Another limitation might be special provisions in procedures to control the use of such temporary configurations adequately, including removal verifications, especially if the use or misuse of such configurations could affect safety or availability.

4.3.2 TSR-Required Surveillances

When the system being described is the subject of TSR Surveillance Requirements, the SDD shall summarize the methods used to meet the requirements in this area (including confirmation that the acceptance criteria have been met), and refer to the procedures used to implement these requirements.

4.3.3 Non-TSR Inspections and Testing

When the system being described is the subject of non-TSR inspection, testing, or surveillance requirements, the SDD should summarize the methods used to meet the requirements in this area (including confirmation that the acceptance criteria have been met), and should provide references to the implementing procedures.

4.3.4 Maintenance

This section is aimed primarily at meeting the needs of maintenance personnel, although it contains some information that is important to operating personnel. This information is also important to the Cognizant System Engineer responsible for all aspects of the system, which includes testing and maintenance actions. This section should summarize the routine actions required by preventive maintenance procedures and post-maintenance modification testing procedures. This section should provide references to appropriate maintenance procedures or technical manuals.

4.3.4.1 Post-Maintenance Testing

This section should explain the extent to which a post-maintenance testing program is applied to the system. It shall identify key performance or acceptance criteria that are required to be satisfied or verified during post-maintenance testing (for the system to fulfill its functions identified in the hazards and accident analyses). This section should provide the applicable references to post-maintenance testing procedures and any additional operability considerations. For many systems,

both the TSR and non-TSR inspections and tests will have been described in earlier sections of the SDD; therefore, those sections should be referenced as appropriate.

4.3.4.2 Post-Modification Testing

In some cases, the maintenance organization also serves as the construction or installation organization for system modifications. In such cases, care should be taken to ensure that change activities are recognized as different from maintenance. The SDD should explain the extent to which a post-modification testing program applies to the system being described. As in the previous section, both the TSR and non-TSR inspections and tests already may have been described in earlier sections of the SDD; therefore, those sections should be referenced as appropriate.

4.4 Supplemental Information

Some have found it beneficial to address supplemental topics in the SDD in order to facilitate other considerations, including the Unreviewed Safety Question process. This section may include the following topics:

a. Summary of potential system and component failures and reference to any failure modes and effects analyses (FMEA) or related analyses, failure modes, probability/likelihood consequences (effects of failures) and mitigative features
b. Margins of safety in the design
c. Optional extra performance capabilities
d. Summary of critical engineering studies and calculations
e. System limitations and precautions
f. Other

APPENDICES TO THE SDD

Appendix A: Source Documents

This appendix should contain the bibliographical information for documents that are referenced in the body of the SDD. Separate appendices may be included for documents of various types, such as design documents, procurement documents, vendor documents, etc., or a single appendix may be subdivided into sections that address different document types.

Appendix B: System Drawings and Lists

This appendix should identify the diagrams and drawings and other relevant information provided in separate documents, tables, or lists associated with or affecting the system being described. These include physical arrangement diagrams, isometric drawings, installation drawings, P&IDs, functional control diagrams, process flow diagrams, schematic and one-line diagrams, wiring diagrams, sketches of particular portions or features of the system, load lists, setpoint tables, and instrument calibration lists.

This appendix should also identify (but not duplicate) master equipment lists, parts lists, Bills of Materials, and lists showing the hierarchy of drawings that are pertinent to the system being described.

To avoid unnecessary revisions of the SDD, this tabulation of the system drawings should not include specific revision numbers/letters or revision dates. Instead, this appendix should state that the most recently approved version is to be used.

Appendix C: System Procedures

This appendix should contain a listing of the procedures associated with or affecting the system being described. In a manner similar to the System Drawings appendix, this appendix should avoid specific revision information. Procedures should be listed in groups according to their general type; for example, operating procedures, TSR surveillance procedures, and maintenance procedures.

Appendix D: System History

This appendix is optional and may be more appropriately maintained in the CSE System Notebook, Facility Maintenance History, or other facility record. If included, this appendix should list those system modifications or changes considered to be of significance, such as those that result in changes to requirements, bases, TSRs, and setpoints. The maintenance and repair actions considered to be of major significance should also be identified. Each such modification or change and maintenance or repair action should be briefly summarized and the appropriate documentation referenced, such as design change packages or work packages. System history information may be kept in separate referenced files or systems.

This section should also include applicable lessons learned from testing, start-up, and operations.

APPENDIX F: COMPILING TECHNICAL INFORMATION FOR THE DEVELOPMENT OF SDDS

A key variable in determining the level of effort involved in development of an SDD is the amount of effort required for locating, screening, and reviewing source documents, and extracting the desired information from them. The more technical information used, the more useful the resulting SDD will be. Facility management should establish a plan for collecting and reviewing design information. This attachment provides information that can help with that plan.

1. AVAILABILITY OF DESIGN INFORMATION

Field experience in both the commercial nuclear industry and the DOE nuclear complex indicates that some virtually new facilities have already "lost" important design information that once existed, and that many "existing" facilities, including those dating back to the 1940s, have design information still on hand or reasonably retrievable. The need to capture the design information when it was produced was not recognized, and as a result, it may have been simply discarded at the end of the design effort. The same may be true for modifications to existing facilities. At some new DOE facilities, a moderate amount of information is on hand but some essential information is no longer available. At others, a moderate amount of information is on hand, but the reliability or trustworthiness of the information is questionable. At a few DOE Sites, a vast amount of highly trustworthy information is available.

For all new Hazard Category 1, 2 or 3 nuclear facilities or for select high hazard facilities for which this Standard is to be applied, it is important to define, as specific contract deliverables, the data that should be captured early in the preliminary design stage on a system-by-system basis. This will ensure that the data is methodically captured and maintained from the beginning.

Whether a facility is new or an existing facility is not a significant factor in developing SDDs; rather, development is affected by the amount of design information needing to be captured, and whether that information is on-hand or can be retrieved within reasonable efforts.

2. THE DOE-STD-3009 APPROACH

DOE-STD-3009 provides a sound approach to establishing the important technical requirements for safety SSCs that are used in the development of DSAs to meet 10 CFR 830. That approach involves a combination of two points: 1) using design information that is immediately available or can be retrieved through reasonable efforts; and 2) developing new information regarding the functional requirements as part of the process hazards analysis effort in sufficient detail to support the safety analysis. Documented engineering judgments (including their bases) can be used to extrapolate existing information and thereby establish the performance capabilities of the existing systems. The assumed performance capabilities can often be verified against records of operating experience or by testing at relatively small costs. These capabilities, once verified to be adequate by analysis and validated in the field, then become requirements. This approach has technical merit and is suggested by OSHA in its rulemaking regarding the process hazards analysis program. When sufficient technical information is not on hand or reasonably retrievable, this second method is recommended.

3. DOCUMENT RETRIEVAL

Efforts to retrieve design information have sometimes been limited to searches only for specific types of information under the perception that such a limitation will lead to cost-effective results. Although general decisions regarding how far to look for information can be made and are valid, experience has shown that a priori limiting the search to certain types of information may neither be effective nor efficient.

Reasonable general limitations can be placed on the search for design information. A recommended approach is to try to identify the most promising locations and search only those places. Identifying those locations that are most likely to have the desired information is usually possible. Contacting long-term technical staff to learn where key documents are should be an early step.

An important management consideration is to know when to stop. To facilitate answering this question, management must understand the information needed and the types of documents that are likely to contain the information. Engineers with design experience can usually describe what types of documents typically are produced for different types of systems and components. The search can be stopped upon completion of reasonable efforts to retrieve the types of documents that would be expected to contain the needed information. Compiling all information and data should not be a requirement to begin the SDD development process. Cost effectiveness may be gained by obtaining readily available information and data on the system, then developing a draft of the SDD from which a determination can be made as to any additional information that is needed. Typically, this will result in a parallel SDD development and information search that supports phased and graded approaches to the development of an SDD.

4. REVIEWING RETRIEVED DOCUMENTS

The Cognizant System Engineer should ascertain which of the retrieved documents contain information that is applicable to the current configuration of the facility.

A question arises about what to do with documents that are not related to the current SDD task. Some suggest disposing of the documents or sending them to Records Management. An approach might be to make a list of the documents found, to be maintained in the System Notebook. Another approach used by some facilities to establish the initial baseline is to conduct the search/retrieval process for all the SDD systems as one consolidated task and to keep an inventory of other documents found for broader future uses. These or other approaches result in an SDD project document list (PDL) for future reference. Some facilities have chosen to include this PDL as an appendix in the SDD so as to document and preserve this information. Some facilities have recognized further benefits from a PDL, such as providing the basis for determining that necessary information/documents for the system are in the “Master Document List” or in records management for ready retrieval. Maintaining a PDL may also assist engineers and management in determining when to stop searching for information.

Having retrieved some documents related to the system, one effective approach is to organize and sort the documents by system, then by type of document (reports and studies, analysis, calculations, drawings, specifications, procurement documents), and finally by document date with the most recent documents on top.

Older records are not likely to be segregated as safety design information and non-safety design information. Including this non-safety information in the SDD at the same time that safety data is being captured is cost-effective.

5. RESOLVING CONFLICTING INFORMATION

When information in one source document does not agree with information in another source document, the Cognizant System Engineer may be able to identify information that is outdated and no longer applicable. However, sometimes the conflicts cannot be easily resolved. In such cases, the conflict should be formally documented and tracked until it is resolved. Keeping a log of open items for the SDD for this purpose is recommended.

The open items need to be reviewed to determine if any are safety significant. Safety-significant open items should be treated as discrepancies within the facility non-conformance program. Also, the discrepancies need to be reviewed to determine whether they have an impact on the operability of any systems, or any reportable occurrences. Open items that are not safety-significant but involve critical information that could have an adverse impact on facility operations also should be formally tracked to closure.

6. MISSING INFORMATION

With the retrieval of design information completed, a determination should be made regarding what information may still be missing and if any of that information is truly critical to safety or to effective and efficient operations. If the missing information is not critical, no more time or money should be invested in perfecting the data bank. If the missing information is critical, a plan should be developed to recover that information. In a few cases, calculations or analyses might have to be regenerated.

APPENDIX G: APPLICATION OF THE GRADED APPROACH TO THE DEVELOPMENT OF SDDS

Substantial flexibility is allowed for the development of SDDs to address priorities and resources available to the facility. This appendix addresses the systems for which SDDs may be appropriate and the application of the graded approach to SDDs, including phased development. The DOE should provide direction to the contractor via the Contracting Officer if the DOE expects to have SDDs or FDDs developed for specific systems beyond safety class and safety significant active systems. If the contract does not require the implementation of this Standard, then the DOE may, through the Contracting Officer, define a subset (graded approach) of SDDs they wish to see developed. For new construction, the level of detail and number of SDDs should be defined as part of the contract deliverables at the beginning of design, with a focus on assuring that DOE has sufficient information to effectively implement DOE O 420.1B. The graded approach for a new project is to be defined in the project-specific QA Plan per DOE O 414.1C. Phasing of the development of the SDDs against the design process should also be defined at the beginning of design. Phasing could be based on the state of design (e.g., all SDDs initiated but only for those sections that can be supported by the design state completed), by safety system, or by equipment procurement status.

The use of an enterprise system rather than hard copy documents should be considered and encouraged for new projects.

1. FACILITY CATEGORIZATION

The graded approach should be applied based on a number of considerations, including the hazard categorization of the facility (in accordance with DOE-STD-1027) and the function of the system. Appropriately graded levels of effort could then be established, each of which would provide system requirements and system description information. At a Hazard Category 1 nuclear facility, the decision might be, for example, that a facility design description (FDD) will be developed and SDDs will be developed for all safety and mission- critical systems. At a Hazard Category 2 nuclear facility, the decision might be, for example, that SDDs will be developed only for safety SSCs. At a Hazard Category 3 nuclear facility, the decision might be, for example, that separate SDDs will not be developed, but instead, an FDD will be developed that describes the facility from an overall perspective and summarizes all the SSCs. Such an FDD would most likely emphasize the system requirements and system descriptions for each system.

2. FACILITY REMAINING LIFETIME

The useful life of the completed SDD should be long enough to make it worth the resources expended to develop the SDD. If the remaining lifetime of the facility is less than five years, development of SDDs may not be considered worthwhile. However, if the facility is required by its safety analysis to contain a significant source term for a number of years, SDDs are effective to convey needed information across staff or contract changes. The contractor should formally document the decision and basis for that decision if SDDs are not developed for Hazard Category 2 nuclear facilities.

3. SSC CLASSIFICATION

The systems within the facility should be classified in accordance with 10 CFR 830. The system importance classification should be used to determine which systems need to have SDDs developed. All active safety SSCs should have SDDs developed (safety SSCs include both safety-class SSCs and safety-significant SSCs). Development of SDDs for passive safety SSCs should be determined and

documented on a case-by-case basis, depending on the complexity of the passive SSC and the needs of the facility. Developing SDDs for environmental-protection and mission-critical systems is also encouraged, especially if the system fulfills a regulatory requirement.

4. GRADING WITHIN AN SDD

When the decision has been made to develop an SDD for a particular system, the graded approach determines the level of effort to be applied during development. The factor that will have the greatest effect on the level of effort required to develop an SDD is the complexity of the system involved. Simple systems might yield an SDD of only a few pages. Complex systems might necessitate many pages to describe requirements, bases, and operational aspects.

The topics to be addressed in an SDD may be adjusted. The most important active systems would have SDDs that are the most comprehensive. Less important systems or passive safety systems might not warrant the cost of developing such comprehensive SDDs. For example, sections of the outline such as “Operations” (Appendix E, Section 4.2) and “Testing and Maintenance” (Appendix E, Section 4.3) might be considered for omission. When a section is not included, the author should provide a brief explanation as to the basis for excluding the information.

Having determined which topics of the outline need to be addressed in an SDD for a particular system, the next consideration is the level of detail to which a topic should be addressed. For important systems, a particular topic in the outline may warrant a page or more of discussion. For a less important system, that same topic may warrant one paragraph or simply a reference to appropriate procedures. This is particularly pertinent with regard to Section 4 of the SDD.

The graded approach is not used to justify inaccuracies in SDDs. Bad information is worse than no information. Care should be exercised to ensure that all statements, tables, drawings, and other information in an SDD are accurate, regardless of the system classification and the graded approach.

5. PHASED APPROACH

In addition to the decisions regarding which systems warrant SDDs and the extent of the content of particular SDDs, another consideration is whether to schedule or divide the development of those SDDs into time phases. For example, SDDs for safety-class systems might be developed during the first year, followed by SDDs for safety-significant systems the second year. The remaining SDDs would be scheduled for subsequent years. This approach is particularly relevant for existing systems.

The content of the SDDs should be scheduled for development in stages, particularly for new projects/designs and for major upgrades of existing facilities (e.g., line item upgrades). For example, the system requirements and bases would be developed for all SDDs early in the project and issued to the project team. Then, as additional information becomes available during the subsequent design and construction phases, the SDDs would be updated (and issued) by developing the additional sections, or further developing sections initiated in prior revisions. Population of particular sections should be based on when the information for that section is available.

APPENDIX H: PREPARATION OF FACILITY DESIGN DESCRIPTIONS (FDDs)

Facility Design Descriptions (FDDs) generally should be prepared using the guidance contained within this document for SDDs. However, the content of FDDs should focus on facility SSCs (e.g., structural features, architectural features, site features), systems that are facility-wide that are not the subject of an SDD (e.g., potable water system, electrical distribution system), and information that is common to multiple systems (e.g., acceleration spectra). The limitations section of the FDD should clearly state the boundaries of information contained within the document.

For some facilities with limited systems, only an FDD should be developed. This particularly should be considered where the facility does not contain any active SC/SS systems. In other facilities, where the number of systems is very small, it may be more appropriate to develop only SDDs. No requirement exists that a facility requires both FDDs and SDDs.

The FDD should be a higher level document than the SDDs and, in many cases, should contain details on overall facility functions, facility systems that support process systems (e.g., electrical distribution system) in lieu of placing this information in SDDs. The SDDs should then refer to the FDD for the higher level functions, requirements, and programs. The FDD should also reference any lower tier SDDs for further details that are specific to those systems.

The structure of the FDD should be similar to the SDD outline format with a few exceptions. In most cases, the SDD sections should be placed in the FDD with "facility" replacing "system." The FDD should clearly distinguish content of facility SSCs and minor systems not within the scope of SDDs, such as potable water. Instead of a system diagram in Section 2.3, Basic Operational Overview, the FDD should contain a simplified facility plan diagram. In addition, in any section discussing boundaries/interfaces, the FDD should delineate facility SSCs and boundaries/interfaces with any systems that are in SDDs.

Section 3, Requirements and Bases, of the FDD should contain requirements and bases that apply to the overall facility such that they need not be repeated in lower tier SDDs. For example, programmatic requirements, general nuclear criticality safety requirements for facility draining (e.g., floor design with sloping), mezzanines, structural columns, and seismic spectra that apply to all SSCs in the facility would be examples of content ideally placed in the FDD rather than repeated in each SDD. Many sections in the SDD outline may not apply to the FDD (e.g., Section 3.1.5, Operability) and may be omitted from the FDD. In Section 3.2.6, human interface requirements and logical layouts should be included in the FDD. For better division in the FDD, Section 3 may be applied to the facility and an identical Section 4 may be used for SSCs that are in other systems not covered in SDDs, such as potable water system.

The last section in the FDD (Section 4 or 5) is the Facility Description. The subsections in this section should contain, at a minimum: description of facility SSCs, description of boundaries/interfaces with other SSCs, and description of layout and location. Principles of operation and description of controls, setpoints, and ranges should be included if applicable.

The appendices in the FDD should include the following, at a minimum:

- Appendix A: Source Documents
- Appendix B: Facility Drawings
- Appendix C: System Design Descriptions
- Appendix D: Facility-Level Procedures

- Appendix E: Facility History (including significant facility-wide changes and additional facility projects)